NOTES ON ALGEBRAIC NUMBER THEORY: SCHOOF

ALAN ZHAO

The following notes seek to consolidate my memory of the material within [Sch03]. My goal is to write about the most critical techniques in the construction of key results in algebraic number theory. Proofs will be presented with principal focus on main ideas and motivic ideas behind constructed objects. This will be more helpful for a review of the material, as the details of the proof are already written in [Sch03], so reproducing them would not do much good.

1. Some Context

Number theory enjoys the close company of Diophantine equations. These equations, conceived hundreds of years ago, still receive the attention of a large audience of mathematicians (see for instance the many authors referenced in [Bro09]). One of the most well-known Diophantine equations is the Pythagorean equation ($X^2 + Y^2 = Z^2$) and its generalization to higher integer powers ($X^n + Y^n = Z^n$, $n \geq 3$). Equations to the former have been completely classified by Diophantus $(X, Y, Z) = (a^2 - b^2, 2ab, a^2 + b^2)$, and Wiles has proven that the latter has no solutions where $XYZ \neq 0$ (this is Fermat's Last Theorem). The proof of the former is achieved by basic considerations of the GCD, while the latter is extremely difficult (see [Wil95]). In a move of intense confidence, Fermat asserted he couldn't provide a proof for his Last Theorem because the margins in Diophantus' book were too small. Unfortunately, it does not seem to have worked, as after reading Wiles' proof, many mathematicians believed the proof would have been too complicated for Fermat to find.

We conclude this section with an illustration of the method of infinite descent. This is a method of proof that produces a contradiction of minimality by showing that an integral solution to some Diophantine equations produce a "smaller" solution.

Theorem 1.1 (Fermat)**.** *The only integral solutions of the equation*

$$X^4 + Y^4 = Z^2 \tag{1.1}$$

are those where $XYZ \neq 0$.

Proof. Suppose otherwise. Let $(X, Y, Z) = (x, y, z)$ be such a solution. Because the integers are discrete, we may assume $|z| > 0$ is minimal. If $p \mid \gcd(x, y, z)$, then $p^2 \mid z$. So, $(x/p, y/p, z/p^2)$ is a non-trivial solution which contradicts minimality. So, we know $\gcd(x, y, z) = 1$.

Remark. *GCD observations on both sides of Diophantine equations are simple but very useful, as it endows the variables with more rigid structure.*

Notice that the solution (x^2, y^2, z) provides a solution to $X^2 + Y^2 = Z^2$, and so by Diophantus has the form $(a^2 - b^2, 2ab, a^2 + b^2)$ where $a > b > 0$ and $\gcd(a, b) = 1$.

Now consider $X^2 + b^2 = a^2$, and by Diophantus we have $X = c^2 - d^2$, $b = 2cd$, and $a = c^2 + d^2$, with $c > d > 0$ and $\gcd(c, d) = 1$. By substitution into $Y^2 = 2ab$ we conclude $cd(c^2 + d^2)$ is a

Date: August 2020.

perfect square. Also, c, d, and $c^2 + d^2$ are pairwise coprime, so each is a square itself (using that $\mathbb{Z}$ is a UFD). Letting $c = U^2$, $d = V^2$, and $c^2 + d^2 = W^2$ yields a solution $(X, Y, Z) = (U, V, W)$ with $|W| < |z|$. This contradicts minimality, so we're done. □

2. Number Fields

A number field K is a finite extension of $\mathbb{Q}$. A critical result on number fields is that they are all simple extensions of $\mathbb{Q}$. We present two proofs, due to different authors.

Schoof. Let $a \in K$. The essential fact is that if f is the minimal polynomial of a over $\mathbb{Q}$, then f has no repeated roots, which we now prove. If $\deg f = 1$, we're done. Otherwise, let $a_1, \ldots, a_{n-1}$ be the other (not necessarily distinct) roots. Without loss of generality, suppose a_1 is a repeated root. Let g be the minimal polynomial of a_1. Then, since f is irreducible, $f = c \cdot g$. But f and g are monic, $c = 1$. Then, $f' | g$ but also has a_1 as a root, a contradiction of the minimal properties of g. So, f must have all distinct roots.

