TIFR VSRP Programme

Project Report

Algebraic Number Theory

Milind Hegde

Under the guidance of Prof. Sandeep Varma

July 4, 2015

ACKNOWLEDGMENTS

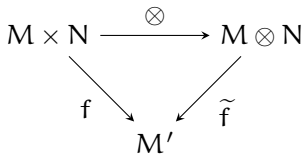
I would like to express my thanks to TIFR for selecting me to participate in the Visiting Students' Research Programme 2015, which has been a wonderful experience. I would also like to thank Prof. Sandeep Varma for being my guide during this project and teaching me many aspects of algebraic number theory, without which I would not have been able to create this report.

CONTENTS

1.1 TENSOR PRODUCTS

Definition. *(Tensor Product).* Given two modules M and N over a ring R, we can define a *tensor product* of the modules, denoted $M \otimes N$, which comes equipped with a bilinear map $\otimes : M \times N \to M \otimes N$ and satisfies the following universal property:

Given a bilinear map $f : M \times N \to M'$, there exists a unique linear map $\widetilde{f} : M \otimes N \to M'$ such that $f(m, n) = \tilde{f}(m \otimes n)$ for all $(m, n) \in M \times N$, which is to say that the following diagram commutes:



The tensor product of any two R-modules exist, and it can be constructed as a quotient of the free module with basis of all formal symbols $m \otimes n$, $(m, n) \in M \times N$ by appropriate relations.

The tensor product respects direct sums, i.e. $M' \otimes (M \oplus N) = (M' \otimes M) \oplus (M' \otimes N)$.

We must also define the tensor product of maps. Given maps $f : M \to M'$ and $g : N \to N'$, we have a map $f \otimes g : M \otimes N \to M' \otimes N'$, which we obtain as the unique map satisfying the universal property of $M \otimes N$, when applied to the bilinear map $(m, n) \mapsto f(m) \otimes g(n)$ from $M \times N$ to $M' \otimes N'$.

The tensor product is right exact, which means given a short exact sequence

$$0 \to N' \to N \to N'' \to 0,$$

we can get a new exact sequence by tensoring with a R-module M, namely

$$M \otimes N' \to M \otimes N \to M \otimes N'' \to 0.$$

The maps in the new exact sequence are the corresponding maps in the original, tensored with the identity map on M.

(Saying the tensor product is right exact is the same as saying that the tensoring of R-linear maps preserves surjectivity.)

We will use the following proposition several times:

Proposition. *Let k be a field, Ω be an extension of k, and $f \in k[X]$ a monic irreducible polynomial. Then,*

$$k[X]/(f(X)) \otimes_k \Omega \cong \Omega[X]/(f(X))$$

Proof. First we will prove that $k[X] \otimes_k \Omega \cong \Omega[X]$. Consider the following ring homomorphisms

$$g : k[X] \otimes_k \Omega \to \Omega[X], \quad p(X) \otimes \omega \mapsto \omega p(X)$$
$$h : \Omega[X] \to k[X] \otimes_k \Omega, \quad a_n X^n + \ldots + a_0 \mapsto X^n \otimes a_n + \ldots 1 \otimes a_0$$

It can be easily checked that $g \circ h$ and $h \circ g$ are identity maps on the respective rings, and so the two rings are isomorphic.

Now consider the short exact sequence below:

$$0 \to (f(X)) \to k[X] \to k[X]/(f(X)) \to 0.$$

Tensoring this with Ω, we get (using the above isomorphism)

$$(f(X)) \otimes_k \Omega \to \Omega[X] \to k[X]/(f(X)) \otimes_k \Omega \to 0.$$

Hence $k[X]/(f(X)) \otimes_k \Omega$ is isomorphic to $\Omega[X]$ quotiented by the image of $(f(X)) \otimes_k \Omega$ in $\Omega[X]$. But this can easily be seen to be $(f(X))$: any element of $(f(X))$ in $\Omega[X]$ is of the form $g(X)f(X)$ for some $g \in \Omega[X]$. Writing $g(X) = g_n X^n + \ldots + g_0$, we see that the image of $X^n f(X) \otimes g_n + \ldots + f(X) \otimes g_0 \in (f(X)) \otimes_k \Omega$ is $g(X)f(X)$. □

1.2 NORM, TRACE, AND DISCRIMINANT

Definition. *(Norm and Trace).* Suppose L/K is a finite field extension and that $\alpha \in L$. Then multiplication by α is a linear map from L to L. The determinant and trace of the map $T_\alpha : L \to L, x \mapsto \alpha x$ are well-defined, and are respectively called the norm and trace of α (and denoted $\mathrm{Nm}_{L/K}(\alpha)$ and $\mathrm{Tr}_{L/K}(\alpha)$).

