A Learning Note on Number Theory

Fang-Rong ZHAN(詹方榕)

https://zhanfangrong.cn

June 26, 2022

Contents

This rather brief learning note is aimed to introduce some basic constructions in algebraic number theory. I assume that the reader is familiar with a knowledge of ungraduate-level abstract algebra.

1 Ring of Integer

We call a finite extension of rational number field as **(algebraic) number field**, whose theory is then called **algebraic number theory**.

For a number field K, we can define ring of integer

$$\mathcal{O}_K := \{x : x^n + a_{n-1}x^{n-1} + \cdots + a_0 = 0, \forall a_i \in K\},$$

which is an analogue of $\mathbb{Z}$ as for $\mathbb{Q}$ in the sense that $\mathcal{O}_K$ is the integral closure of $\mathbb{Z}$.

Theorem 1.1. *$\mathcal{O}_K$ does form a ring.*

A common proof to this theorem is via symmetric polynomials, which is credited to Eisenstein. However, Dedekind gave out a more elegant proof via the following lemma.

Lemma 1.2. *Let L be a field containing A. An element α of L is integral over A iff there exists a non-zero f.g. A-submodule of L s.t. $\alpha M \subset M$.*

Definition 1.3. *The ring of elements of K integral over A is called **integral closure** of A in K. The integral closure of $\mathbb{Z}$ in an algebraic number field K is called the **ring of integer** $\mathcal{O}_K$ in K.*

Example 1.4. $K = \mathbb{Q}(\zeta_n), \mathcal{O}_K = \mathbb{Z}[\zeta_n] = \{\sum_{i=0}^{r} a_i \zeta_n^i | r \geq 0, \forall a_i \in \mathbb{Z}\}$.

If K is a quadratic field, say $K = \mathbb{Q}(\sqrt{m})$, where $m \neq 1$ is an integer that is not divisible by a square, then we have

$$\mathcal{O}_K = \begin{cases} \mathbb{Z}[\sqrt{m}] = \{a + b\sqrt{m} : a, b \in \mathbb{Z}\} & m \equiv 1 \bmod 4 \\ \mathbb{Z}\left[\frac{1+\sqrt{m}}{2}\right] = \left\{a + b\frac{1+\sqrt{m}}{2} : a, b \in \mathbb{Z}\right\} & m \equiv 1 \bmod 4 \end{cases}.$$

From the general theory of integral closure, we have as an additional group $\mathcal{O}_K \cong \mathbb{Z}^{\oplus n}, n = [K : \mathbb{Q}]$.

2 Unique Factorization

The *fundamental theorem of arithmetic* claims that every non-zero number has a factorization as

$$n = \pm p_1 \cdots p_s$$

with all p_i's prime, which is essentially unique up to order. Generally, an element π in a integral domain A is said to be **prime** if it is neither zero nor unit, and if

$$\pi | ab \implies \pi | a \text{ or } \pi | b.$$

If A is moreover a PID, then every non-zero element of A also has a factorization as

$$a = u\pi_1 \cdots \pi_s$$

with u an unit and all π_i's prime, unique up to order and replacing π_i with an associate.

We want to know to what extent such unique factorization holds or fails to hold in a number field. Firstly, it only make senses when we consider a subring of number field, actually the ring of integer in the field as we defined above. However, the ring of integer is not generally a PID. So we should make a modification. Lastly, in order to understand the arithmetic of the field, it is essential to understand the structure of its units, which we will investigate in the following section.

Example 2.1. $\mathbb{Q}(\sqrt{-26})$. *Notice that it holds*

$$3^3 = (1 + \sqrt{26})(1 - \sqrt{26}),$$

but neither $1+\sqrt{26}$ *nor* $1-\sqrt{26}$ *divided 3. Thus 3 is not prime. However, suppose* $3 = \alpha\bar{\alpha}, \alpha = x + y\sqrt{-26}, x, y \in \mathbb{Z}$, *then* $3 = x^2 + 26y^2$, *which has no solution. This means that the prime factorization fails to hold.*

