LECTURE 2

YIHANG ZHU

The Main reference is the first three sections of [Neu99]

1. Sum of two squares

Quadratic fields arise when studying quadratic Diophantine equations.

Question 1.1. *Let p be a prime. When is p of the form x^2+y^2 with $x, y \in \mathbb{Z}$?*

If $p = 2$ the answer is yes. If $p \equiv 3 \mod 4$, then no. We need to prove $p \equiv 1 \mod 4 \Rightarrow p = x^2 + y^2$. The equation can be rewritten as

$$p = (x + iy)(x - iy), i = \sqrt{-1}.$$

The idea is that finding a solution $(x, y) \in \mathbb{Z}^2$ is the same as finding a number $z = x + iy \in \mathbb{Z}[i]$ such that $p = z\bar{z}$. We use the following basic fact.

Fact 1.2. *The ring of Gaussian integers $\mathbb{Z}[i]$ is a UFD.*

We go on to determine the units and prime elements of $\mathbb{Z}[i]$. Define the norm map

$$N : \mathbb{Z}[i] \to \mathbb{Z}, z \mapsto z\bar{z}.$$

It is multiplicative and $Nz = N\bar{z}$. An element $u \in \mathbb{Z}[i]$ is a unit if and only if $Nu = 1$, so the group of units is $\{\pm 1, \pm i\}$. We factorize an odd rational prime p inside $\mathbb{Z}[i]$:

$$p = \prod \mathfrak{p}_i^{e_i}.$$

Then $p^2 = Np = \prod N(\mathfrak{p}_i)^{e_i}$ Which shows the factorization can only be one of the two forms

$$p = \mathfrak{p} \text{ or } p = \mathfrak{p}\bar{\mathfrak{p}}.$$

Note the second case implies $p = N\mathfrak{p} = x^2 + y^2$. If $p \equiv 3 \mod 4$, then the second case cannot happen, so $p = \mathfrak{p}$. Suppose $p \equiv 1 \mod 4$, then $(\frac{-1}{p}) = 1$, so p divides $x^2 + 1 = (x + i)(x - i)$ for some $x \in \mathbb{Z}$. Suppose $p = \mathfrak{p}$. Then $\mathfrak{p}$ can divide only one of $x + i, x - i$, but then $\bar{\mathfrak{p}} = \mathfrak{p}$ always divides the other! Contradiction. Hence $p = \mathfrak{p}\bar{\mathfrak{p}}$. Question 1.1 is solved.

The above discussion classifies the prime elements in $\mathbb{Z}[i]$ completely. In fact, if $\mathfrak{p}$ is prime element, then we claim that $\mathfrak{p}$ appears in the factorization of a rational prime p. This is because $\mathfrak{p}$ divides $N\mathfrak{p}$, hence it divides a rational prime factor of $N\mathfrak{p}$. Therefore $\mathfrak{p}$ falls into one of the three categories:

(1) $\mathfrak{p} \sim 1 + i$, which appears in $2 = \mathfrak{p}\bar{\mathfrak{p}} = -i\mathfrak{p}^2$.
(2) $\mathfrak{p} = x + yi$, with $x^2 + y^2$ equal to a rational prime p.
(3) $\mathfrak{p}$ is a rational prime $p \equiv 3 \mod 4$.

Correspondingly, the factorization of a rational prime p inside $\mathbb{Z}[i]$ has three behaviors:

(1) $2 = -i(1 + i)^2$. We say 2 is ramified.

(2) $p = \mathfrak{p}\bar{\mathfrak{p}}$ when $p \equiv 1 \mod 4$. We say p is split.
(3) p remains prime when $p \equiv 3 \mod 4$. We say p is inert.

Thus we have seen that solving the problem $p = x^2 + y^2$ is quite equivalent to determining the arithmetic structure of the ring $\mathbb{Z}[i]$. In the above discussion, a crucial input is determining $(\frac{-1}{p})$ for odd p according to $p \mod 4$. Later we will see that the Legendre symbol is a special case of the Artin symbol $(p, L/\mathbb{Q})$ for L a number field, which governs the factorization of p just as in this case. The Artin symbol is also called the Frobenius at p. In this case, we view $(\frac{-1}{p})$ as an element $\sigma \in \mathrm{Gal}(\mathbb{Q}(i)/\mathbb{Q}) \cong \{\pm 1\}$. Then $\sigma a \equiv a^p \mod \mathfrak{p}$ for $a \in \mathbb{Z}[i]$ and $\mathfrak{p}|p$. This is why we use the name Frobenius.

Exercise 1.3. Prove the last statement.

2. Number fields

The ring of Gaussian integers $\mathbb{Z}[i]$ can be recovered from its fraction field $\mathbb{Q}(i)$. The former consists of elements of $\mathbb{Q}(i)$ whose monic minimal polynomial over $\mathbb{Q}$ lies in $\mathbb{Z}[X]$.