From the definitions it clearly follows that the norm and trace are respectively multiplicative and additive, i.e.

$$\mathrm{Nm}(\alpha\beta) = \mathrm{Nm}(\alpha)\,\mathrm{Nm}(\beta) \quad \text{and} \quad \mathrm{Tr}(\alpha + \beta) = \mathrm{Tr}(\alpha) + \mathrm{Tr}(\beta).$$

Next we begin defining the important quantity called the discriminant, which has many formulations, depending on the context.

Definition. *(Discriminant).*

- If V is a finite dimensional vector space over a field F and $\psi : V \times V \to F$ is a bilinear form, then the discriminant of ψ, with respect to a basis $\{e_i\}$ of V, is defined as $\det(\psi(e_i, e_j))$.

  If we find the discriminant with respect to a different basis, say $\{f_i\}$, then we have that

  $$\det(\psi(f_i, f_j)) = \det(a_{ij})^2 \det(\psi(e_i, e_j)), \tag{1}$$

  where $f_j = \sum a_{ji} e_i$.

  A bilinear form for which the discriminant is non-zero with respect to some basis (and hence any basis, by (1)) is said to be non-degenerate.

- For a finite field extension L/K, the discriminant of the extension is defined as the discriminant of the bilinear form $(\alpha, \beta) \mapsto \mathrm{Tr}_{L/K}(\alpha\beta)$ (regarding L as a vector space over K). From (1), we see that this quantity is well-defined upto multiplication by the square of an element of K, i.e. it is an element of $K^\times/K^{\times^2}$.

1.3 THE RING OF INTEGERS

For an extension K of $\mathbb{Q}$, we want to find a subring of K which will play the same role as what $\mathbb{Z}$ plays with $\mathbb{Q}$. To this end, we define when an element is said to be integral.

Definition. *(Integral Elements).* Let A be a subring of a field K. Then an element $\alpha \in K$ is said to be integral over A if it satisfies a monic polynomial with coefficients in A.

First we verify that the only elements of $\mathbb{Q}$ integral over $\mathbb{Z}$ lie in $\mathbb{Z}$, to ensure that the definition is really what we want. So suppose $\frac{p}{q} \in \mathbb{Q}$ with $(p, q) = 1$ satisfies a monic polynomial with integral coefficients, say $X^n + a_{n-1}X^{n-1} + \ldots + a_1X + a_0$. Substituting and clearing the denominators, we get

$$p^n + a_{n-1}p^{n-1}q + \ldots + a_1pq^{n-1} + a_0q^n = 0$$

Now if $q \neq 1$, let π be a prime dividing q and not p. The above equation implies $\pi \mid p^n \implies \pi \mid p$, a contradiction. So $q = 1$, as required.

The observation that the set of elements of $\mathbb{Q}$ integral over $\mathbb{Z}$ equals $\mathbb{Z}$ leads us to the following definition.

Definition. *(Integrally Closed).* An integral domain A is said to be integrally closed if the set of elements of its fraction field K that are integral over A equals A itself.

The above argument directly extends to any UFD, and so we get the following proposition:

Proposition. *Any UFD is integrally closed.*

These observations lead us to suspect that the set of integral elements over an integral domain will form a ring (which agrees with our prototypical example of $\mathbb{Z}$), which we prove next.

Theorem 1. *If L is a field and $A \subset L$ is a subring (and hence an integral domain), then the set of integral elements of L over A forms a ring. This ring is denoted $\mathcal{O}_L$ and is called the ring of integers.*

The majority of the proof lies in an important lemma which will be useful later as well.

Lemma. *An element $\alpha \in L$ is integral over A if and only if there exists a finitely generated A-submodule M of L such that $\alpha M \subseteq M$.*

Proof. If α is integral, there exists a monic polynomial with coefficients in A that it satisfies, i.e. for some $a_i \in A$,

$$\alpha^n + a_{n-1}\alpha^{n-1} + \ldots + a_1\alpha + a_0 = 0$$

This implies that $M = A[\alpha]$ is finitely generated, and clearly $\alpha M \subseteq M$.