Now, it suffices to consider $K = \mathbb{Q}(\alpha, \beta)$. Now let $\lambda \in \mathbb{Q}^*$ and let F and G be the minimal polynomial of α and β over $\mathbb{Q}$, respectively. Then we choose a linear combination $\theta = \alpha + \lambda\beta$ with a suitable $\lambda \in \mathbb{Q}^*$. We choose λ so that $\beta \in \mathbb{Q}(\theta)$, which is equivalent to showing that $T - \beta \in \mathbb{Q}(\theta)[T]$. We know that $g \in \mathbb{Q}(\theta)[T]$ and $g(\beta) = 0$. From here, we want a way to find divisors of g are contained in $\mathbb{Q}(\theta)[T]$. We know that, given $h \in \mathbb{Q}(\theta)[T]$, we have $\gcd(g, h) \in \mathbb{Q}(\theta)[T]$ (this is the most direct way to produce such divisors). We now set out to find a polynomial h such that $\gcd(g, h) = T - \beta$.

We know $\beta = \frac{\theta - \alpha}{\lambda}$. An easy guess is then to set $h = f(\theta - \lambda T)$. From there, we know the roots of h are of the form $(\theta - \alpha_i)/\lambda$, where $f(\alpha_i) = 0$. We are certainly able to choose λ such that, for $\beta_j \neq \beta$ such that $g(\beta_j) = 0$, $(\theta - \alpha_i)/(\lambda) \neq \beta_j$. So, we're done. □

Dummit. By [DF04, Chapter 14, Section 4, Theorem 25], it remains to prove that K is separable. But $\mathbb{Q}$ is a perfect field (in particular, irreducible polynomials over $\mathbb{Q}$ have distinct roots) and so K must be separable. □

Corollary 2.0.1. *There are precisely* $[K : \mathbb{Q}]$ *embeddings* $\varphi : K \hookrightarrow \mathbb{C}$.

Proof. Let $K = \mathbb{Q}(\alpha)$. Then, φ is determined by its action on 1 and α. Because φ is a homomorphism, $\varphi(1) = 1$ always. So, $0 = \varphi(f(\alpha)) = f(\varphi(\alpha))$. So, $\varphi(\alpha)$ is a root of f, of which there are precisely n possibilities. □

The next proposition provides a necessary and sufficient condition for $\omega_1, \ldots \omega_n \in K$ to be a basis of F over $\mathbb{Q}$. We omit the proof as it is basic linear algebra.

Proposition 2.1. *Let K be a number field of degree n over $\mathbb{Q}$. Let the ω_i be as above. Then, they form a basis for K if and only if* $\det(\varphi(\omega_i))_{\varphi,i} \neq 0$.

With the basics of number fields set, we turn to a key map intrinsic to K. Let $K = \mathbb{Q}(\alpha)$ and let f be the minimal polynomial of α. Then, say f has r_1 real zeroes and r_2 non-conjugate complex zeroes. By the corollary, this means that K has r_1 embeddings into $\mathbb{R}$ and r_2 non-conjugate embeddings into $\mathbb{C}$.

We now begin with construction of the map. There is a natural map $\Phi : K \to K \otimes \mathbb{R} \simeq \mathbb{R}[T]/(f(T))$ by the inclusion $\mathbb{Q}[T]/(f(T)) \subset \mathbb{R}[T]/(f(T))$. Let $\alpha_1, \ldots, \alpha_{r_1}$ be the real roots and $\beta_1, \ldots, \beta_{r_2}$ be the non-conjugate complex roots. By the Chinese Remainder Theorem we can decompose $\mathbb{R}[T]/(f(T))$ into $\prod_{i=1}^{r_1} \mathbb{R}[T]/(T - \alpha_i)) \times \prod_{j=1}^{r_2} \mathbb{R}[T]/((T - \beta_i)(T - \overline{\beta_i})) \simeq \mathbb{R}^{r_1} \times \mathbb{C}^{r_2}$. Hence, we

