Indian Institute of Technology Gandhinagar

Applications to theory of Dedekind Domains

Discipline of Mathematics

Master of Science in Mathematics

Candidate

Tejas Pujari
Roll number 20510071

Thesis Advisor

Prof. Akshaa Vatwani

A dissertation submitted in partial fulfillment of the requirements for the degree of Master of Science in Mathematics

May 2, 2022

Thesis defended on in front of the Department Steering Committee composed by:

Prof.Akshaa Vatwani (chairman)
& other faculty members of Mathematics

Applications to theory of Dedekind Domains
M.Sc. Dissertation. Indian Institute of Technology Gandhinagar

This dissertation has been typeset by LaTeX and the IIT Gandhinagar class.

Version: May 2, 2022

Author’s email: akshaa.vatwani@iitgn.ac.in

Disclaimer

I, Tejas Pujari, declare that the ideas in this document have been expressed in my own words and, wherever needed, I have adequately cited and referenced the literature. I also declare that I have adhered to all principles of academic honesty and integrity and have not misrepresented or fabricated or falsified any idea/data/fact/source in my submission. I also declare that this document has not been submitted elsewhere for a degree.

(Tejas Pujari)

Dedicated to all those who helped me achieve this.

Abstract

The main goal is to prove that the Dedekind domain is not far from being a PID by proving that the ideal class group is finite. Firstly we shall prove the various versions of the Chinese remainder theorem and prove that every ideal in the Dedekind domains is either principal or generated by at most two generators. This information implies that the Dedekind domain is an almost principal ideal domain. Hence, our next primary task is to find how far the ring of algebraic integers is from being PID. For this work, we define the ideal class group of a number ring and then prove this group is finite, which is done by Minkowski was the first to prove this finiteness. We shall prove some results from geometric number theory to achieve our final goal.

Acknowledgments

I want to take this opportunity to thank Prof. Akshaa Vatwani for encouraging and helping me to enjoy my project along with the difficulties. I am also thankful to Dr. Sampa Dey, who took responsibility for my conceptual understanding by taking virtual and personal interactions, which helped me study this subject and complete my project.

Contents

List of Symbols

- $\mathbb{Z}/n\mathbb{Z}$ denotes the ring of integers modulo n.
- I, J denotes the ideals of the ring.
- P_i denotes prime ideals of that index.
- d_k denotes discriminant of number field unless mentioned.
- Δ_k denotes discriminant of number field unless mentioned K.
- Δ_I denotes discriminant of ideal I.
- $N(I)$ denotes norm of an ideal I.

Chapter 1

Introduction

Our aim is to study the applications of the theory developed by the 19-th century mathematician Richard Dedekind known as the theory of Dedekind domains. In the 19th century, it became a common technique to gain insight into integer solutions of polynomial equations using rings of algebraic numbers of higher degrees.In 1847 Gabriel Lamé announced a solution of Fermat's Last Theorem for all $n > 2$; that is, Fermat equation has no solutions in nonzero integers, but it turned out that his solution hinged on the assumption that the cyclotomic ring $\mathbb{Z}[\zeta_n]$ is a UFD. But Kummer has already shown that the unique factorization fails for the number rings $\mathbb{Z}[\zeta_n]$ through $n = 23$.So to proceed further in an attempt to prove Fermat's last theorem unique factorization of numbers in the number rings is a significant factor. However, Dedekind handled this concept in a new fashion and defined what we know today called as the Dedekind domains. This idea of Dedekind introduces the new concept known as the unique factorization of ideals in the number ring, so even if numbers are not expressed uniquely, Dedekind proved ideals are! Furthermore, this structure again resumes the work in the direction of Fermat's conjecture. Informally, Dedekind domains are integral domains in which every nonzero proper ideal factor into a product of prime ideals. It can be shown that such a factorization is then necessarily unique up to the order of the factors. It has been proved that the Dedekind domain is UFD if and only if it is PID.So the work was reduced to checking the ideal structure of such domains. Hence, our primary goal is to study the ideal structure by assuming the unique factorization property and how a Dedekind domain fails to be a PID by using various information from the Chinese remainder theorem and ideal class groups.

Chapter 2

Chinese Remainder Theorem and application to Dedekind Domains

- Chinese Remainder Theorem is one of the oldest known theorem. The earliest known statement of the theorem, as a problem with specific numbers, appears in the 3rd-century book Sun-tzu Suan-ching by the Chinese mathematician Sun-tzu. There are certain things whose number is unknown. If we count them by threes, we have two left over; by fives, we have three left over; and by sevens, two are left over. How many things are there?
    - The first solution is by Aryabhata (6 CE)

Statement - Let $n_1, n_2, ...n_r$ be pairwise coprime integers then the system of linear congruence [7]

$$\begin{array}{rcl} x & \equiv & a_1 \ (mod \ n_1) \\ x & \equiv & a_2 \ (mod \ n_2) \\ x & \equiv & a_3 \ (mod \ n_3) \\ \vdots & & \\ x & \equiv & a_r (mod \ n_r) \end{array}$$

admits a solution which is unique modulo $n_1 n_2 n_3 ... n_r$.