Now suppose we have a finitely generated A-submodule $M \subseteq L$ with $\alpha M \subseteq M$. Then consider the linear map

$$T_\alpha : M \to M, \quad m \mapsto \alpha m,$$

which is well-defined since $\alpha M \subseteq M$.

Let $e_1, \ldots, e_n$ be a generating set of M. Then there exist $a_{ij} \in A$ (not necessarily unique) such that

$$\alpha e_i = \sum_j a_{ij} e_j, \qquad j = 1, \ldots, n$$

Bringing the right side to the left, we get

$$\begin{aligned}
(\alpha - a_{11})e_1 - a_{12}e_2 - \ldots - a_{1n}e_n &= 0 \\
-a_{21}e_1 + (\alpha - a_{22})e_2 - \ldots - a_{2n}e_n &= 0 \\
&\vdots \\
-a_{n1}e_1 - a_{n2}e_2 - \ldots + (\alpha - a_{nn})e_n &= 0
\end{aligned}$$

Regarding this as a system of equations with coefficients in L, we see that it has a non-trivial solution, since all the $e_i \in L$ cannot be zero. Hence if the matrix of coefficients is A, we have that $\det A = 0$, which on expanding gives a monic polynomial in α with coefficients in A. □

Proof of Theorem 1. We are given α, β integral over A. By the lemma we have finitely generated A-submodules of L, M and N, such that $\alpha M \subseteq M$ and $\beta N \subseteq N$.

The submodule

$$MN = \left\{ \sum_{i=1}^{k} m_i n_i \mid m_i \in M, n_i \in N, k \in \mathbb{N} \right\}$$

is also finitely generated and it is clear that $(\alpha\beta)MN \subseteq MN$ and $(\alpha + \beta)MN \subseteq MN$, and so by the lemma we have that $\alpha + \beta$ and $\alpha\beta$ are integral over A, as required. □

Example. Here is an application of the lemma which shows its use. (Exercise 2-5 in J.S. Milne's *Algebraic Number Theory*).

Let A be a subring of a ring B, and let β be a unit in B. Show that every $\alpha \in A[\beta] \cap A[\beta^{-1}]$ is integral over A.

Let $\alpha \in A[\beta] \cap A[\beta^{-1}]$. It can be written as a polynomial in β and as a polynomial in β^{-1}, so

$$\begin{aligned}
\alpha &= \beta^n + a_{n-1}\beta^{n-1} + \ldots + a_1\beta + a_0 \\
\alpha &= \beta^{-m} + b_{m-1}\beta^{-m+1} + \ldots + b_1\beta^{-1} + b_0
\end{aligned}$$

Multiplying by β^m in the second and substituting for α from the first, we get that β is integral over A.

So the A-module $M = A[\beta^{-m}, \beta^{-m+1}, \ldots, \beta^{-1}, 1, \beta, \ldots, \beta^n]$ is finitely generated, and from the above equations, $\alpha M \subseteq M$. Thus α is integral by the lemma.

(Note that we are not given that A is an integral domain, and so we are actually using a modification of the lemma here. In its proof, the argument can be rephrased to saying that $\det(a_{ij})$ is an annihilator of M, and hence must be zero as any submodule of a field cannot have non-trivial annihilators. Here also any annihilator must be trivial as $1 \in M$, and so the conclusion of the lemma still holds.)

1.4 DEDEKIND DOMAINS

1.4.1 *Unique Factorization of Ideals*

Definition. *(Dedekind Domain)* A Dedekind domain is an integral domain with the following properties:

- It is Noetherian.
- It is integrally closed.
- Every prime ideal is maximal.

Dedekind domains are important because the above properties are precisely those needed to obtain unique factorization of ideals as products of prime ideals, which was the original motivation behind the concept of ideals. In this section we will prove this unique factorization. We will need a few preliminary lemmas.

Throughout this section, A will denote a Dedekind domain.

Lemma. *Let $\mathfrak{a} \subseteq A$ be an ideal. Then there exist $\mathfrak{p}_1, \ldots, \mathfrak{p}_n$ prime ideals such that $\mathfrak{p}_1 \cdots \mathfrak{p}_n \subseteq \mathfrak{a}$.*

Proof. Suppose the lemma is false, and consider the non-empty set of ideals which do not contain a product of prime ideals. Since A is Noetherian, this set contains a maximal element, $\mathfrak{a}$, which cannot be a prime ideal. Thus there exist $x, y \in A$ such that $x \notin \mathfrak{a}, y \notin \mathfrak{a}$ but $xy \in \mathfrak{a}$.