obtain an explicit description of $\Phi : K \to \mathbb{R}^{r_1} \times \mathbb{C}^{r_2}$ by $x \mapsto (\varphi_1(x), \dots \varphi_{r_1}(x), \varphi_{r_1+1}(x), \dots \varphi_{r_1+r_2}(x))$ where $\varphi_i(\alpha) = \alpha_i$ and $\varphi_{r_1+i} = \beta_i$. Some basic properties that can be proven by linear algebra: (1) Φ maps a $\mathbb{Q}$-basis of K to an $\mathbb{R}$-basis of $\mathbb{R}^{r_1} \times \mathbb{C}^{r_2}$, (2) Φ is injective, and (3) $\Phi(K)$ is dense in $\mathbb{R}^{r_1} \times \mathbb{C}^{r_2}$.

We close this section with a result on cyclotomic polynomials.

Proposition 2.2. *The cyclotomic polynomial* $\Phi_m(T) := \prod_{k \in (\mathbb{Z}/m\mathbb{Z})^*} (T - e^{2\pi i k/m})$ *is irreducible in* $\mathbb{Q}[T]$.

Proof. Write $T^m - 1 = g(T)h(T)$ where g is monic, irreducible, and divides Φ_m. Gauss' Lemma shows that $g, h \in \mathbb{Z}[T]$. Let $\alpha \in \mathbb{C}$ be a zero of g. The context of cyclotomic polynomials leads us to consider α^p for $p \nmid m$. If for all α, $g(\alpha^p) = 0$, then $h(\alpha^p) = 0$ and so $g(T) \mid h(T^p)$. If we go into $\mathbb{F}_p[T]$, we see that in this ring we have $\gcd(g, h^p) \mid h^p$. Since $\gcd(g, h^p) \neq 1$, we obtain that $T^m - 1$ has a double root over $\mathbb{F}_p$, which is a contradiction.

So, $g(\alpha^p) = 0$. By prime decomposition we obtain that $g(\alpha^k) = 0$ for every k coprime to m, and so g and Φ_m have the same number of zeroes. So, we're done. □

3. Linear Algebra of Number Fields

Let $x \in K$. The action of multiplication by x on a $\mathbb{Q}$-basis for K admits a linear transformation $M_x : F \to F$, where one can view M_x as a square matrix.

Definition 3.1. *Let* $f^x_{char}(T) = \det(T \cdot I_n - M_x)$. *Define the the trace* $Tr(x)$ *and norm* $N(x)$ *by the trace of* M_x *and determinant of* M_x, *respectively. The norm is multiplicative, trace is additive.*

Remark. *The reader will notice that the roots of the characteristic polynomial are precisely the eigenvalues of* M_x. *A later result shows that the roots of the characteristic and minimal polynomial are the same, but with different multiplicity.*

It is a fact of linear algebra upon writing $f^x_{char}(T) = T^n + a_{n-1}T^{n-1} + \cdots + a_0$, we have $\det(M_x)$ is $(-1)^{[K:\mathbb{Q}]}a_0$ and $\mathrm{Tr}(M_x) = -a_{n-1}$.

Proposition 3.2. *We have the following:*

i. $f^x_{char}(T) = \prod_{\varphi : F \hookrightarrow \mathbb{C}} (T - \varphi(x))$
ii. $f^x_{char}(T) = f^x_{min}(T)^{[F:\mathbb{Q}(x)]}$
iii. $N(x) = \prod_\varphi \varphi(x)$ *and* $Tr(x) = \sum_\varphi \varphi(x)$

