HOMEWORK 4 : THE FINITENESS OF THE CLASS NUMBER

HYOJIN KIM

In this note and the following one, we will sketch the proof of that the class number of a number field is finite. The method of proof gives an algorithm for computing the class group.

1. Basic notions

We will define some basic notions and prove briefly some propositions in this section.

Let A be a Dedekind domain with field of fractions K, and let B the integral closure of A in a finite separable extension L. We want to define a homomorphism $\mathrm{Nm} : \mathrm{Id}(B) \to \mathrm{Id}(A)$ which is compatible with taking norms of elements, i.e., such that the following diagram commutes:

$$\begin{array}{ccc} L^\times & \xrightarrow{b \mapsto (b)} & \mathrm{Id}(B) \\ \big\downarrow{\scriptstyle \mathrm{Nm}} & & \big\downarrow{\scriptstyle \mathrm{Nm}} \\ K^\times & \xrightarrow{a \mapsto (a)} & \mathrm{Id}(A). \end{array} \tag{1.1}$$

Let $\mathfrak{p}$ be a prime ideal of A, and factor $\mathfrak{p}B = \prod \mathfrak{B}_i{}^{e_i}$ where $\mathfrak{B}_i$'s are the prime ideals dividing $\mathfrak{p}$ and e_i's are the ramification indices. If $\mathfrak{p}$ is principal, say $\mathfrak{p} = (\pi)$, then we should have

$$\mathrm{Nm}(\mathfrak{p}B) = \mathrm{Nm}(\pi \cdot B) = \mathrm{Nm}(\pi) \cdot A = (\pi^m) = \mathfrak{p}^m, \ m = [L : K].$$

Also, because Nm is to be a homomorphism, we should have

$$\mathrm{Nm}(\mathfrak{p}B) = \mathrm{Nm}(\prod \mathfrak{B}_i{}^{e_i}) = \prod \mathrm{Nm}(\mathfrak{B}_i)^{e_i}.$$

On comparing these two formulas, we should define $\mathrm{Nm}(\mathfrak{B}) = \mathfrak{p}^{f(\mathfrak{B}/\mathfrak{p})}$ where $\mathfrak{p} = \mathfrak{B} \cap A$ and $f(\mathfrak{B}/\mathfrak{p}) = [B/\mathfrak{B} : A/\mathfrak{p}]$. I sometimes use $\mathcal{N}$ to denote norms of ideals.

Definition 1.1. *Let $\mathfrak{a}$ be a nonzero ideal in the ring of integers $\mathcal{O}_K$ of a number field K. Then $\mathfrak{a}$ is of finite index in $\mathcal{O}_K$, and we let $\mathbb{N}\mathfrak{a}$, the **numerical norm** of $\mathfrak{a}$, be this index:*

$$\mathbb{N}\mathfrak{a} = (\mathcal{O}_K : \mathfrak{a}).$$

Remark 1.2. *Let $\mathcal{O}_K$ be the ring of integers in a number field K.*
(a) For any ideal $\mathfrak{a}$ in $\mathcal{O}_K$, $\mathcal{N}_{K/\mathbb{Q}}(\mathfrak{a}) = (\mathbb{N}(\mathfrak{a}))$; therefore $\mathbb{N}(\mathfrak{a}\mathfrak{b}) = \mathbb{N}(\mathfrak{a})\mathbb{N}(\mathfrak{b})$.
(b) Let $\mathfrak{b} \subset \mathfrak{a}$ be fractional ideals in K; then

$$(\mathfrak{a} : \mathfrak{b}) = \mathbb{N}(\mathfrak{a}^{-1}\mathfrak{b}).$$

Definition 1.3. *Let V be a vector space of dimension n over $\mathbb{R}$. A **lattice** Λ in V is a subgroup if the form*

$$\Lambda = \mathbb{Z}e_a + \cdots + \mathbb{Z}e_r$$

*with $e_1, \ldots, e_r$ linearly independent elements of V. Thus a lattice is the free alelian subfroup of V generated by elements of V that are linearly independent over $\mathbb{R}$. When $r - n$, the lattice is said to be **full**.*

The subgroup $\mathbb{Z} + \mathbb{Z}\sqrt{2}$ of $\mathbb{R}$ is a free abelian group of rank 2, but it is *not* a lattice in $\mathbb{R}$.