Before proving the theorem in more generality we will prove for the ring of integers $\mathbb{Z}$ then extend our idea to general ring.

Informally it states that the natural map

$$\mathbb{Z}/(n_1 n_2 ... n_r)\mathbb{Z} \longrightarrow \mathbb{Z}/n_1\mathbb{Z} \oplus \mathbb{Z}/n_2\mathbb{Z} \oplus ... \oplus \mathbb{Z}/n_r\mathbb{Z}$$

that sends a to reduction modulo n_i is an isomorphism.

Proof- Let us consider the natural map

$$\phi : \mathbb{Z} \longrightarrow \mathbb{Z}/n_1\mathbb{Z} \oplus \mathbb{Z}/n_2\mathbb{Z} \oplus ... \oplus \mathbb{Z}/n_r\mathbb{Z}$$

$$\phi(z) = (z\,mod(n_1), z\,mod(n_2), z\,mod(n_3), ..., z\,mod(n_r)$$

clearly this is an homomorphism

$$Ker(\phi) = \{z|\phi(z) = 0\}$$

$$Ker(\phi) = n_1\mathbb{Z} \cap n_2\mathbb{Z} \cap n_3\mathbb{Z} ... \cap n_r\mathbb{Z}$$

since $(n_i, n_j) = 1$ so,

$$n_1\mathbb{Z} \cap n_2\mathbb{Z} \cap n_3\mathbb{Z} ... \cap n_r\mathbb{Z} = lcm[n_1, n_2, ...n_r]\mathbb{Z}$$

$$n_1\mathbb{Z} \cap n_2\mathbb{Z} \cap n_3\mathbb{Z} ... \cap n_r\mathbb{Z} = n_1.n_2...n_r\mathbb{Z}$$

so the inclusion map

$$\mathbf{i} : \mathbb{Z}/(n_1n_2...n_r)\mathbb{Z} \longrightarrow \mathbb{Z}/n_1\mathbb{Z} \oplus \mathbb{Z}/n_2\mathbb{Z} \oplus ... \oplus \mathbb{Z}/n_r\mathbb{Z}$$

is injective.
Surjectivity:
let us consider a random element from $\mathbb{Z}/n_1\mathbb{Z} \oplus \mathbb{Z}/n_2\mathbb{Z} \oplus ... \oplus \mathbb{Z}/(n_r\mathbb{Z})$

say $(a_1, a_2, ...a_r)$ we have to show that $\exists a \in \mathbb{Z}/(n_1n_2...n_r)\mathbb{Z}$ such that $i(a) = (a_1, a_2, ...a_r)$

since n_i are pairwise coprime by bezout's lemma $\exists x, y \in \mathbb{Z}$ such that $xn_1 + y.n_2n_3n_4...n_r = 1$
$y.n_2.n_3...n_r = 1 - x.n_1$

observe that $y.n_2...n_r \equiv 1\; mod(n_1)$and $0\; mod(n_i)$ where $i \neq 1$

but then $i(y.n_2.n_3...n_r) = (1,0,0,0...,0)$ and similarly one can prove that $(0,1,0,....,0), (0,0,1,0,0,...0)....(0,0,0,....,1$
are in the range of the map which actually generates whole $\mathbb{Z}/n_1\mathbb{Z} \oplus \mathbb{Z}/n_2\mathbb{Z} \oplus ... \oplus \mathbb{Z}/n_r\mathbb{Z}$

hence surjectivity follows so the inclusion map is isomorphism.
so let us take $(a_1, a_2, ...a_r)$ where a_i are corresponding reminders module n_i in our system of congruences then by above isomorphism

$x = a_1.i^{-1}(1,0,0,...,0) + a_2.i^{-1}(0,1,0....,0) + a_3.i^{-1}(0,0,1,...,0) + ... + a_ri^{-1}(0,0,0,...,1)$ is the required solution for our system.

Note - By observing the above proof we actually get the idea to give the general construction of x and that is given as follows

Example

We will solve one problem to see this thing clearly

$$\begin{aligned} x &\equiv 2\ (mod\ 3) \\ x &\equiv 3\ (mod\ 5) \\ x &\equiv 2\ (mod\ 7) \end{aligned}$$

Find such x
Solution :- All modulus are pairwise coprime where $a_1 = 2, a_2 = 3, a_3 = 2$

so we induce the solution $x = 2c_1 + 3c_2 + 2c_3$ where

$c_i \equiv 1\ mod(n_i)$ and$c_i \equiv 0\ mod(n_j)$for$j \neq i$

after simple solving we get $c_1 = 70, c_2 = 21, c_3 = 15$

and hence $x = 233$ is the solution to above problem.

Coprime ideals = I, J be ideals of a ring R are said to be coprime ideals if $I + J = (1) = R$.

Lemma - Let I, J be coprime ideals of ring R then $I \cap J = IJ$.

proof- Given that I, J are coprime so by definition $I + J = (1)$ implies that $\exists x$ and y in I and J such that $x + y = 1$.