This implies that $\mathfrak{a} + (x)$ and $\mathfrak{a} + (y)$ are ideals which strictly contain $\mathfrak{a}$, and hence, by choice of $\mathfrak{a}$, they must each contain a product of prime ideals. But now note that

$$(\mathfrak{a} + (x))(\mathfrak{a} + (y)) \subseteq \mathfrak{a} + (xy) = \mathfrak{a},$$

implying that $\mathfrak{a}$ contains a product of prime ideals, a contradiction. □

Lemma. *Let $\mathfrak{a}, \mathfrak{b} \subseteq A$ be ideals which are coprime (i.e. $\mathfrak{a} + \mathfrak{b} = A$). Then for any $m, n \in \mathbb{N}$, $\mathfrak{a}^m$ and $\mathfrak{b}^n$ are also coprime.*

Proof. Suppose not. Then let $\mathfrak{m}$ be the maximal (and hence prime) ideal containing $\mathfrak{a}^m + \mathfrak{b}^n$. Then $\mathfrak{a}^m \subseteq \mathfrak{m} \implies \mathfrak{a} \subseteq \mathfrak{m}$ and similarly $\mathfrak{b} \subseteq \mathfrak{m}$, thus contradicting that $\mathfrak{a} + \mathfrak{b} = A$. □

Lemma. *Let $\mathfrak{m}$ be a maximal ideal in an integral domain A, and let $\mathfrak{n}$ be the ideal it generates in $A_{\mathfrak{m}} (= S^{-1}A,\ S = A \setminus \mathfrak{m})$, so that $\mathfrak{n} = \mathfrak{m}A_{\mathfrak{m}}$. Then for any $r \in \mathbb{N}$ we have an isomorphism:*

$$a + \mathfrak{m}^r \mapsto a + \mathfrak{n}^r : \ A/\mathfrak{m}^r \to A_{\mathfrak{m}}/\mathfrak{n}^r$$

Proof. First we claim that if $s \in S$, then it is a unit in $A/\mathfrak{m}^r$. Since $s \notin \mathfrak{m}$, (s) and $\mathfrak{m}$ are coprime in A. By the previous lemma, (s) and $\mathfrak{m}^r$ are also coprime, so there is a $b \in A, m \in \mathfrak{m}^r$ such that

$$bs + m = 1 \implies bs = 1 \mod \mathfrak{m}^r.$$

Thus s is a unit in $A/\mathfrak{m}^r$.

We now show that the map is injective, i.e. $\mathfrak{n}^r \cap A = \mathfrak{m}^r$. Since $\mathfrak{n}^r$ is the ideal in $A_{\mathfrak{m}}$ corresponding to $\mathfrak{m}^r$, any element $\frac{a}{s} \in \mathfrak{n}^r \cap A$ has $a \in \mathfrak{m}^r, s \in S, \frac{a}{s} \in A$. Then

$$a = s \cdot \frac{a}{s} \in \mathfrak{m}^r \implies s \cdot \frac{a}{s} = 0 \mod \mathfrak{m}^r \implies \frac{a}{s} = 0 \mod \mathfrak{m}^r,$$

since s is a unit.

Now we show surjectivity. Any element of the range can be written as $\frac{a}{s} + \mathfrak{n}^r$. Getting b as above, we get that $ab \mapsto as^{-1} + \mathfrak{n}^r$. □

Theorem 2. *In a Dedekind domain A, every non-zero ideal $\mathfrak{a}$ can be written uniquely in the form*

$$\mathfrak{a} = \mathfrak{p}_1^{r_1} \cdots \mathfrak{p}_n^{r_n}$$

for prime ideals $\mathfrak{p}_i$ and natural numbers r_i.

Proof. Given an ideal $\mathfrak{a}$, we have that it contains an ideal $\mathfrak{b}$ which is a product of prime ideals, say

$$\mathfrak{b} = \mathfrak{p}_1^{r_1} \cdots \mathfrak{p}_n^{r_n}$$

with the $\mathfrak{p}_i$ distinct. Since they are maximal, using the lemma and the Chinese remainder theorem, we get

$$A/\mathfrak{b} \cong A/\mathfrak{p}_1^{r_1} \times \cdots \times A/\mathfrak{p}_n^{r_n} \cong A_{\mathfrak{p}_1}/\mathfrak{q}_1^{r_1} \times \cdots \times A_{\mathfrak{p}_n}/\mathfrak{q}_n^{r_n}$$

where $\mathfrak{q}_i$ is the image of $\mathfrak{p}_i$ in $A_{\mathfrak{p}_i}$. Under these isomophisms, $\mathfrak{a}$ corresponds to $\mathfrak{q}_1^{s_1}/\mathfrak{q}_1^{r_1} \times \cdots \times \mathfrak{q}_n^{s_n}/\mathfrak{q}_1^{r_n}$ for some $s_i \leqslant r_i$.

