LECTURE 3

YIHANG ZHU

The Main reference is [Neu99] §§3,8,9.

1. Number fields

Let R be a Dedekind domain with fraction field K. Using unique factorization, we see that the set of nonzero ideals of R form a semi-group under multiplication which is isomorphic to $\bigoplus_p \mathbb{Z}_{\geq 0}$. We can produce a group $\bigoplus_p \mathbb{Z}$ out of it by formally introducing the negative powers of a prime ideal. This can be done in a more concrete way, with the concept of a *fractional ideal*.

Definition 1.1. A *fractional ideal* is a nonzero finite R-submodule of K. Equivalently, it is a nonzero R-submodule I of K such that $\exists a \in R - \{0\}, aI \subset R$.

Definition 1.2. Let I be a fractional ideal. Define $I^{-1} := \{a \in K | aI \subset R\}$.

We define the product of two fractional ideals in the same way as ideals.

Proposition 1.3. *Every fractional ideal is uniquely factorized as* $I = \prod_{i=1}^{g} \mathfrak{p}_i^{e_i}$, *where* $\mathfrak{p}_i$ *are prime ideals and* $e_i \in \mathbb{Z}$. *The set of fractional ideals form a group under multiplication, where the identity element is* R *and the inverse of* I *is* I^{-1} *defined as before. This group is free abelian on the set of prime ideals.*

Now let K be a number field. Any element $a \in K^\times$ gives rise to a fractional ideal $a\mathcal{O}_K$, called a principal fractional ideal. Let I_K be the group of fractional ideals. Define the *class group* to be $\mathrm{Cl}(K) = \mathrm{Cl}(\mathcal{O}_K) := I_K/K^\times$. We have an exact sequence of abelian groups

$$1 \to \mathcal{O}_K^\times \to K^\times \to I_K \to \mathrm{Cl}(K) \to 1.$$

We see the difference between elements and fractional ideals of K are measured by the groups $\mathcal{O}_K^\times$ and $\mathrm{Cl}(K)$. Among the main achievements of 19th century algebraic number theory is the determination of the structure of these two groups.

Theorem 1.4. $\mathrm{Cl}(K)$ *is a finite group.*

The proof uses geometry of numbers. The same technique yields to prove:

Theorem 1.5. *Let* r_1 *be the number of real embeddings of* K, *and* r_2 *be the number of pairs of conjugate complex embeddings of* K, *so that* $[K : \mathbb{Q}] = r_1 + 2r_2$. *The group* $\mathcal{O}_K^\times$ *is a finitely generated abelian group isomorphic to* $\mathbb{Z}^{r_1+r_2-1} \oplus T$, *where* T *is the finite cyclic group consisting of the roots of unity in* K.

For proofs of these two theorems see §§4,5,6,7 of [Neu99]. The proofs are extremely beautiful.

Example 1.6. $\mathcal{O}_K^\times$ is finite if and only if $K = \mathbb{Q}$ or is an imaginary quadratic field. Let K be an imaginary quadratic field, then the group of roots of unity in K is $\{\pm 1\}$ unless $K = \mathbb{Q}(\sqrt{-1}), \mathbb{Q}(\sqrt{-3})$. When K is a real quadratic field, the group

$\mathcal{O}_K^\times/\{\pm 1\} \cong \mathbb{Z}$. A generator is called a *fundamental unit*, which is closely related to the study of Pell equations.

The class group $\mathrm{Cl}(K)$ governs the arithmetic complexity of K, and also has an amazing link to zeta values. We call the order of $\mathrm{Cl}(K)$ the *class number* of K, denoted by h_K.

Proposition 1.7. *Let K be a number field. TFAE.*

(1) $\mathcal{O}_K$ is a PID.
(2) $\mathcal{O}_K$ is a UFD.
(3) $h_K = 1$.

Example 1.8. Baker and Stark proved in 1967 that there are only nine imaginary quadratic fields with class number 1, which are $\mathbb{Q}(\sqrt{-n})$ with $n = 1$, 2, 3, 7, 11, 19, 43, 67, 163. It is conjectured by Gauss that there are infinitely many real quadratic fields with class number 1. The conjecture is still open today.