$IJ \subset I \cap J$ is follows trivially so the only reamaining part is $I \cap J \subset IJ$

lets us consider $c \in I \cap J$

$c = c.1 = c.(x + y) = cx + cy \in IJ + IJ = IJ$

so $c \in IJ$. hence $I \cap J = IJ$.

Lemma- Suppose $I_1, I_2, ...I_s$ are pairwise coprime then I_1 is coprime to product $I_2...I_s$.

proof-
we prove the result for $s = 3$ and further it follows by induction Let I_1, I_2, I_3 are pairwise coprime ideals

$$\begin{aligned} I_1 &+ I_2 = \langle 1 \rangle \\ I_2 &+ I_3 = (1) \\ I_1 &+ I_3 = (1) \end{aligned}$$

using eqn-1 and 3 we have ,

$$\begin{aligned} x_1 + y_1 = 1 \quad x_1 \in I_1, y_2 \in I_2 \\ a_1 + b_3 = 1 \quad a_1 \in I_1, b_3 \in I_3 \end{aligned}$$

multiply above 2 eqn we get

$$x_1 a_1 + x_1 b_3 + y_2 a_1 + y_2 a_3 = 1$$

which is nothing but an element of

$$I_1 + I_2 I_3$$

hence $I_1, I_2 I_3$ are coprime.
hence rest of the result follows by induction so proved

CRT for Rings

Suppose $I_1, I_2, ... I_r$ are non-zero ideals of a ring R such that I_m, I_n are pairwise coprime for $m \neq n$ then the natural homomorphism $\phi : R \longrightarrow \bigoplus_{n=1}^{r} R/I_n$ induces an isomorphism
[1]

$$\psi : R/\prod_{n=1}^{r} I_n \longrightarrow \bigoplus_{n=1}^{r} R/I_n$$

.
Thus given any $a_n \in R$ for $n = 1, 2, ... r$ $\exists$ some $a \in R$ s.t $a \equiv a_n \ mod(I_n)$ moreover a is unique modulo $\prod_{n=1}^{r} I_n$.

Proof- R is a ring and $I_1, I_2, ... I_r$ be coprime ideals.

$\phi : R \longrightarrow \bigoplus_{n=1}^{r} R/I_n$ be the natural reduction map which is homomorphism

observe that $Ker(\phi) = \cap_{n=1}^{r} I_n$

but since ideals are coprime by lemma-1

$$\cap_{n=1}^{r} I_n = \prod_{n=1}^{r} I_n$$

so substituting above in induced map we have

$$\psi : R/\prod_{n=1}^{r} I_n \longrightarrow \bigoplus_{n=1}^{r} R/I_n$$

is injective

since the projection map $R \longrightarrow R/I_n$ is surjective.

It is enough to show that $(1,0,0,...,0),(0,1,0,...,0),(0,0,1,0,...0),...(0,0,0,....,1)$ are in the range of ψ.

By Lemma-2
I_1 is coprime to $\prod_{n=2}^{r} I_n$

implies $\exists\, x \in I_1, y \in \prod_{n=2}^{r} I_n$ such that $x+y=1 \Rightarrow y=1-x$

$\phi(y) = (1,0,0,0,.....,0) \in img(\phi)$
similarly one can be show that other factors are in img(ϕ).

Hence ψ is surjective so the map is isomorphism.

Structural applications of CRT-

We will give the application of CRT in dedekind domains. Let's recall some basic notions about dedekind domains.

Dedekind Domain - An integral domain R is a Dedekind domain if it is Noetherian, integrally closed in its field of fractions and every prime ideal is maximal.

I,J be ideals then I divides J if $J \subset I$

Every ideal in a dedekind domain has a unique factorisation.

Theorem- R be a Dedekind Domain and I,J be non-zero ideals in R then there exists an $a \in I$ such that the ideal $(a)I^{-1}$ is coprime to J.
[1] **Proof-** First observe that if I is principle ideal say (b) then simply choose $a=b$ and then $(a).I^{-1} = (a)(a^{-1}) = (1)$ and which is coprime to every ideal so result follows trivially.

so the other part of the proof we have I a non-principle ideal.

Let $p_1,...p_r$ be the prime divisors of J for each i e_i is the largest power of p_i that divides I. Since $p_i^{e_i} \neq p_i^{e_{i+1}}$,

we can choose an element $a_i \in p_i^{e_i} - p_i^{e_{i+1}}$
observe that

$$p_1^{e_1+1}.p_2^{e_2+1},.....,p_r^{e_r+1},I.(\prod p_i^{e_i})^{-1}$$

are coprime ideals.

then by chinese remainder theorem applied to these $r+1$ coprime ideals implies there exists $a \in R$ such that

$$a \equiv a_i \; mod(p_i^{e_i+1}) \forall 1 \leq i \leq r$$

and also

$$a \equiv 0 \; mod \left(I.(\prod p_i^{e_i})^{-1}\right)$$

Now we prove $(a)I^{-1}$ is not divisible by any p_i or if we prove that $p_i^{e_i}$ completely divides (a)

then multiplying by I^{-1} nullifies the prime effect and we get the required thing, Hence we prove that $p_i^{e_i}$ divides (a) by above