Definition 2.1. Let $B \supset A$ be a rings. An element $b \in B$ is said to be *integral* over A if it is killed by a monic polynomial in $A[X]$. We say B is *integral* over A if each element of B is integral over A. The *integral closure* of A in B is the set of elements of B that are integral over A. We say A is *integrally closed* in B if A is equal to its integral closure in B. If A is an integral domain, we say A is *integrally closed* if A is integrally closed in its fraction field.

Exercise 2.2. Prove that a UFD is integrally closed.

Fact 2.3. *Let $B \supset A$ be rings. The integral closure of A in B is always a ring.*

Definition 2.4. A *number field* K is a finite extension of $\mathbb{Q}$. The ring of integers $\mathcal{O}_K$ of K is defined to be the integral closure of $\mathbb{Z}$ in K.

The ring $\mathcal{O}_K$ has very nice properties. One should have in mind that it is to K what $\mathbb{Z}$ is to $\mathbb{Q}$.

Proposition 2.5. *The fraction field of $\mathcal{O}_K$ inside K is K. In fact any $x \in K^\times$ is of the form a/b with $a \in \mathcal{O}_K, b \in \mathbb{Z}$. Any finite $\mathcal{O}_K$-submodule of K, in particular $\mathcal{O}_K$ itself, is a free $\mathbb{Z}$-module of rank $[K : \mathbb{Q}]$.*

The latter assertion means that there exists an integral basis, namely $n = [K : \mathbb{Q}]$ elements $\alpha_1, \ldots, \alpha_n \in \mathcal{O}_K$ such that

$$\mathcal{O}_K = \mathbb{Z}\alpha_1 \oplus \cdots \oplus \mathbb{Z}\alpha_n.$$

Define the trace and norm maps as in field theory, denoted by $\mathrm{Tr}_{K/\mathbb{Q}}, \mathrm{N}_{K/\mathbb{Q}} : K \to \mathbb{Q}$. Since $\mathbb{Q}$ is perfect, we have $\mathrm{Tr}_{K/\mathbb{Q}}(x) = \sum_\sigma \sigma x, \mathrm{N}_{K/\mathbb{Q}}(x) = \prod_\sigma \sigma x$, where σ runs through $\mathrm{Hom}(K, \bar{\mathbb{Q}})$. The trace and norm maps send $\mathcal{O}_K$ into $\mathbb{Z}$, because $\mathbb{Z}$ is integrally closed.

Definition 2.6. Let α_i be an integral basis for $\mathcal{O}_K$. The *discriminant* of $\mathcal{O}_K$ is the integer

$$\mathrm{disc}\, \mathcal{O}_K = \det(\mathrm{Tr}_{K/\mathbb{Q}}(\alpha_i \alpha_j)).$$

This number is independent of the choice of $\{\alpha_i\}$. It is also called the discriminant of K, denoted by disc_K or d_K.

Lemma 2.7. *Let* $\{\sigma_1, \ldots, \sigma_n\} = \mathrm{Hom}_{\mathbb{Q}}(K, \bar{\mathbb{Q}})$. *Then* $d_K = \det(\sigma_i \alpha_j)^2$.

Remark 2.8. Suppose $\mathcal{O}_K = \mathbb{Z}[\alpha]$. Then $K = \mathbb{Q}(\alpha)$ and we can take an integral basis to be $1, \alpha, \ldots, \alpha^{n-1}$, where $n = [K : \mathbb{Q}]$. In this case we see that d_K is equal to the discriminant of the minimal polynomial of α. (d_K is the van der Monde determinant $\det(\sigma_i \alpha^j) = \prod_{i \neq j}(\sigma_i \alpha - \sigma_j \alpha)$).

Exercise 2.9. Let $K = \mathbb{Q}(\sqrt{n})$ with n square free. If $n \equiv 1 \mod 4$, then $\mathcal{O}_K = \mathbb{Z}[\frac{1+\sqrt{n}}{2}]$ and $d_K = n$. If $n \equiv 2, 3 \mod 4$, then $\mathcal{O}_K = \mathbb{Z}[\sqrt{n}]$ and $d_K = 4n$. Concisely written we have $\mathcal{O}_K = \mathbb{Z}[\frac{d_K + \sqrt{d_K}}{2}]$ in any case.

Example 2.10. Let ζ be a primitive n-th root of unity. Consider the cyclotomic field $K = \mathbb{Q}(\zeta)$. It is the splitting field of $X^n - 1$. It is quite nontrivial to see that $\mathcal{O}_K = \mathbb{Z}[\zeta]$

We used fact that $\mathbb{Z}[i] = \mathcal{O}_{\mathbb{Q}(i)}$ is a UFD to study the problem of sum of two squares. However in general $\mathcal{O}_K$ fails to be a UFD.