Consider the equation

$$210 = 6 \times 35 = 10 \times 21.$$

By uniqueness of factorization we found that

$$210 = (2 \times 3)(5 \times 7) = (2 \times 5)(3 \times 7).$$

Therefore we wish to define some "prime ideal factors" such that, say in $\mathbb{Q}(-\sqrt{26})$,

$$27 = (\mathfrak{p}_1\mathfrak{p}_2)^3 = (\mathfrak{p}_1)^3(\mathfrak{p}_2)^3.$$

Now we want to characterize such prime ideal factors. It definitely comes from the algebraic integers it divides, i.e.

$$\mathfrak{a}|0; \mathfrak{a}|a, \mathfrak{a}|b \implies \mathfrak{a}|a \pm b; \mathfrak{a}|a \implies ab(\forall b \in \mathcal{O}_K); \mathfrak{a}|ab \implies \mathfrak{a}|a \text{ or } \mathfrak{a}|b.$$

Since we focus on multiples, we can let the ideal factors identity with the set of elements it divides, that is to say,

$$0 \in \mathfrak{a}; a, b \in \mathfrak{a} \implies a \pm b \in \mathfrak{a}; a \in \mathfrak{a} \implies ab \in \mathfrak{a}(\forall b \in \mathcal{O}_K); ab \in \mathfrak{a} \implies a \in \mathfrak{a} \text{ or } b \in \mathfrak{a}.$$

This is exactly what we have learnt about **ideal** in ring theory.

Definition 2.2. *For ideal $\mathfrak{a}, \mathfrak{b}$, their product is defined as*

$$\mathfrak{ab} = \{\sum_{i=1}^{n} a_i b_i : n \geq 1, a_i \in \mathfrak{a}, b_i \in \mathfrak{b}\},$$

again an ideal.

Example 2.3. $\mathbb{Q}(\sqrt{-26})$*, continued. Consider the following ideals in* $\mathbb{Z}[\sqrt{-26}]$

$$\mathfrak{a} = (3, 1 + \sqrt{-26}), \mathfrak{b} = (3, 1 - \sqrt{-26}),$$

both are not principal. We have

$$(3) = \mathfrak{ab}, (1 + \sqrt{-26}) = \mathfrak{a}^3, (1 - \sqrt{-26}) = \mathfrak{b}^3.$$

To sum up,

$$(3^3) = \mathfrak{a}^3\mathfrak{b}^3 = ((1 + \sqrt{-26}))((1 - \sqrt{-26})).$$

Such phenonmenon can be summarized by the following definition and theorem.

Definition 2.4 (Dedekind domain)**.** *For a non-zero ideal $\mathfrak{a}$, there is a factorization*

$$\mathfrak{a} = \mathfrak{p}_1 \cdots \mathfrak{p}_s$$

with all $\mathfrak{p}_i$'s prime, unique up to order.

Theorem 2.5. *$\mathcal{O}_K$ does form a Dedekind domain.*

One more word about fractional ideal.

Definition 2.6. *A **fractional ideal** of $\mathcal{O}_K$ is a non-zero $\mathcal{O}_K$-submodule $\mathfrak{a}$ of K such that $d\mathfrak{a}$ is contained in A for some non-zero $d \in A$, equivalently, $\mathfrak{a}$ is a non-zero f.g. $\mathcal{O}_K$-submodule in K. For $\alpha \in K^\times$, write $(\alpha) = \alpha\mathcal{O}_K$ and call it **principal fractional ideal**.*

3 Class Number and Unit Group

Definition 3.1. *For fractional ideals $\mathfrak{a}, \mathfrak{b}$ in K, their product is defined to be $\{\sum_{i=1}^{n} a_i b_i : n \geq 1, a_i \in \mathfrak{a}, b_i \in \mathfrak{b}\}$, again a fractional ideal.*

Theorem 3.2. *Let $\mathfrak{a}$ be a fractional ideal, then we have a factorization*

$$\mathfrak{a} = \prod_{\mathfrak{p}} \mathfrak{p}^{e_\mathfrak{p}},$$

where $\mathfrak{p}$ run over all non-zero prime ideals in $\mathcal{O}_K, e_\mathfrak{p} \in \mathbb{Z}$, and $e_\mathfrak{p} = 0$ holds for all but finitely many $\mathfrak{p}$.