$a \equiv a_i \; mod(p_i^{e_{i+1}})$ there exist $b \in p_i^{e_{i+1}}$ such that $a = a_i + b$ since $a_i \in p_i^{e_i}$ and since $p_{i+1}^{e_i+1} \subset p_i^{e_i}$ so $b \in p_i^{e_i}$ so $a \in p_i^{e_i} \implies p_i^{e_i} divides(a)$

now suppose $p_i^{e_i+1}$ divides (a) then $a_i = a - b \in p_i^{e_i+1}$ contradiction because of choice a , so $(a)I^{-1}$ is coprime to J

Theorem- R be a dedekind domain I be an ideal of R then I is generated by atmost 2 elements.

Proof- If $I = (0)$ then it is the ideal generated by 1 element and we are done. Suppose I is a non-zero ideal of R let a be a non zero element of I

we prove that there exist $b \in I$ such that $I = (a,b)$. Let $J = (a)$ then by above theorem there exists $b \in I$ such that $(b)I^{-1}$ is coprime to J. since $a,b \in I \implies I|(a) \;\&\; I|(b)$ so $I|(a,b)$

Now suppose $p^n|(a,b)$ where p is prime and $n \neq 0$ then $p^n|(a) \;\&\; p^n|(b)$ since $(b)I^{-1}$ is coprime to (a)

so $p \nmid (b).I^{-1}$. so we have $p^n|(b) = I.(b)I^{-1} \;\&\; p \nmid (b)I^{-1}$ so $p^n|I$

hence by unique factorisation in R $(a,b)|I$ combining above 2 we conclude that $I = (a,b)$.

Chapter 3

Finiteness of Ideal Class groups

Definition-An integral domain A satisifies the properties

1. A is a Noetherian ring;

2. A is integrally closed ;

3. Every nonzero prime ideal of A is maximal.

is called as Dedekind domain.

example K be a number field then ring of integers of K denoted by

$$O_K = \{x \in K | x \text{ satisifies a monic polynomial with coefficients in } \mathbb{Z}\}$$

is dedekind domain.

Fractional Ideal Let K be number field and O_K be ring of integers of K then an O_K -submodule I of K is said to be fracti

$\alpha \in O_K$ such that $\alpha I \subseteq O_K$

$K = \mathbb{Q}$, $O_K = \mathbb{Z}$ then

$$I = \left(\frac{1}{2}\right)\mathbb{Z} = \left\{\frac{m}{2} | m \in \mathbb{Z}\right\}$$

is a fractional ideal of $\mathbb{Z}$ as there exist $2 \in \mathbb{Z}$ such that $2 \cdot I = \mathbb{Z} \subseteq \mathbb{Z}$

Some Results-

1. The set of all fractional ideals of a Dedekind Domain O_K is an abelian group under multiplication with identity element O$_K$.It is denoted by F_{O_K}

2. Let I is a non-zero integral ideal of O$_K$ then I can be written as the product of prime ideals of O$_K$ and the representation is unique up to order. More generally, every nonzero Ideal I of O$_K$ factors as

$$I = \mathfrak{p}_1^{e_1} \cdots \mathfrak{p}_r^{e_r}$$

, for some non-negative integer r, distinct prime ideals $\mathfrak{p}_1,\ldots,\mathfrak{p}_r$ and nonzero positive integers $e_1,\ldots,e_r$ Furthermore, the prime ideals $\mathfrak{p}_1,\ldots,\mathfrak{p}_r$ and the corresponding exponents $e_1,\ldots,e_r$ are uniquely determined by I.

$$F_K = \{I: \ I \text{ is fractional ideals of } O_K\}$$

$$P_K = \{J: \ J \text{ principal fractional ideals of } O_K\}$$

We have already seen that F_A has a group structure and P_A is a subgroup of it.

Ideal class group

[9] The ideal class group denoted by $Cl(K)$, is

$$Cl(K) = F_K/P_K$$

We will call the elements of $Cl(K)$ ideal classes; thus an ideal class $[a]$ is simply a coset of P_K.

By definition of $Cl(K)$, two fractional ideals a and b lie in the same ideal class$(a\sim b)$ if and

only if there exist some $\gamma\in K^*$ such that,

$$\gamma\cdot a = b$$

The elements of this group are the ideal classes $[a] = \{xa : x\in K\}$, with the group law being

multiplication of representatives.

The group Cl(K) is abelian, and this group is trivial if and only if all fractional ideals in K are principal, which is equivalent to O_K being a PID.

Our main purpose is to prove this ideal class group is finite that is card$(Cl(K)$ is finite

Remark - Every ideal class can be represented as an integral ideal class i.e an ideal of ring O_K by using above equivalence relation and since every fractional ideal is of the form $\frac{1}{d}I$ for some integral ideal I so it follows that $\frac{1}{d}I\sim I$ so there belongs to same class hence every ideal class of $Cl(K)$ is represented by an integral ideal.