This ideal is also the image of $\mathfrak{p}_1^{s_1} \times \cdots \times \mathfrak{p}_n^{s_n}$, and so

$$\mathfrak{a} = \mathfrak{p}_1^{s_1} \times \cdots \times \mathfrak{p}_n^{s_n} \text{ in } A/\mathfrak{b}.$$

Both of these ideals contain $\mathfrak{b}$, so the one-to-one correspondence between ideals of A and ideals of $A/\mathfrak{b}$ implies that we have equality of the two ideals in A itself.

To show that the factorization is unique, suppose that

$$\mathfrak{a} = \mathfrak{p}_1^{r_1} \times \cdots \times \mathfrak{p}_n^{r_n} = \mathfrak{p}_1^{s_1} \times \cdots \times \mathfrak{p}_n^{s_n}$$

(r_i's and s_i's may be zero to ensure the same set of prime ideal factors.) Suppose $r_1 > s_1$. Then looking at the equality modulo $\mathfrak{p}_1^{r_1}$ gives that the LHS is zero while the RHS is not, a contradiction. Proceeding similarly we get that $r_1 = s_i$ for all $i = 1, \ldots, n$. □

Corollary. *For any ideal $\mathfrak{a} \subset A$ and element $a \in \mathfrak{a}$, there exists an ideal $\mathfrak{a}^*$ such that $\mathfrak{a}\mathfrak{a}^* = (a)$.*

Proof. Factorize $\mathfrak{a}$ and (a) into prime ideals. If $\mathfrak{a} = \mathfrak{p}_1^{r_1} \cdots \mathfrak{p}_n^{r_n}$ and $(a) = \mathfrak{p}_1^{s_1} \cdots \mathfrak{p}_n^{s_n}$, we must have $s_i \geqslant r_i$ for each i since $(a) \subseteq \mathfrak{a}$. Define $\mathfrak{a}^* = \mathfrak{p}_1^{s_1 - r_1} \cdots \mathfrak{p}_n^{s_n - r_n}$. □

Here we state without proof the following result, which implies that the ring of integers in a number field is always a Dedekind domain. Hence we obtain the unique factorization of ideals in the ring of integers, though we do not have unique factorization of elements.

Theorem 3. *Let A be a Dedekind domain and K its field of fractions. If B is the integral closure of A in a finite extension L of K, then B is also a Dedekind domain.*

1.4.2 *Fractional Ideals and the Ideal Class Group*

We introduce special modules called fractional ideals which will play the role of multiplicative inverses to "standard" (referred to as integral) ideals, thus giving the set of fractional and integral ideals a group structure. Fractional ideals can be thought of as "ideals with a denominator":

Definition. *(Fractional Ideals).* A fractional ideal $\mathfrak{a}$ is an A-submodule of K (field of fractions of A) such that for some $d \in A$,

$$d \cdot \mathfrak{a} := \{da \mid a \in \mathfrak{a}\} \subset A.$$

Fractional ideals can be equivalently defined as finitely-generated A-submodules of K: Given a fractional ideal $\mathfrak{a}$, there is a nonzero $d \in A$ such that $d\mathfrak{a}$ is an integral ideal (follows from the definition), so $d\mathfrak{a}$ is finitely generated as an A-module. The map $x \mapsto dx : \mathfrak{a} \to d\mathfrak{a}$ is an isomorphism of modules. Conversely if $\mathfrak{a}$ is a finitely generated A-submodule of K, find the common denominator of the generators.

Multiplication of fractional ideals is the same as multiplication of modules defined earlier, i.e. the product is the set of finite sums of products of elements of the two fractional ideals. It is simple to see that this is also a fractional ideal.

We also define principal fractional ideals. If $b \in K$,

$$(b) = bA = \{ba \mid a \in A\}$$

Theorem 4. *The set of fractional ideals forms an abelian group $\mathrm{Id}(A)$ under multiplication, and in fact is freely generated by the prime ideals.*

Proof. It is simple to see that the multiplication defined is associative and commutative, and we have already observed that the set is closed under multiplication. Since it is clear that A plays the role of the identity, we need only verify the existence of inverses.