Exercise 2.11. Show that the identity $3 \cdot 7 = (1+2\sqrt{-5})(1-2\sqrt{-5})$ gives two essentially different factorizations of 21 into irreducible elements in the ring $\mathcal{O}_{\mathbb{Q}(\sqrt{-5})} = \mathbb{Z}[\sqrt{-5}]$.

In fact, if $\mathcal{O}_K$ were always a UFD, then number theory would have been much easier. For instance one can come up with a false proof of Fermat's Last theorem by using the factorization $c^p = a^p + b^p = \prod_{i=1}^{p}(a + \zeta^i b)$ and the assumption that $\mathbb{Z}[\zeta]$ was a UFD to deduce a contradiction. Such a "proof" was outlined by Gabriel Lamé in 1847. Quite soon afterwards Ernst Kummer exhibited a counterexample to the unique factorization of $\mathbb{Z}[\zeta]$. Moreover Kummer came up with an absolutely great idea to rescue the situation. He defined objects called the "ideal numbers" and proved that they satisfy unique factorization. Using that Kummer was able to prove Fermat's Last Theorem for *regular primes*, for instance all the primes less than 100 except $2, 37, 59, 67$. However the language of "ideal numbers" used by Kummer was not widely understood by others until Dedekind clarified all the concepts using the modern language of ideals of rings. This is the origin of the name "ideal".

We recall some basic definitions in ring theory.

Definition 2.12. Let R be a ring. An *ideal* of R is a subset I of R such that for any $a, b \in I, r \in R$, we have $a + b \in I, ra \in I$. An ideal I is *maximal* if it is not equal to R and the only ideal $J \supsetneq I$ is $J = R$. An ideal I is *prime* if whenever $a, b \in R$ are such that $ab \in I$, we have $a \in I$ or $b \in I$. Let I, J be ideals. Define $I + J = \{a + b | a \in I,\ b \in J\}$. Define $IJ = \{\sum_{i=1}^{n} a_i b_i | n \geq 1, a_i \in I, b_i \in J\}$. Both $I + J$ and IJ are still ideals.

Example 2.13. Let A be an integral domain, $a \in A$. Then a is a prime element if and only if (a) is a prime ideal. In particular all the prime ideals of $\mathbb{Z}$ are (p) and (0).

Definition 2.14. Let R be an integral domain. R is called *Noetherian* if any ideal of R is generated by finitely many elements. R is said to be *one-dimensional* if any prime ideal of R is either zero or maximal. R is said to be *integrally closed or normal* if it is integrally closed in its fraction field. R is said to be a *Dedekind domain* if it is a one-dimensional Noetherian normal integral domain.

Example 2.15. Any PID is Dedekind.

Proposition 2.16. *Let K be a number field. Then $\mathcal{O}_K$ is a Dedekind domain.*

Later we will see that there is a strong analogy between Dedekind domains and smooth algebraic curves. This analogy is in a sense an elaboration of the naive observation that $\mathbb{Z}$ and $\mathbb{F}_p[t]$ are quite similar.

The concept of a Dedekind domain is not just an arbitrary enumeration of nice properties, but it is characterized by the unique ideal factorization property.

Theorem 2.17. *Let R be an integral domain. TFAE.*

1. *R is Dedekind.*
2. *Any nonzero ideal $I \subset R$ can be written as $I = \mathfrak{p}_1 \cdots \mathfrak{p}_k$, where $\mathfrak{p}_i$ are prime ideals of R. Convention: the empty product is R. The factorization is unique up to switching the order of the $\mathfrak{p}_i$'s.*

Remark 2.18. Using the unique factorization we can define when an ideal I divides another J in an obvious way. We have $I|J \Leftrightarrow J \subset I$.

Exercise 2.19. In a previous exercise, we saw that unique factorization fails in $\mathbb{Z}[\sqrt{-5}]$ because for instance

$$3 \cdot 7 = (1 + 2\sqrt{-5})(1 - 2\sqrt{-5}).$$

But we have the factorizations into prime ideals

$$\begin{aligned}(3) &= (3, \sqrt{-5} + 1)(3, \sqrt{-5} - 1),\\ (7) &= (7, \sqrt{-5} + 3)(7, \sqrt{-5} - 3),\\ (1 + 2\sqrt{-5}) &= (3, \sqrt{-5} - 1)(7, \sqrt{-5} - 3)\\ (1 - 2\sqrt{-5}) &= (3, \sqrt{-5} + 1)(7, \sqrt{-5} + 3).\end{aligned}$$

Prove these identities.

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 2.20. 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 2.21. 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 2.22. *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.*

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)