Norm of an Ideal

Let K is an algebraic number field of degree n and O_K is the ring of integers of K. Also I is a nonzero ideal of O_K then norm of the ideal I is defined by

$$N(I) = \text{card}(O_K/I)$$

Example Let $K = \mathbb{Q}$ and then$O_K = \mathbb{Z}$ and $I = \langle 4 \rangle$ then

$$N(I) = \left| \frac{\mathbb{Z}}{4\mathbb{Z}} \right| = 4$$

Properties of Norm

1. $N(IJ) = N(I)N(J)$
2. $N(\langle \alpha \rangle) = |N(\alpha)|$
3. $N(I)^2 = \frac{\Delta(I)}{d_K}$

We have the following important lemma which is the key towards the proof of finiteness of ideal class group:

Lemma- If every ideal class of K contains an integral ideal I with $N(I) \leq C$, where C is a positive real number independent of I (but may depend on K), then $Cl(K)$ is finite.
proof It suffices to show that that the number of nonzero ideals I of O_K with $N(I) = m$ is finite, for any positive integer m. Now, if $N(I) = m$, then the additive abelian group O_K/I has order m and thus $ma \in I$ for all $a \in O_K$. In particular, I contains $m\mathbb{Z}$. but since there are only finitely many primes dividing m in the ring O_k it is clear that there are only finitely many ideals of A containing $m\mathbb{Z}$.

Embeddings [10]

Let K be Number field and $n = [K : Q]$. Since K/Q is separable and also algebraic closure of K can be found in $\mathbb{C}$ it follows that there are exactly n distinct $\mathbb{Q}$-homomorphisms of $K \to \mathbb{C}$. These homomorphisms are called the embeddings of K (in $\mathbb{C}$). If an embedding $\sigma : K \to \mathbb{C}$ is such that $\sigma(K) \subseteq \mathbb{R}$, then it is called a real embedding; otherwise it is called a complex embedding.In particular, if $\sigma : K \to \mathbb{C}$ is a complex embedding, then $\bar{\sigma} : K \to \mathbb{C}$ defined by

$$\bar{\sigma}(u) = \overline{\sigma(u)} = \text{ the complex conjugate of } \sigma(u), \quad \text{for } u \in K,$$

is an embedding of K different from σ. It follows that the number of complex embeddings of K is even. We usually denote the number of real embeddings of K by r and the number of complex embeddings of K by $2s$. We have $r + 2s = n$.

Example For $K = \mathbb{Q}(\sqrt{2})$, we have $r = 2$ and $s = 0$, since any embedding is of the form $a + b\sqrt{2} \mapsto a \pm b\sqrt{2}$. On the other hand, for $K = \mathbb{Q}(i)$, we have $r = 0$ and $s = 1$. For the cubic field $K = \mathbb{Q}(\sqrt[3]{2})$, we have $r = 1$ and $s = 1$, and the embeddings of K are essentially given by $\sqrt[3]{2} \mapsto \sqrt[3]{2}, \sqrt[3]{2} \mapsto \omega\sqrt[3]{2}$ and $\sqrt[3]{2} \mapsto \omega^2\sqrt[3]{2}$, where ω denotes a primitive cube root of unity.

Lattices

A subset L of $\mathbb{R}^n$ such that

$$L = \mathbb{Z}v_1 + \cdots + \mathbb{Z}v_n$$

some $\mathbb{R}$-basis $\{v_1, \ldots, v_n\}$ of $\mathbb{R}^n$, is called a lattice in the Euclidean space $\mathbb{R}^n$. We call the set

$$P = \{\lambda_1 v_1 + \cdots + \lambda_n v_n : 0 \leq \lambda_i < 1 \text{ for } i = 1, \ldots, n\}$$

the Fundamental parallelotope of L. Also we have $\mathbb{R}^n$ is just covered by translates of P by L i.e

$$\mathbb{R}^n = \bigsqcup_{x \in L} x + P$$

Volume

We define Volume of lattice L to be the absolute determinant of the coefficient matrix of lattice (L). Also the volume of lattice is L is denoted by vol($\mathbb{R}^n/L$)=vol(P) where P is fundamental parallelotope of L.

Recall that for any measurable subset E of $\mathbb{R}^n$, the volume of E is defined by

$$\operatorname{vol}(E) = \int_E d\mu$$

where μ denotes the Lebesgue measure on $\mathbb{R}^n$.Also note that if $E' = \lambda E := \{\lambda x : x \in E\}$, then E' is measurable and $\operatorname{vol}(E') = \lambda^n \operatorname{vol}(E)$.

Theorem: [10] L be a Lattice in $\mathbb{R}^n$, S be a Convex, measurable, symmetric subset of $\mathbb{R}^n$ such that:

$$\operatorname{vol}(S) > 2^n \operatorname{vol}(\mathbb{R}^n/L)$$

Then S contains a non zero point of L. If S is compact then $\operatorname{vol}(S) = 2^n \operatorname{vol}(\mathbb{R}^n/L)$ also works.