Example 1.9. Let K be a number field. There is a way to associate a function to K, called the Dedekind zeta function ζ_K. When $K = \mathbb{Q}$ it is Riemann's zeta function. There is a deep result called the class number formula, relating various arithmetic invariants of K to the special values of ζ_K. In particular, by the class number formula the fact that $\mathbb{Q}(i)$ has class number one is equivalent to the following identity:

$$1 - \frac{1}{3} + \frac{1}{5} - \frac{1}{7} + \cdots = \frac{\pi}{4}.$$

The class number formula also yields the following way to compute h_K for an imaginary quadratic field $K = \mathbb{Q}(\sqrt{n}), n < 0$ square free. Let w_K be the number of roots of unity in K. (4 for $\mathbb{Q}(i)$, 6 for $\mathbb{Q}(\sqrt{-3})$, 2 otherwise.) Let $N = |d_K|$. Then

$$h_K = -\frac{w_K}{2N}\sum_{a=1}^{N} a\chi(a),$$

where $\chi : (\mathbb{Z}/N\mathbb{Z})^\times \to \{\pm 1\}$ is a character characterized by $\chi(p) = (\frac{n}{p})$ for odd primes $p \not| n$.

Exercise 1.10. Compute the class numbers of $\mathbb{Q}(\sqrt{-5}), \mathbb{Q}(\sqrt{-6}), \mathbb{Q}(\sqrt{-10})$.

2. Prime factorization

Let L/K be a finite extension of number fields. For $\mathfrak{p}$ a prime ideal of $\mathcal{O}_K$, it generates an ideal $\mathfrak{p}\mathcal{O}_L$ of $\mathcal{O}_L$. The fundamental question in algebraic number theory is to determine how $\mathfrak{p}\mathcal{O}_L$ factorizes into prime ideals of $\mathcal{O}_L$. Write

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

where $\mathfrak{P}_i$'s are distinct prime ideals of $\mathcal{O}_L$. We say these $\mathfrak{P}_i$'s *lie above or divides* $\mathfrak{p}$. Note that every prime ideal $\mathfrak{P}$ of $\mathcal{O}_L$ divides a unique prime ideal of $\mathcal{O}_K$, namely $\mathcal{O}_K \cap \mathfrak{P}$. We call $e_i =: e(\mathfrak{P}_i, \mathfrak{p})$ the *ramification index*. The fields $\mathcal{O}_L/\mathfrak{P}_i \supset \mathcal{O}_K/\mathfrak{p}$ are finite fields, called the *residue fields*, usually denoted by $\kappa(\mathfrak{P}_i)$ and $\kappa(\mathfrak{p})$.

Define $f_i = f(\mathfrak{P}_i, \mathfrak{p}) := [\mathcal{O}_L/\mathfrak{P}_i : \mathcal{O}_K/\mathfrak{p}]$, called the *inertia degree*. We have the fundamental identity relating these numbers.

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

Definition 2.1. We say $\mathfrak{P}_i$ is *unramified* over $\mathfrak{p}$ if $e_i = 1$. We say $\mathfrak{p}$ is *unramified* in L if $e_i = 1, 1 \leq i \leq g$. We say $\mathfrak{p}$ is *inert* if $\mathfrak{p}\mathcal{O}_L$ is a prime ideal of $\mathcal{O}_L$, i.e. if $g = 1, e_1 = 1$. We say $\mathfrak{p}$ is *split* in L if $g = [L : K]$, or equivalently, $e_i = f_1 = 1, 1 \leq i \leq g$.

One should think of ramification as an exceptional case. In fact only finitely many primes of K are ramified in L. For $K = \mathbb{Q}$, the primes that are ramified in L are exactly the factors of d_L. In general the ramified primes are determined using the different and the relative discriminant. We introduce a useful way of computing prime factorization.