Theorem 3.3. *All fractional ideals with their multiplication form a group. $\mathcal{O}_K$ is the unit. The inverse $\mathfrak{a}^{-1}$ is given by*

$$\mathfrak{a}^{-1} = \{x \in K : x\mathfrak{a} \subset \mathcal{O}_K\}.$$

Definition 3.4. *We define the **ideal class group** $\mathrm{Cl}(K)$ to be the quotient of the group of all fractional ideals by the subgroup of all principal fractional ideals $\mathrm{Cl}(K) = \mathrm{Id}(K)/\mathrm{P}(K)$*

Definition 3.5. *The **class number** is the order of $\mathrm{Cl}(K)$.*

One of two main results in algebraic number theory is

Theorem 3.6. *The class number of a number field is always finite.*

The other main result involve the unit group.

Definition 3.7. *The **unit group** of K is the multiplicative group of all invertible elements of $\mathcal{O}_K$.*

The structure of unit group can be well-expressed. Let r_1 denote the number of real embeddings of a number field K and $2r_2$ the number of non-real complex embedding. Therefore

$$K \otimes_{\mathbb{Q}} \mathbb{R} \cong \mathbb{R}^{r_1} \oplus \mathbb{C}^{r_2}$$

and $r_1 + 2r_2 = [K : \mathbb{Q}]$.

Theorem 3.8 (Dirichlet)**.** *Let $r = r_1 + r_2 - 1$. Then*

$$\mathcal{O}_K^\times \cong \mathbb{Z}^{\oplus r} \oplus (\textit{finite cyclic group}).$$

Example 3.9. $K = \mathbb{Q}(\sqrt{2}), r_1 = 2, r_2 = 0,$

$$\mathcal{O}_K^\times \cong \{\pm(1+\sqrt{2})^n : n \in \mathbb{Z}\} \cong \mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}.$$

Let K be a quadratic field $\mathbb{Q}(\sqrt{m}), m \in \mathbb{Q}_{>0}$, then $r_1 = 2, r_2 = 0$, as well as

$$\mathcal{O}_K^\times = \{\pm\varepsilon^n : n \in \mathbb{Z}\}.$$

We call such ε the **fundamental unit** of K.

Example 3.10. $1+\sqrt{2}$ *is the fundamental unit of* $\mathbb{Q}(\sqrt{2})$.

As an application, let's consider the Pell equation.

Proposition 3.11. *Suppose N is a non-square natural number. Let $P_N = \{(x,y) \in \mathbb{Z} \times \mathbb{Z} : x^2 - Ny^2 = \pm 1\}, P'_n = \{(x,y) \in P_N : x, y \geq 1\}$.*

1. $$\theta : P_N \to \mathbb{Z}[\sqrt{N}]^\times : (x,y) \mapsto x + y\sqrt{N}$$

   is a bijection.

2. *Let (x_0, y_0) be with the smallest x in P'_N, then it is also with the smallest y. Moreover,*

$$\mathbb{Z}[\sqrt{N}]^\times = \{\pm(x_0 + y_0\sqrt{N})^n : n \in \mathbb{Z}\},$$

$$\theta(P'_N) = \{(x_0 + y_0\sqrt{N})^n : n \geq 1\}.$$

For a proof, consult [1].

4 p-adic field $\mathbb{Q}_p$

This section devotes to define what a p-adic field is.

Let's consider the existence of rational points on a quadratic curve $ax^2 + by^2 = 1$. We introduce the Hilbert's symbol $(a, b)_v$, valued 1 if the rational solution exists, -1 otherwise, in $\mathbb{Q}_v$ if $v < \infty$ a prime, or in $\mathbb{R}$ if $v = \infty$.

To make the definition precise, we should first define what $\mathbb{Q}_p$ is.

Definition 4.1 (p-adic valuation)**.** $\mathrm{ord}_p(a) = k$ *if* $a = p^k \frac{m}{n}, p \nmid m, n$.