Let P be fundamental parallelotope of L

$$P = \{\lambda_1 v_1 + \cdots + \lambda_n v_n | \, 0 \leq \lambda_i < 1\}$$

Let E be measurable subset of $\mathbb{R}^n$

We know that:

$$\mathbb{R}^n = \bigsqcup_{x \in L} (x + P)$$

$$E \subset \mathbb{R}^n \Rightarrow \; E = \bigsqcup_{x \in L} E \cap (x + P)$$

Therefore:

$$\operatorname{vol}(E) = \sum_{x \in L} \operatorname{vol}(E \cap (x + P))$$

Observe that we translate P by x as $P + x$ and then take intersection with E

Also observe that we are doing same with E but just translation is by $(-x)$ and then intersection with

P.Therefore As a set $(E\cap(x+P))\neq(E-x)\cap P$ but since this process is exactly reverse so:

$$\text{vol}\,(E\cap(x+P))=\text{vol}((E-x)\cap P)$$

So:

$$\text{vol}(E)=\sum_{x\in E}\text{vol}\,(E\cap(x+P))=\sum_{x\in L}\text{vol}\,((E-x)\cap P)$$

Now consider $E=\dfrac{1}{2}S$

$$\text{vol}(E)=\frac{1}{2^n}\text{vol}(S)>\text{vol}\,(\mathbb{R}^n/L)=\text{vol}(P)$$

So:

$$\text{vol}(E)>\text{vol}(P)$$

If the sets $((E-x)\cap P)$ an all disjoint $\forall x\in L$ then:

$$P=\bigsqcup(E-x)\cap P\quad\forall x\in L$$

$$\text{vol}(P)\geq\sum_{x\in L}\text{vol}\,((E-x_i)\cap P)=\text{vol}(E)$$

So

$$\text{vol}(E)\leq\text{vol}(P)$$

Contradiction.

Therefore $((E-x)\cap P)$ an not all disjoint for $x\in L$

So $\exists\ a,b\in S$ and $x\neq y\in L$ such that:

$$\left(\left(\frac{1}{2}S-x\right)\cap P\right)\cap\left(\left(\frac{1}{2}S-y\right)\cap P\right)\neq\phi$$

$\exists p\in P$ such that:

$$p=\frac{1}{2}a-x,\quad p=\frac{1}{2}b-y$$

$$\frac{1}{2}a-x=\frac{1}{2}b-y\Rightarrow x-y=\frac{1}{2}a+\frac{1}{2}(-b)$$

Since the set S is convex , symmetric subset of $\mathbb{R}^n$ using that

$$x-y\in L\Rightarrow\left(\frac{1}{2}\right)a+\left(\frac{1}{2}\right)(-b)\in L\text{ and }\left(\frac{1}{2}\right)a+\left(\frac{1}{2}\right)(-b)\in S$$

So $S\cap L\neq\phi$

Now assume that $\text{vol}(S)=2^n\text{vol}(\mathbb{R}^n/L)$ and S is given to be compact.

For every $\varepsilon>0$ consider:

$$\begin{array}{rcl}\text{vol}((1+\varepsilon)S)&=&(1+\varepsilon)^n\text{vol}(S)\\&=&(1+\varepsilon)^n2^n\text{vol}(\mathbb{R}^n/L)\\&>&2^n\text{vol}(\mathbb{R}^n/L),\ \text{for all }\varepsilon>0.\end{array}$$

Therefore what we have just proved implies that, $\lambda_\varepsilon\in L\cap(1+\varepsilon)S$

In particular, if $\varepsilon < 1$, then

$$\lambda_\varepsilon \in 2S \cap L$$

. The set $2S \cap L$ is compact and discrete because

$$(2S \cap L) \subseteq L \subseteq \mathbb{R}^n$$

is discrete subset of $\mathbb{R}^n$ hence closed.
Now, $(2S \cap L) \subseteq 2S$ which implies us $2S \cap L$ is compact (Closed Subset of a Compact Set). Therefore it is finite.
Now consider the sequence λ_ε with infinitely many terms as since there is one for every $0 < \varepsilon < 1$ which belongs to intersection which is finite.
Therefore this sequence must converge to a point $\lambda \in L$ which belongs to $(1+\varepsilon)S$ for infinitely many $\varepsilon > 0$ because $(1+\varepsilon)S$ is compact hence contains all its limit points.
Thus

$$\lambda \in L \cap (\cap_{\varepsilon \to 0}(1+\varepsilon)S)$$

since S is closed we have $\lambda \in S$. Therefore $L \cap S \neq \phi$.

Theorem Let K be a number field of degree n over $\mathbb{Q}$. Let $\sigma_1, \ldots, \sigma_n$ be the real embeddings

and $\tau_1, \ldots, \tau_s, \overline{\tau}_1, \ldots, \overline{\tau}_s$ be the complex embeddings of K. Define $f : K \to \mathbb{R}^n$ by,

$$f(u) = (\sigma_1(u), \ldots, \sigma_r(u), \mathrm{Re}(\tau_1(u)), \mathrm{Im}(\tau_1(u)), \ldots, \mathrm{Re}(\tau_s(u)), \mathrm{Im}(\tau_s(u)))$$

We prove the image of O_K under f is a lattice L_K in $\mathbb{R}^n$.