Write $L = K(\theta)$ with $\theta \in \mathcal{O}_L$, which can always be arranged. Consider the ring $\mathcal{O}_K[\theta]$. It is a subring of $\mathcal{O}_L$ and its fraction field is K. Such subrings of $\mathcal{O}_L$ are called *orders*. Define the *conductor* of $\mathcal{O}_K[\theta]$ to be

$$\mathfrak{F} = \{a \in \mathcal{O}_L | a\mathcal{O}_L \subset \mathcal{O}_K[\theta]\}.$$

It is the largest ideal of $\mathcal{O}_L$ that is contained in $\mathcal{O}_K[\theta]$. When $\mathcal{O}_K[\theta] = \mathcal{O}_L$, which can luckily happen in many cases, we have $\mathfrak{F} = \mathcal{O}_L$. We can determine the factorization of any prime ideals of $\mathcal{O}_K$ that is prime to $\mathfrak{F}$.

Proposition 2.2. *Let $\mathfrak{p}$ be a prime of K that is prime to $\mathfrak{F}$. (i.e. $\mathfrak{p}\mathcal{O}_L$ is prime to $\mathfrak{F}$.) Let $\kappa = \mathcal{O}_K/\mathfrak{p}$. Let $f(X) \in \mathcal{O}_K[X]$ be the monic minimal polynomial of θ over K. Over κ, factorize $f(X)$ into irreducible polynomials:*

$$f(X) = \prod_{i=1}^{g} f_i(X)^{e_i} \in \kappa[X],$$

where $f_i(X)$ are irreducible polynomials in $\kappa[X]$. Then the factorization of $\mathfrak{p}$ is given by:

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

where $\mathfrak{P}_i = \mathfrak{p}\mathcal{O}_L + f_i(\theta)\mathcal{O}_L$. Moreover, the inertia degree of $\mathfrak{P}_i$ is equal to the degree of $f_i(X)$.

Corollary 2.3. *If $\mathfrak{p}$ is a prime of K that is prime to $\mathfrak{F}$ and the discriminant of $f(X)$, then $\mathfrak{p}$ is unramified in L. In particular, this holds for all but finitely many primes.*

Example 2.4. Let K be a quadratic field with discriminant d. Recall $d \equiv 0, 1 \mod 4$. Then $\mathcal{O}_K = \mathbb{Z}[\theta]$ with $\theta = \frac{d+\sqrt{d}}{2}$. So we can apply the above proposition to determine the factorization of *all* the primes of $\mathbb{Z}$ in K. Let p be an odd prime. We have

(1) p is ramified in K if and only if $p|d$. We have $(p) = (p, \sqrt{d/4})^2$ when $4|d$, and $(p) = (p, \theta)^2$ when $4 \not| d$.

(2) Let p be prime to d and suppose $(\frac{d}{p}) = 1$. Then p is split. If $4|d$, we have $(p) = (p, \sqrt{d/4} - a)(p, \sqrt{d/4} + a)$ where $a \in \mathbb{Z}$ is any solution to $a^2 \equiv d/4 \mod p$. If $4 \not| d$, we have $(p) = (p, \theta - (d+a)b)(p, \theta - (d-a)b)$, where $a, b \in \mathbb{Z}$ are any solutions to $a^2 \equiv d, 2b \equiv 1 \mod p$.

(3) If p is prime to d and $(\frac{d}{p}) = -1$, then p is inert in K.

Moreover, 2 is ramified in K if and only if $4|d$, in which case $(2) = (2, \sqrt{d/4} - d/4)^2$. Suppose $4 \not| d$. When $\frac{d-1}{4}$ is odd, 2 is inert. When $\frac{d-1}{4}$ is even, $(2) = (2, \theta)(2, \theta + 1)$ is split.

Exercise 2.5. Work out the details.

Example 2.6. Recall $\mathcal{O}_{\mathbb{Q}(\zeta_p)} = \mathbb{Z}[\zeta_p]$. Assuming this, we have $(p) = (\zeta_p - 1)^{p-1}$.

3. 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 3.1. *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 $\{\mathfrak{P}_i\}_{1\le i\le g}$ 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 3.2. 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 3.3. 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 $\mathfrak{P}_Z$.

References

[Neu99] Jürgen Neukirch, *Algebraic number theory*, Grundlehren der Mathematischen Wissenschaften [Fundamental Principles of Mathematical Sciences], vol. 322, Springer-Verlag, Berlin, 1999, Translated from the 1992 German original and with a note by Norbert Schappacher, With a foreword by G. Harder. MR 1697859 (2000m:11104)