Suppose $\mathfrak{a}$ is an integral ideal and that $a \in \mathfrak{a}$. Then from the corollary above we have an integral ideal $\mathfrak{a}^*$ such that $\mathfrak{a}\mathfrak{a}^* = (a)$. Then the fractional ideal $a^{-1}\mathfrak{a}^*$ is the

inverse of $\mathfrak{a}$. If $\mathfrak{a}$ is fractional, then $d\mathfrak{a} \subset A$ has an inverse $\mathfrak{a}^*$ for some non-zero d. Then $d\mathfrak{a}^*$ is the inverse of $\mathfrak{a}$.

To verify that the group is freely generated by the prime ideals, let $\mathfrak{a}$ be a fractional ideal and $d \in A \setminus \{0\}$ be such that $d\mathfrak{a} \subseteq A$. Then let $d\mathfrak{a} = \mathfrak{p}_1^{r_1} \cdots \mathfrak{p}_n^{r_n}$ and $(d) = \mathfrak{p}_1^{s_1} \cdots \mathfrak{p}_n^{s_n}$, giving that

$$\mathfrak{a} = \mathfrak{p}_1^{r_1 - s_1} \cdots \mathfrak{p}_n^{r_n - s_n}.$$

This factorization is unique by the unique factorization of integral ideals. □

The set of principal fractional ideals $P(A)$ clearly forms a subgroup, and since the group is abelian, we can quotient by this subgroup. The resulting group is of importance:

Definition. *(Ideal Class Group).* The ideal class group of A, denoted $\mathrm{Cl}(A)$, is defined as the quotient of the group of fractional ideals by the subgroup of principal fractional ideals:

$$\mathrm{Cl}(A) = \mathrm{Id}(A)/P(A)$$

The *class number* of A is defined as the order of the class group of A.

An important theorem is to show that the class number is finite for number fields.

1.4.3 *Factorization of Primes in Extensions*

Let A be a Dedekind domain and K its field of fractions. Let B be the integral closure of A in a separable extension L of K, which we know to also be a Dedekind domain. Then prime ideals in A will factor in B:

$$\mathfrak{p}B = \mathfrak{P}^{e_1} \cdots \mathfrak{P}_n^{e_n}$$

Definition. *(Ramification and Splitting).* The prime ideal $\mathfrak{p}$ is said to *ramify* if any $e_i > 1$, with ramification index e_i. Define $f_i = f(\mathfrak{P}_i/\mathfrak{p}) = [B/\mathfrak{P}_i : A/\mathfrak{p}]$ to be the residue class degree. The prime ideal $\mathfrak{p}$ is said to *split* if each $e_i = f_i = 1$.

Theorem 5. *Let L be a finite extension of a number field K, let A be a Dedekind domain in K with field of fractions K (e.g., $A = \mathcal{O}_K$), and let B be the integral closure of A in L. Assume that B is a free A-module. Then a prime $\mathfrak{p}$ ramifies in B if and only if $\mathfrak{p} \mid \mathrm{disc}(B/A)$. In particular, only finitely many prime ideals ramify. (In fact the assumption that B is a free module is not necessary, but this requires a more general definition of the discriminant.)*

1.5 FINITENESS OF CLASS NUMBER

In this section we will prove that the class number of any number field is finite. The method of proof is significantly less algebraic, and will use the geometry of numbers. For example, Minkowski's theorem will play an important role.

We are interested in showing the class number is finite because it measures how far the ring of integers is from being a PID, and hence a UFD (in fact, all UFDs are PIDs in Dedekind domains).

Definition. *(Lattices).* A lattice Λ is a free $\mathbb{Z}$-submodule of V (an n-dimensional real vector space) with basis vectors $e_1, \ldots, e_m$ which are linearly independent over $\mathbb{R}$, i.e. are linearly independent in V.

Λ is said to be a full lattice if $m = n$.