It suffices to prove that if $\{\alpha_1, \ldots, \alpha_n\}$ is an integral basis for O_K, then $f(\alpha_1), \ldots, f(\alpha_n)$ is a basis for $\mathbb{R}^n$.
For this, we need to show that $n \times n$ matrix A obtained by writing out by n column vectors $\{f(\alpha_1), \ldots, f(\alpha_n)\}$ has non zero determinant in $\mathbb{R}^n$.

$$\begin{Vmatrix} \sigma_1(\alpha_1) & \cdots & \sigma_1(\alpha_n) \\ \vdots & & \vdots \\ \sigma_r(\alpha_1) & \cdots & \sigma_r(\alpha_n) \\ \mathrm{Re}(\tau_1(\alpha_1)) & \cdots & \mathrm{Re}(\tau_1(\alpha_n)) \\ \mathrm{Im}(\tau_1(\alpha_1)) & \cdots & \mathrm{Im}(\tau_1(\alpha_n)) \\ \vdots & & \vdots \\ \mathrm{Re}(\tau_s(\alpha_1)) & \cdots & \mathrm{Re}(\tau_s(\alpha_n)) \\ \mathrm{Im}(\tau_s(\alpha_1)) & \cdots & \mathrm{Im}(\tau_s(\alpha_n)) \end{Vmatrix}$$

First, we add $i\text{Im}(\tau_i(\alpha_j))$ to $\text{Re}(\tau_i(\alpha_j))$ which does not affect our determinant of A.

$$\begin{Vmatrix} \sigma_1(\alpha_1) & \cdots & \sigma_1(\alpha_n) \\ \vdots & & \vdots \\ \sigma_r(\alpha_1) & \cdots & \sigma_r(\alpha_n) \\ \tau_1(\alpha_1) & \cdots & \tau_1(\alpha_n) \\ \text{Im}(\tau_1(\alpha_1)) & \cdots & \text{Im}(\tau_1(\alpha_n)) \\ \vdots & & \vdots \\ \tau_s(\alpha_1) & \cdots & \tau_s(\alpha_n) \\ \text{Im}(\tau_s(\alpha_1)) & \cdots & \text{Im}(\tau_s(\alpha_n)) \end{Vmatrix}$$

Next, we multiply $\text{Im}(\tau_i(\alpha_j))$ by $-2i$ which gives det(A)=$(-2i)^s$det(A)

$$\begin{Vmatrix} \sigma_1(\alpha_1) & \cdots & \sigma_1(\alpha_n) \\ \vdots & & \vdots \\ \sigma_r(\alpha_1) & \cdots & \sigma_r(\alpha_n) \\ \tau_1(\alpha_1) & \cdots & \tau_1(\alpha_n) \\ -2i\text{Im}(\tau_1(\alpha_1)) & \cdots & -2i\text{Im}(\tau_1(\alpha_n)) \\ \vdots & & \vdots \\ \tau_s(\alpha_1) & \cdots & \tau_s(\alpha_n) \\ -2i\text{Im}(\tau_s(\alpha_1)) & \cdots & -2i\text{Im}(\tau_s(\alpha_n)) \end{Vmatrix}$$

Finally, we add $\tau_i(\alpha_j)$ to $-2i\text{Im}\tau_i(\alpha_j)$ and the determinant is $(-2i)^s$det(A):

$$\begin{Vmatrix} \sigma_1(\alpha_1) & \cdots & \sigma_1(\alpha_n) \\ \vdots & & \vdots \\ \sigma_r(\alpha_1) & \cdots & \sigma_r(\alpha_n) \\ \tau_1(\alpha_1) & \cdots & \tau_1(\alpha_n) \\ \bar{\tau}_1(\alpha_1)) & \cdots & \bar{\tau}_1(\alpha_n)) \\ \vdots & & \vdots \\ \tau_s(\alpha_1) & \cdots & \tau_s(\alpha_n) \\ \bar{\tau}_s(\alpha_1)) & \cdots & \bar{\tau}_s(\alpha_n)) \end{Vmatrix}$$

which equals $\pm|\Delta_K|^{\frac{1}{2}} = (-2i)^s\text{det}(A)$, where Δ_K is the discriminant of O_K.

Since $\Delta_K \neq 0$, we find that $|\text{det}(A)| = 2^{-s}|\Delta_K|^{\frac{1}{2}} \neq 0$ which implies $f(O_K)$ is a lattice.

Corollary- I be an ideal of O_K.

$$\mathrm{vol}(\mathbb{R}^n/f(I)) = \mathrm{vol}(\mathbb{R}^n/f(O_K))N(I)$$

proof- By above theorem we have

$$vol(\mathbb{R}^n/f(O_k)) = 2^{-s}\sqrt{\Delta_K}$$

Also we have $\Delta_I = N(I)^2 d_k$ Substituting the values,
$vol(\mathbb{R}^n/f(I)) = 2^{-s}\sqrt{\Delta_I}$
we get,

$$\mathrm{vol}(\mathbb{R}^n/f(I)) = 2^{-s}\sqrt{N(f(I))^2 d_K}$$

$$\mathrm{vol}(\mathbb{R}^n/f(I)) = 2^{-s}\sqrt{d_K}N(I)$$

$$\mathrm{vol}(\mathbb{R}^n/f(I)) = \mathrm{vol}(\mathbb{R}^n/f(O_K))N(I)$$

Theorem [8] Let K be a number field with discriminant δ_K.

