Handout: Overview of Algebraic Number Theory

Vincent Zahlen

April 8, 2022

1 Motivation

Here, let all rings be commutative with 1.
We want to understand the ring of integers $\mathbb{Z}$, which has many strong properties, mainly being a principal ideal domain (*PID*). This is untrue for many extension of $\mathbb{Z} : \mathbb{Z}[\sqrt{-6}]$, would be an example. Here we can consider the equation $25 = 5^2 = (1+2\sqrt{-6})(1-2\sqrt{-6})$. We have two different decompositions of 25 into irreducible elements.
To substitute the unique factorisation property of $\mathbb{Z}$ with another one for algebraic extension of $\mathbb{Z}$ is the main motivation in basic algebraic number theory.

2 Rings of Integer

Subject of algebraic number theory are *rings of integers* in number fields (algebraic extensions of $\mathbb{Q}$). The ring of integers $\mathcal{O}_K \subset K$ is defined as the integral closure of $\mathbb{Z}$ in the field K, meaning that it contains all algebraic elements of K that are zeros of polynomials of the form:

$$1 \cdot X^l + a_{l-1}X^{l-1} + \cdots + a_1 X + a_0, a_i \in \mathbb{Z}.$$

The simplest ring of integers is $\mathbb{Z} \subset \mathbb{Q}$. Understanding rings of integers helps us to understand elliptic curves and integer equation, since as it turns out, the factorisation in these rings gives solutions to integer equations. We will see that in the case of $\mathbb{Q}(\sqrt{\cdot})$ the ring $\mathcal{O}_K$ will always contain $\mathbb{Z}[\sqrt{\cdot}]$ which is what we want. In general $\mathcal{O}_K$ will be larger.

3 Arithmetic on Ideals

Ideals in a ring can be added, multiplied and divided in the following way:

$$\mathfrak{a} + \mathfrak{b} = \{a + b | a \in \mathfrak{a}, b \in \mathfrak{b}\}$$

$$\mathfrak{a} \cdot \mathfrak{b} = \{\sum a_i b_i | a_i \in \mathfrak{a}, b_i \in \mathfrak{b}\}$$

We say that $\mathfrak{a}|\mathfrak{b}$ if and only if $\exists \mathfrak{c} \subset A : \mathfrak{a} \cdot \mathfrak{c} = \mathfrak{b}$. The following are equivalent:

$$\mathfrak{a} \subset \mathfrak{p} \Leftrightarrow \mathfrak{p}|\mathfrak{a}.$$

3.1 Fractional Ideals

A $\mathbb{Z}-$submodule $\mathfrak{a} =< k_1, \ldots, k_l >_{\mathbb{Z}} \subset K$ is called a fractional ideal. We also see that $\mathcal{O}\mathfrak{a} = \mathfrak{a}$. Thus $\mathcal{O}$ acts as a 1 on the set of ideals.
The fractional ideal $\mathfrak{a}^* = \{x \in K | x \cdot \mathfrak{a} \subset \mathcal{O}\}$ may be considered the inverse of $\mathfrak{a}$ in K : $\mathfrak{a}^*\mathfrak{a}\mathfrak{b} = \mathcal{O}\mathfrak{b} = \mathfrak{b}$. Thus the set of fractional ideals forms an abelian group: $J_K = \{\mathfrak{a} \text{ fract. ideal in } K\}$. Note that by definition all "normal" ideals $\mathcal{O}$ are also fractional ideals!

4 Prime Ideal Factorisation

Consider a noetherian domain A that is also integrally closed, where every prime ideal is also maximal. These rings are called *Dedekind domains*. They have the property that every ideal $\mathfrak{a} \neq (0), (1)$ in A has a unique factorisation into prime ideals, completely analogous to the factorisation into prime elements in $\mathbb{Z}$.

$$\mathfrak{a} = \mathfrak{p}_1^{v_1} \cdots \mathfrak{p}_n^{v_n}, v_i \in \mathbb{N}_0.$$

We now replace the arithmetic of numbers in for example $\mathbb{Z}[\sqrt{\cdot}] =: B$ with arithmetic on ideals, just by considering instead of $x \in B$, the ideal $(x) \subset B$.
Another useful fact is that all the integer-rings of finite algebraic extensions of $\mathbb{Q}$ are always Dedekind domains: $\mathcal{O}_K \subset K, K|\mathbb{Q}$ has unique *PIF*.

5 The Class Group

By considering the group J_K that was introduced in (3.1) we can "measure" how much any Dedekind domain differs from a principal ideal domain (*PID*), which is in some way the "ideal situation" to do number theory in.

We find a subgroup $P_K \subset J_K$ that is made up of the fractional *principal* ideals. We consider the quotient group $Cl_K = J_K/P_K$ that will be trivial if and only if all frac. ideals in K, and thus all ideal in $\mathcal{O}$, are already *principal*.
With some extra construction we can prove that this group will always be *finite*.

5.1 Consequence of the Finite Class Group

For every number field $K|\mathbb{Q}$, there exists a finite extension $L|K$, which has ring of integers $\mathcal{O}_L \subset L$ that is principal. That means that every ring of integers is only finitely many adjoined elements away from being a principal ideal domain.

6 Units of $\mathcal{O}_K$

By replacing the arithmetic of numbers in these rings with the arithmetic of ideals, we lose all information on the units in the ring:

$$1 \to \mathcal{O}^\times \to K^\times \to J_K \to Cl_K \to 1.$$

This sequence is *exact*, meaning here that $\mathcal{O}^\times \hookrightarrow \mathcal{O} \in J_K$, which as we recall is the neutral element in J_K. Exactness implies that the units of $\mathcal{O}$ are exactly the kernel of the map that "replaces" the arithmetic of numbers with ideals.

We can however recover this information with the

6.1 Dirichlet Unit Theorem

This theorem gives the structure of the unit group $\mathcal{O}^\times \subset \mathcal{O}$ for a given ring of integers $\mathcal{O} \subset K|\mathbb{Q}$.

$$\mathcal{O}^\times \cong \mu(K) \oplus \mathbb{Z}^{r+s-1}.$$

The numbers r, s depend on the way we have to embed K into $\mathbb{C}$. If the algebraic numbers adjoined to $\mathbb{Q}$ to get K are complex, one has to use complex embeddings $K \to \mathbb{C}$, these always come in pairs, while real embeddings don't. Explicitly: when computing the units of a specific ring of integers, we find $r+s-1$ units ϵ_i so that we can write every unit of $\mathcal{O}$ as

$$\varepsilon = \zeta \epsilon_1^{v_1} \cdots \epsilon_{r+s-1}^{v_{r+s-1}}, v_i \in \mathbb{Z},$$

where ζ is some root of unity that is contained in $K|\mathbb{Q}$.