Proof. (iii) follows directly from (i). We now prove (i), then (ii). The proof of (i) first uses a change of basis. Write P for the matrix of Φ. Then we have that $M_x = P^{-1}AP$, where A is the matrix of the map of multiplication of $\varphi_i(x)$ on the ith coordinate. Using the identification of $\mathbb{C}$ with $\mathbb{R}^2$, we identify $\mathbb{R}^{r_1} \times \mathbb{C}^{r_2}$ with $\mathbb{R}^n$. It turns out that A is an almost-diagonal matrix consisting of matrices of the form $(\varphi_i(x))$ or the 2×2 matrix

$$\begin{pmatrix} \Re\varphi_i(x) & -\Im(\varphi_i(x)) \\ \Im(\varphi_i(x) & \Re\varphi_i(x) \end{pmatrix}. \tag{3.1}$$

As this matrix is almost diagonal, it is easy to see it has eigenvalues $\varphi_i(x)$. The characteristic polynomial of M_x doesn't depend on choice of basis, so we're done with (i).

For (ii), we consider an irreducible factor g of f^x_{char}. By (i), we know that $g(\varphi_i(x)) = 0$ for some i, and so $\varphi_i(g(x)) = 0$. Thus, $g(x) = 0$. Since g is irreducible, we know $g = f^x_{min}$. Finally, the degree of f^x_{char} is $[K : \mathbb{Q}]$ while the degree of f^x_{min} is $[\mathbb{Q}(x) : \mathbb{Q}]$. So, (ii) follows. □

Definition 3.3. *Let K be a number field of degree n and $\omega_1, \ldots, \omega_n \in K$. We define the discriminant* $\Delta(\omega_i) := \det\left(Tr(\omega_i\omega_j)_{1\le i,j\le n}\right)$.

The following proposition's proof is all standard linear algebra, so we omit it here.

Proposition 3.4. *We have the following:*

i. $\Delta(\omega_i) = \det(\varphi(\omega_i))^2_{i,\varphi}$

ii. $\Delta(\omega_i) \neq 0$ *if and only if the* ω_i *form a basis for* $K/\mathbb{Q}$.

iii. If $\omega_i' = \sum_{j=1}^n \lambda_{ij}\omega_j$ *with* $\lambda_{ij} \in \mathbb{Q}$, *then*

$$\Delta(\omega_i') = \det(\lambda_{ij})^2 \cdot \Delta(\omega_i). \tag{3.2}$$

We close this section with a discussion on the discriminant and resultant of polynomials. Let F be a field, let $b, c \in K^*$ and let $\beta_1, \ldots, \beta_r \in K$ and $\gamma_1, \ldots, \gamma_s \in K$. Put

$$g(T) = b \cdot \prod_i (T - \beta_i), h(T) = c \cdot \prod_j (T - \gamma_i). \tag{3.3}$$

Definition 3.5. *The resultant* $Res(g, h)$ *of* g *and* h *is defined by*

$$Res(g,h) = b^s c^r \prod_i \prod_j (\beta_i - \gamma_j) = (-1)^{rs} b^s c^r \left(\prod_i h(\beta_i)\right)\left(\prod_j g(\gamma_j)\right). \tag{3.4}$$

The discriminant of a polynomial with roots $\alpha_1, \ldots, \alpha_n$ is defined by

$$\mathrm{Disc}(f) = \prod_{0\le i<j\le n} (\alpha_i - \alpha_j)^2. \tag{3.5}$$

Differentiation yields the relation

$$\mathrm{Disc}(f) = (-1)^{n(n-1)/2} \cdot \mathrm{Res}(f, f'). \tag{3.6}$$

We are now in a position to establish the following proposition:

Proposition 3.6. *Let K be a number field of degree n. Let $\alpha \in K$ and let f be its characteristic polynomial. Then,*

$$\Delta(1, \alpha, \ldots, \alpha^{n-1}) = Disc(f) = (-1)^{n(n-1)/2} N(f'(\alpha)) = (-1)^{n(n-1)/2} \cdot Res(f, f'). \tag{3.7}$$

Proof. The third equality is explained directly above. The second is proved by differentiating both sides of $f(T) = \prod_j (T - \varphi_j(\alpha))$, substituting $\varphi_i(\alpha)$ for T for $i = 1, \ldots, n$, multiplying all resulting inequalities together, and applying Proposition 3.2(iii). The first is proven by using Proposition3.4(i) and the Vandermonde determinant. □

4. Rings of Integers

Definition 4.1. *Let K be a number field. An element $a \in K$ is called* ***integral*** *if there is a monic polynomial $f \in \mathbb{Z}[T]$ such that $f(a) = 0$.*

We let $\mathcal{O}_K$ denote the set of integral elements. We will now prove that this set is in fact a ring. We start with the following lemma, most critical of which are statements (i) and (iv).