There exists a constant $C = C_{r,s} > 0$ (which only depends on r and s) such that every ideal class (that is every coset of $Cl(K)$) contains an integral ideal whose norm is at most

$$C\sqrt{|\Delta_K|}.$$

Proof: Since I is a fractional ideal of O_K and by above $f(I)$ is a lattice in $\mathbb{R}^n$ so is $f(I^{-1})$.

So by the corollary we proved earlier gives

$$\mathrm{vol}(\mathbb{R}^n/f(I^{-1})) = \mathrm{vol}(\mathbb{R}^n/f(O_K))N(I^{-1}) = \frac{\sqrt{|\Delta_K|}}{2^s N(I)}$$

Let S be a compact, convex, symmetrical subset of $\mathbb{R}^n$ so to use Minkowiski Convex Body Theorem we have to set a scaling factor:

$$\lambda^n = 2^n \frac{\mathrm{vol}(\mathbb{R}^n/f(I^{-1}))}{\mathrm{vol}(S)}$$

Because If we consider the set λS and substituting λ^n implies

$$\mathrm{vol}(\lambda S) = \lambda^n \mathrm{vol}(S) = 2^n \mathrm{vol}(\mathbb{R}^n/f(I^{-1}))$$

$$\mathrm{vol}(\lambda S) = 2^n \mathrm{vol}(\mathbb{R}^n/f(I^{-1}))$$

So by Minkowiski Convex Body Theorem there exists $f(\alpha) \in f(I^{-1}) \cap \lambda S$. Since $\alpha \in I^{-1}$, we have that αI is an integral ideal in the same ideal class as I, and

$$N(\alpha I) = |N_{K/\mathbb{Q}}(\alpha)|N(I) = \left|\prod_{i=1}^{n} \sigma_i(\alpha)\right| N(I) \leq M\lambda^n N(I),$$

where $M = \max_{x \in S} \prod |xi|, x = (x_1, \ldots, x_n)$, so that the maximum over λS gives $\lambda^n M.$ Thus, by definition of λ^n, we have that

$$\begin{aligned}
\mathrm{N}(\alpha I) &\leq \frac{2^n \operatorname{vol}\left(\mathbb{R}^n / f\left(I^{-1}\right)\right)}{\operatorname{vol}(S)} M \, \mathrm{N}(I) \\
&= \frac{2^n M}{2^s \operatorname{vol}(S)} \sqrt{\Delta_K} \\
&= \frac{2^{r+s} M}{\underbrace{\operatorname{vol}(X)}} C \sqrt{\Delta_K}
\end{aligned}$$

Theorem The class group $Cl(K)$ is finite.

proof-By using above theorem we have every integral ideal has a bound only depends on r, s therefore given any ideal class we represent that ideal class by integral ideal and applying above theorem we have
norm is less than $C\sqrt{\Delta_K}$ and recall the equivalence relation on two ideals to be equivalent is

$$a \sim b \text{ iff } \exists \ \gamma \ \in K^*$$

$$\gamma a = b$$

applying Norm on both sides we get,
$N(\gamma a) = N(b)$ for every ideal in that coset but taking integral ideal we have

$$N(\gamma a) \leq C\sqrt{\Delta_K}$$

and by lemma we prove above below a constant m there are finitely many ideals with the norm = m hence there are only finitely many ideals in each coset therefore the ideal class group is finite.

Bibliography

[1] William Stein, Algebraic number theory a computational approach; Springer, New York,2005

[2] H. Cohen, A course in computational algebraic number theory, Springer-Verlag, Berlin, 1993. MR 94i:11105.

[3] J. W. S. Cassels and A. Frohlich (eds.), Algebraic number theory,London,Academic Press Inc. [Harcourt Brace Jovanovich Publishers], 1986, Reprint of the 1967 original

[4] Marcus, D.A., "Number Fields", Springer 1977

[5] Stewart, I., and Tall, D., "Algebraic Number Theory", Chapman and Hall 1987

[6] S. Lang, Algebraic numbers, Addison-Wesley Publishing Co., Inc., Reading, Mass.-Palo Alto-London, 1964. MR 28 3974

[7] Elementary Number Theory David M. Burton,Boston : McGraw-Hill, 2002

[8] Notes Algebraic Number Theory Mathew Baker, School of Mathematics, Georgia Institute of Technology Atlanta, 2006

[9] Keith Conrad,expository articles,Harvard University, Fall, 1996

[10] Lectures on Topics in Algebraic Number Theory (Univ. zu Kiel, Germany, Dec. 2001), Mumbai, January 2002