Some results of Algebraic number theory

Hugo Trebše (hugo.trebse@gmail.com)

5. avgust 2024

Kazalo

1 Pell's primes

1.1 Theoretical necessities

Definition 1.1

Very important stuff:

1. What is $1\frac{1}{2}$ generator property?
2. How to determine $\mathcal{C}(\mathcal{O}_K)$?
3. The equivalence classes in $C(\mathcal{O}_K)$ are under the following relation:

$$a \sim b \iff ab^{-1} \in \mathcal{F}(K) \text{ (the group of principal fractional ideals)}$$

First we state a certain theorem from the lectures (I definitely know how to prove it, I just don't want to :P).

Theorem 1.2: Inert, split and ramified primes of $\mathbb{Z}$ in $\mathcal{O}_{\mathbb{Q}(\sqrt{m})}$

Let $p \in \mathbb{P}$ be a rational prime. Then $\langle p \rangle$ factorizes as follows in $\mathcal{O}_{\mathbb{Q}(\sqrt{m})}$:

- if $p \mid m$, then $\langle p \rangle = \langle p, \sqrt{m} \rangle^2$
- if $p = 2$, then $\begin{cases} \text{if } m \equiv 3 \pmod 4 : \langle p \rangle = \langle 2, 1+\sqrt{m} \rangle^2 \\ \text{if } m \equiv 1 \pmod 8 : \langle p \rangle = \langle 2, \frac{1+\sqrt{m}}{2} \rangle \cdot \langle 2, \frac{1-\sqrt{m}}{2} \rangle \\ \text{if } m \equiv 5 \pmod 8 : \langle p \rangle \text{ is inert} \end{cases}$
- else: $\begin{cases} \text{if } m \equiv n^2 \pmod p : \langle p \rangle = \langle p, n+\sqrt{m} \rangle \cdot \langle p, n-\sqrt{m} \rangle \\ \text{if } m \not\equiv n^2 \pmod p : \langle p \rangle \text{ is inert} \end{cases}$

1.2 Pell's primes

If $p \nmid m$ and $p \neq 2$, then we know that $\langle p \rangle$ ramifies or splits if and only if m is a quadratic residue mod p.

If p splits then we know that the ideal $\langle p \rangle$ must be a product of at least two ideals. Since p is an element of the base field in a quadratic extension, it holds that $N(\langle p \rangle) = p^2$. Since norms of ideals, like norms of elements, lie in the base fields, which means that the norms of the decomposition ideals must multiply to give p^2. Since we define the norm of an ideal $\mathfrak{a} \trianglelefteq \mathcal{O}_K$ as $\mathcal{O}_K/\mathfrak{a}$, the norm of $\mathfrak{a}$ equals 1 when $\mathfrak{a} = \mathcal{O}_K$, which can't occur if $\langle p \rangle$ splits.

It follows that $\langle p \rangle$ splits into two prime ideals, each of which has norm p. Hence there exists an element in each of these ideals, which has the norm p.

It hence follows that for a fixed d, the diophantine equation

$$x^2 + dy^2 = p$$

has a solution $x, y \in \mathbb{Z}$ and $p \in \mathbb{P}$ if and only if d is a square modulo p.

2 Weak approximation theorem

We state the following less-known cousin of the *Chinese remainder theorem*.

Theorem 2.1: Weak approximation theorem

For all prime ideals $\mathfrak{p}_1, \mathfrak{p}_2, \ldots, \mathfrak{p}_n$ of a **Dedekind domain** D and for all choices of integers $e_1, e_2, \ldots, e_n$ there exists $x \in D$, such that

$$\langle p \rangle = \mathfrak{p}_1^{e_1} \mathfrak{p}_2^{e_2} \ldots \mathfrak{p}_n^{e_n} \cdot J,$$

where $J \trianglelefteq D$ is comaximal to every $\mathfrak{p}_i$.

We use this theorem to deduce the one and a half generator property of Dedekind domains.

Theorem 2.2: One-and-a-half generator property

We wish to show that in any Dedekind domain D, for any $I \trianglelefteq D$ and for all $x \in I \setminus \{0\}$, there exists an $y \in I$, such that

$$I = \langle x, y \rangle.$$

Proof. Decompose the ideal $I = {\mathfrak{p}_1}^{e_1} {\mathfrak{p}_2}^{e_2} \ldots \mathfrak{p}_n^{e_n}$. It is clear that $\langle x \rangle \subseteq I$. Factorize the ideal $\langle x \rangle$ as follows:

$$\langle x \rangle = \mathfrak{p}_1^{e'_1} \mathfrak{p}_2^{e'_2} \ldots \mathfrak{p}_n^{e'_n} \mathfrak{q}_1^{v_1} \mathfrak{q}_2^{v_2} \ldots \mathfrak{q}_m^{v_m}.$$

Clearly, $\forall\, 0 \leq i \leq n : e'_i \geq e_i$. Since $\langle x, y \rangle = \langle x \rangle + \langle y \rangle$, we seek y, such that

$$\nu_{\mathfrak{p}_i}(\langle y \rangle) = e_i \quad \text{and} \quad \nu_{\mathfrak{q}_j}(\langle y \rangle) = 0$$

$\forall\, 0 \leq i \leq n$ and $\forall\, 0 \leq j \leq m$. However the existence of such a y is ensured by the weak approximation theorem. It is easy to check that the ideal $\langle x, y \rangle$ indeed equals I, by well known properties of the p-adic valuation function. $\square$

3 Determining $\mathcal{O}_K$

Lemma 3.1

A Dedekind domain K is a PID if and only if it is a UFD.

We define the following equivalence relation on elements of $\mathcal{F}(K)$ - the group of fractional ideals of the Dedekind domain K:

$$a \sim b \iff ab^{-1} \in \mathcal{F}(K).$$

Then the following theorem holds (I also definitely know how to prove this theorem, but choose not to :P)

Theorem 3.2: Minkowski's theorem

Let $\mathcal{O}_K$ be the ring of integers of a number field K. Then for all $x \in \mathcal{C}(\mathcal{O}_K)$ there exists $I \trianglelefteq \mathcal{O}_K$ such that:

$$x = [I]_\sim \quad \text{and} \quad N(I) \leq \lambda_K,$$

where λ_K is the Minkowski bound, defined as follows:

$$\lambda_k = \frac{n!}{n^n}\left(\frac{4}{\pi}\right)^s \sqrt{|\text{disc}(\mathcal{O})_\mathcal{K}|},$$

where $n = [K : \mathbb{Q}]$ and s is the number of pairs of complex embdeddings of K into $\mathbb{C}$.

Since every equivalence class has a representative, it follows we only need to check ideals $\langle p \rangle$, to determine the class group - usually we determine its order and then use some arguments regarding the order of elements to pinpoint it exactly.

Now the question becomes: 'Which ideals of the form $\langle p \rangle$ are prime/maximal in $\mathcal{O}_K$?'. The answer is - look at $\mathcal{O}_K/\langle p \rangle$ and see if its a field/domain. Since