We state the following equivalent characterizations of lattices without proof:

Lemma. *Let $\Lambda \subseteq V$ be a lattice. Since $V \cong \mathbb{R}^n$, we have a topology on V by choosing a basis (the topology is independent of choice of basis). Then the following are equivalent:*

1. *Λ is a lattice.*
2. *The subspace topology of Λ from V is the discrete topology, i.e. singletons are open.*
3. *For any bounded set $C \subseteq V$, $C \cap \Lambda$ is a finite set.*

Definition. *(Fundamental Domain)* Assume Λ is a full lattice with basis $e_1, \ldots, e_n$, i.e.

$$\Lambda = \mathbb{Z}e_1 + \ldots + \mathbb{Z}e_n$$

A fundamental domain of Λ is the set

$$D = \left\{ \lambda_0 + \sum a_i e_i \mid 0 \leqslant a_i < 1 \right\}$$

for any $\lambda_0 \in \Lambda$. Notice that choice of distinct λ_0's results in disjoint fundamental domains.

The volume of a fundamental domain is the Lebesgue measure of D in $\mathbb{R}^n$, and is equivalently equal to

$$\mu(D) = |\det(e_1, \ldots, e_n)|$$

Since the Lebesgue measure is invariant under translations, $\mu(D)$ is independent of the λ_0 chosen.

Now we use the following lemma to prove Minkowski's theorem.

Lemma. *Let Λ be a full lattice in V with a fundamental domain D. Let $S \subset V$ be a measurable set with $\mu(S) > \mu(D)$. Then there exist distinct $\alpha, \beta \in S$, such that $\alpha - \beta \in \Lambda$.*

Proof. Since Λ is a countable set, and translates of D by elements of Λ result in disjoint sets, we have the following equality:

$$\mu(S) = \sum_{\lambda \in \Lambda} \mu(S \cap D_\lambda)$$

where D_λ is a translate of D by λ. Each D_λ is measurable, so $S \cap D_\lambda$ is measurable, and also the sum is a countable sum.

For each λ, we can translate $S \cap D_\lambda$ by $-\lambda$ to get $S \cap D_\lambda \subseteq D$. But since $\mu(S) > \mu(D)$, some two of these translated sets must intersect, i.e. there exist $\alpha, \beta \in S$ such that

$$\alpha - \lambda_1 = \beta - \lambda_2 \implies \alpha - \beta \in \Lambda.$$

□

Theorem 6 (Minkowski's Theorem)**.** *Let* T *be a compact, convex set which is symmetric about the origin (i.e* $x \in T \implies -x \in T$*) with* $\mu(T) \geqslant 2^n \mu(D)$*. Then* T *contains a point of* Λ *that is not the origin.*

Proof. Note that the conditions imply that if $\alpha, \beta \in T$, then $\frac{\alpha-\beta}{2} \in T$, i.e. T contains the difference of any two points of $\frac{1}{2}T$.

First assume $\mu(T) > 2^n \mu(D) \implies \mu\left(\frac{1}{2}T\right) > \mu(D)$. Then the previous lemma with the above observation gives us the conclusion.

Now suppose $\mu(T) = 2^n \mu(D)$. Then for any $\epsilon > 0$, $\mu((1+\epsilon)T) > 2^n \mu(D)$ and so will contain a point of Λ other than the origin. From the third equivalent characterization of lattices, we have that the number of points contained will be finite because $(1+\epsilon)T$ is compact and therefore bounded.

Since T is closed, $T = \bigcap_{\epsilon>0}(1+\epsilon)T$. If T does not contain any of the finitely many points, we can pick ϵ_0 less than the distance of the nearest point from T (so $(1+\epsilon_0)T \cap \Lambda \subseteq \{0\}$), and thereby get a contradiction. □

Now we define a norm on $V \cong \mathbb{R}^r \times \mathbb{C}^s$, which is a real vector space of dimension $n = r + 2s$:

$$\|x\| = \sum_{i=1}^{r} |x_i| + 2 \sum_{i=r+1}^{r+s} |z_i|$$

where $x = (x_1, \ldots, x_r, z_{r+1}, \ldots, z_{r+s})$.

We will need the following result of the measure of a ball in V, whose calculation we omit.