Lemma 4.2. *Let K be a number field and let $a \in K$. TFAE:*

i. a is integral.

ii. The minimial polynomial f_{min} of a over $\mathbb{Q}$ is in $\mathbb{Z}[T]$.

iii. The characteristic polynomial f_{char} of a over $\mathbb{Q}$ is in $\mathbb{Z}[T]$.
iv. There exists a non-trivial finitely generated additive subgroup $M \subset K$ such that $aM \subset M$.

Proof. (i) $\implies$ (ii): Let a be integral and let $f(T) \in \mathbb{Z}[T]$ vanish at $T = a$. Then, we may factorize $f(T) = f_{min}(T)g(T)$, with all polynomials monic. By Gauss' Lemma, we conclude f_{min} is an integral polynomial.
(ii) $\implies$ (iii): Follows from Proposition 3.2(iii).
(iii) $\implies$ (iv): Let $n = \deg f_{min}$. Setting M to be the additive group generated by $1, a, \ldots, a^{n-1}$ suffices.
(iv) $\implies$ (i): Multiplication by a is a linear map M_a. Considerations of eigenstuff yield the result. □

Proposition 4.3. *The set $\mathcal{O}_K$ is a ring.*

Proof. The only hard conditions are to check that if $x, y \in \mathcal{O}_K$, that $x + y, xy \in \mathcal{O}_K$. Construct non-trivial additive groups M_x and M_y such that $xM_x \subset M_x$ and $yM_y \subset M_y$. With M_x generated by $1 = e_0, e_1, \ldots, e_m$ and M_y generated by $1 = f_0, f_1, \ldots, f_n$, let M be the additive group generated by the products $e_i f_j$ where $0 \leq i \leq m$ and $0 \leq j \leq n$. The properties of M_x and M_y tell us $x \in M_x$ and $y \in M_y$. Hence, $(x + y)M \subset M$ and $xyM \subset M$. An application of Lemma 4.2 gives the result. □

The wish that $\mathcal{O}_K = \mathbb{Z}[\alpha]$ for some $\alpha \in \mathcal{O}_K$ is unfortunately not usually true. But it is true in the case of quadratic number fields.

Proposition 4.4. *Let K be a quadratic number field. Then,*

i. $K = \mathbb{Q}(\sqrt{d})$ for a unique $d \in \mathbb{Z}$.
ii. $\mathcal{O}_K = \mathbb{Z}[\sqrt{d}]$ when $d \cong 2, 3 \pmod 4$.
iii. $\mathcal{O}_K = \mathbb{Z}\left[\frac{1+\sqrt{d}}{2}\right]$ when $d \cong 1 \pmod 4$.

Proof. Proofs of (ii) and (iii) are just algebraic manipulation and some reasoning with modular arithmetic and the GCD. It remains to prove (i).

We know that $K = \mathbb{Q}(\alpha)$ where α is some irreducible polynomial of degree 2 over $\mathbb{Q}$. By considering the quadratic formula we know that $K = \mathbb{Q}(\sqrt{d})$ where $d = \text{disc}(f)$. Uniqueness is a bit more subtle. We tie d to an intrinsic property of $\mathcal{O}_K$. Consider the set

$$\{N(a) : a \in \mathcal{O}_K, Tr(a) = 0\}. \tag{4.1}$$

The condition $Tr(a)$ allows us to isolate the possible a to numbers of the form $c\sqrt{d}$, where $c \in \mathbb{Z}$. So, the above set is equal to $\{c^2 d : c \in \mathbb{Z}\}$. Notice the above set is defined independently of d. Thus, d is determined by $\mathcal{O}_K$, and hence by K. □

The next key idea is that a $\mathbb{Z}$-basis of $\mathcal{O}_K$ is a $\mathbb{Q}$-basis of K. Furthermore, one can always find a $\mathbb{Z}$-basis of $\mathcal{O}_K$.