Definition 4.2 (p-adic absolute value)**.** $|a|_p = p^{-\mathrm{ord}_p(a)}$.

The following will give 3 equivalent definition of $\mathbb{Q}_p$.

The first definition. $\mathbb{Q}_p$ is the completion of $\mathbb{Q}$ about the p-adic metric $d_p(a, b) = |a-b|_p$.

Let $\mathbb{Z}_p$ be $\{a \in \mathbb{Q}_p : \mathrm{ord}_p(a) \geq 0\}$ and call it as **p-adic integer**.

The second definition. $\mathbb{Q}_p$ is the fractional field of $\mathbb{Z}_p$, where $\mathbb{Z}_p$ is the inverse limit $\varprojlim_n \mathbb{Z}/n\mathbb{Z}$ of the inverse system

$$\cdots \mathbb{Z}/p^4\mathbb{Z} \to \mathbb{Z}/p^3\mathbb{Z} \to \mathbb{Z}/p^2\mathbb{Z} \to \mathbb{Z}/p\mathbb{Z}.$$

By inverse limit we mean a subset $\{(a_n)_n\}$ of $\prod_n \mathbb{Z}/n\mathbb{Z}$ such that $\pi(a_{n+1}) = a_n$. Two definitions of $\mathbb{Z}_p$ are equivalent up to an isomorphism.

The definitions above both can be interpretated as that the greater n for two numbers both lie together in $\mathbb{Z}/p^n\mathbb{Z}$, the closer they are.

Remark 4.3. *Since* $|x + y|_p \leq \max(|x|_p, |y|_p)$, $|a_n| \to 0$ *is enough for a series in* $\mathbb{Q}_p$ *to be convergent.*

The third definition. p-adic expansion. We let

$$\mathbb{Q}_p = \{\sum_{n=m}^{\infty} c_n p^n : c_n \in \mathbb{Z}/p\mathbb{Z}, m \in \mathbb{Z}\}.$$

It is easy to see it is an analogous of Laurant expansion in complex analysis, which later play an important role in the interplay between number theory and algebraic geometry.

Back to the quadratic curve, we refine Hilbert's symbol from $\mathbb{Q}^\times \times \mathbb{Q}^\times \to \{\pm\}$ to $\mathbb{Q}_p^\times \times \mathbb{Q}_p^\times \to \{\pm\}$. For $a, b \in \mathbb{Q}_p^\times$, express them as

$$a = p^i u, b = p^j v (i, j \in \mathbb{Z}, u, v, \in \mathbb{Z}_p^\times),$$

and let

$$r = (-1)^{ij} a^j b^{-i} = (-1)^{ij} u^j v^{-i} \in \mathbb{Z}_p^\times.$$

We define for $p \neq 2$,

$$(a,b)_p = \left(\frac{r \bmod p}{p} \right),$$

and for $p = 2$,

$$(a,b)_2 = (-1)^{\frac{r^2-1}{s}} (-1)^{\frac{u-1}{2}\frac{v-1}{2}}.$$

We have

Theorem 4.4. $(a,b)_p = 1 \iff$ *there is a* $\mathbb{Q}_p^\times$ *solution on the quadratic curve.*

Finally we can answer when there is a $\mathbb{Q}$ solution by local information.

Theorem 4.5. *Let* $a, b \in \mathbb{Q}_p^\times$. $ax^2 + by^2 = 1$ *has* $\mathbb{Q}$ *solution iff it has* $\mathbb{Q}_v$ *solution for all* v *prime and* $v = \infty$.

P.S. I should have written something about Riemann's ζ function and Dirichlet's L function but I have got no more time. Sorry for that!

References

[1] 加藤和也, 🄵川信重, 🄴藤毅; 胥鸣伟, 印林生译 (2009): 数论 I——Fermat 的梦想和类域论. 现代数学基础 12, 高等教育出版社.

[2] 黎景辉 (2016): 代数数论. 现代数学基础 58, 高等教育出版社.

[3] Milne, James S.(2017). Algebraic Number Theory (v3.07). Available at `www.jmilne.org/math/`.