Date: May 3, 2019.

Definition 1.4. *A subgroup Λ of V is said to be* ***discrete*** *if it is discrete in the induced topology. A topological space is discrete if its points (hence all subsets) are open, and so to say that Λ is discrete means that every point α of Λ has a neighbourhood U in V such that $U \cap \Lambda = \{\alpha\}$.*

Proposition 1.5. *A subgroup Λ of V is a lattice if and only if it is discrete.*

It suffices to show that a discrete subgroup is a lattice and we shall argue by inducion on the order of a maximal $\mathbb{R}$-linearly independent subset of Λ.

2. Finiteness of the class number

We will introduce the statements only and complete this section in the next note.

Let K be an extension of degree n of $\mathbb{Q}$, and let Δ_K be the discriminant of $K/\mathbb{Q}$. Let $2s$ be the number of nonreal complex embeddings of K. Then $B_K = \frac{n!}{n^n}\left(\frac{4}{\pi}\right)^s \mid \Delta_K \mid^{\frac{1}{2}}$ is the **Minkowski bound** and the term $C_K = \frac{n!}{n^n}\left(\frac{4}{\pi}\right)^s$ is called the **Minkowski constant**. The last part of this section, we will show that $\mathbb{N}(\mathfrak{a}) \leq B_K$.

Theorem 2.1. *The class number of K is finite.*

Let K be a number field of degree n over $\mathbb{Q}$. Suppose that K has r real embeddings $\{\sigma_1, \ldots, \sigma_r\}$ and $2s$ complex embedding $\{\sigma_{r+1}, \overline{\sigma_{r+1}}, \ldots, \sigma_{r+s}, \overline{\sigma_{r+s}}\}$. Thus $n = r + 2s$. We have an embedding

$$\sigma : K \hookrightarrow \mathbb{R}^r \times \mathbb{C}^s, \ \alpha \mapsto (\sigma_1\alpha, \ldots, \sigma_{r+s}\alpha).$$

We identify $V := \mathbb{R}^r \times \mathbb{C}^s$ with $\mathbb{R}^n$ using the basis $\{1, i\}$ for $\mathbb{C}$.

Proposition 2.2. *Let $\mathfrak{a}$ be a nonzero ideal in $\mathcal{O}_K$; then $\sigma(\mathfrak{a})$ is a full lattice in V, and the volume of a fundamental parallelopiped of $\sigma(\mathfrak{a})$ is $2^{-s} \cdot \mathbb{N}\mathfrak{a} \cdot \mid \Delta_K \mid^{\frac{1}{2}}$.*

Proposition 2.3. *Let $\mathfrak{a}$ be a nonzero ideal in $\mathcal{O}_K$. Then $\mathfrak{a}$ contains a nonzero element α of K with*

$$\mathrm{Nm}(\mathfrak{a}) \leq B_K \cdot \mathbb{N}\mathfrak{a} = C_K \mathbb{N}\mathfrak{a} \mid \Delta \mid^{\frac{1}{2}}.$$

Theorem 2.4. *Let K be an extension of degree n of $\mathbb{Q}$, and let Δ_K be the discriminant of $K/\mathbb{Q}$. Let $2s$ be the number of nonreal complex embeddings of K. Then there exists a set of representatives for the ideal class group of K consisting of integral ideals $\mathfrak{a}$ with*

$$\mathbb{N}(\mathfrak{a}) \leq \frac{n!}{n^n}\left(\frac{4}{\pi}\right)^s \mid \Delta_K \mid^{\frac{1}{2}} .$$

References

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