Lemma. *For any real* $t > 0$*, define*

$$B(t) = \{x \in V \mid \|x\| \leqslant t\}.$$

Then,

$$\mu(B(t)) = 2^r \left(\frac{\pi}{2}\right)^s \frac{t^n}{n!}$$

Now suppose K is a number field of degree n over $\mathbb{Q}$, with r real embeddings $(\sigma_1, \ldots, \sigma_r)$ and $2s$ complex ones $(\sigma_{r+1}, \bar{\sigma}_{r+1}, \ldots, \sigma_{r+s}, \bar{\sigma}_{r+s})$, so that $n = r + 2s$. Then we have the following embedding:

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

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

Proposition. *For a nonzero ideal* $\mathfrak{a} \subseteq \mathcal{O}_K$*,* $\sigma(\mathfrak{a})$ *is a lattice of full rank in* $\mathbb{R}^n$*, with volume of a fundamental domain* $2^{-s} \cdot (\mathcal{O}_K : \mathfrak{a}) \cdot |\Delta_K|^{1/2}$*.*

Proof (Sketch). Follows from relating the determinant of the matrix with ith row

$$(\sigma_1(\alpha_i), \ldots, \sigma_r(\alpha_i), \mathrm{Re}(\sigma_{r+1}(\alpha_i)), \mathrm{Im}(\sigma_{r+1}(\alpha_i)), \mathrm{Re}(\sigma_{r+s}(\alpha_i)), \mathrm{Im}(\sigma_{r+s}(\alpha_i))$$

(which gives volume of fundamental domain) with that of the matrix $A = (\sigma_j(\alpha_i))$. Also use the fact that $\det A^2 = (\mathcal{O}_k : \mathfrak{a})^2 \cdot \Delta_K$ □

Proposition. *If $\mathfrak{a}$ is a non-zero ideal in $\mathcal{O}_K$, then $\mathfrak{a}$ contains an element α such that*

$$\mathrm{Nm}(\alpha) \leqslant \left(\frac{4}{\pi}\right)^s \cdot \frac{n!}{n^n} \cdot (\mathcal{O}_K : \mathfrak{a}) \cdot |\Delta_K|^{1/2}$$

Proof. Let $X(t)$ be the ball of radius t defined above, and let t be large enough that $X(t)$ contains a point $\sigma(\alpha)$ of $\sigma(\mathfrak{a})$, which is possible by Minkowski's theorem. For this α,

$$\begin{aligned}\mathrm{Nm}(\alpha) &= |\sigma_1\alpha| \cdots |\sigma_r\alpha||\sigma_{r+1}\alpha|^2 \cdots |\sigma_{r+s}\alpha|^2 \\ &\leqslant \left(\sum |\sigma_i\alpha| + 2\sum |\sigma_i\alpha|\right)^n / n^n \\ &\leqslant t^n/n^n\end{aligned}$$

where we have used the AM-GM inequality. Using the formula for the volume of $X(t)$, we get that we need the following inequality on t to hold:

$$t^n \geqslant n! \cdot \frac{2^n - r}{\pi^s} \cdot (\mathcal{O}_K : \mathfrak{a}) \cdot |\Delta_K|^{1/2}$$

Substituting this for t^n in the inequality above (with $\mathrm{Nm}(\alpha)$) and using that $n - r = 2s$, we get the claimed expression. □

Now we prove the important theorem, from which the finiteness of the class number will easily follow by showing that the number of ideals with index less than a fixed number is finite (which is a consequence of unique factorization into prime ideals).

Theorem 7. *Let $K/\mathbb{Q}$ be an extension of degree n, let Δ_K be its discriminant, and 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*

$$(\mathcal{O}_K : \mathfrak{a}) \leqslant \frac{n!}{n^n} \cdot \left(\frac{4}{\pi}\right)^s \cdot |\Delta_K|^{1/2} := B_K$$

Proof. Let $\mathfrak{c}$ be a fractional ideal. We have to find an integral ideal $\mathfrak{a}$ in the same coset as $\mathfrak{c}$ which satisfies the above bound.

For some $d \in K^\times$, we have that $(d) \cdot \mathfrak{c}$ is an integral ideal, say $\mathfrak{b}$. Then by the previous proposition, there exists a non-zero $\beta \in \mathfrak{b}$ with

$$\mathrm{Nm}(\beta) \leqslant B_K \cdot (\mathcal{O}_K : \mathfrak{b})$$

Since $\beta\mathcal{O}_K \subset \mathfrak{b}$, we have that there exists an integral ideal $\mathfrak{a}$ such that $\beta\mathcal{O}_K = \mathfrak{a}\mathfrak{b}$, so that $\mathfrak{a} \sim \mathfrak{b}^{-1} \sim \mathfrak{c}$. Since we have that

$$(\mathcal{O}_K : \mathfrak{a}) \cdot (\mathcal{O}_K : \mathfrak{b}) = \mathrm{Nm}(\beta) \leqslant B_K \cdot (\mathcal{O}_K : \mathfrak{b}),$$

we are done. □