Proposition 4.5. *We have the following:*

i. If $\omega_1, \ldots, \omega_n \in \mathcal{O}_K$, then $\Delta(\omega_i) \in \mathbb{Z}$.
ii. Elements $\omega_1, \ldots, \omega_n \in \mathcal{O}_K$ generate $\mathcal{O}_K$ if and only if $0 \neq \Delta(\omega_i) \in \mathbb{Z}$ has minimal magnitude.
iii. There exists a generating set $\omega_1, \ldots, \omega_n$ of $\mathcal{O}_K$, making $\mathcal{O}_K \simeq \mathbb{Z}^n$. The value of $\Delta(\omega_i)$ depends only on $\mathcal{O}_K$.

Proof. (i): Recall Definition 3.3 of the discriminant. Since Proposition 4.3 tells us $\mathcal{O}_K$ is a ring, we know by looking at the constant coefficient of the characteristic polynomial of $\omega_i\omega_j$ that $\mathrm{Tr}(\omega_i\omega_j) \in \mathbb{Z}$ for $1 \leq i, j \leq n$.
(ii): For the "only if", recall the effect on the discriminant of a $GL_n(\mathbb{Z})$ transformation of the initial input (see Proposition 3.4(iii)). This is enough to conclude this direction. For the "if" part, we can proceed by contradiction, again using Proposition 3.4(iii).
(iii): We must show the natural map $\gamma : \mathbb{Z}^n \to \mathcal{O}_F$ is bijective (it is definitely a homomorphism). The fact that we have a generating set means that γ **surjects**, and Proposition 3.4(ii) allows us to conclude injectivity. Finally, the value of $\Delta(\omega_i)$ does not change because any other basis is related to $\omega_1, \ldots, \omega_n$ by an invertible change of basis matrix in $GL_n(\mathbb{Z})$, and so by Cramer's Rule must have unit determinant in $\mathbb{Z}$. □

Corollary 4.5.1. *Let K be a number field with ring of integers $\mathcal{O}_K$. Then,*

i. Every non-zero ideal $I \subset \mathcal{O}_K$ has finite index.
ii. Every ideal $I \subset \mathcal{O}_K$ is a finitely generated abelian group.
iii. Every prime ideal of $\mathcal{O}_K$ is maximal.

Proof. (i): The set $I \cap \mathbb{Z}$ is an ideal in $\mathbb{Z}$ and non-empty, and so is of the form $m\mathbb{Z}$ for some $m \neq 0$. Hence, $m\mathcal{O}_K \subset I$. The natural projection $\pi : \mathcal{O}_K/m\mathcal{O}_K \to \mathcal{O}_K/I$ is surjective, establishing the latter as a quotient of the former. It suffices to show that $\mathcal{O}_K/m\mathcal{O}_K$ is finite. But it is isomorphic to $\mathbb{Z}^n/m\mathbb{Z}^n$ which is finite.
(ii): We consider quotients again. Assume $I \neq 0$ otherwise the proof is trivial. Since $\mathcal{O}_K/m\mathcal{O}_K$ is finite, so is $I/m\mathcal{O}_K$. Then, it suffices to observe that $m\mathcal{O}_K$ is finitely generated.
(iii): This follows from (i). □

This corollary allows us to define the *norm of an ideal* by $N(I) = [\mathcal{O}_K : I] = \#(\mathcal{O}_K/I)$. The above proposition also allows us to make the definition of the *discriminant of a number field*, defined by $\Delta_K := \Delta(\omega_1, \ldots, \omega_n)$ where the ω_i are a basis for $\mathcal{O}_K$. The final proposition of this section utilizes Proposition 3.4(iii) and Proposition 3.6 to allow us to sometimes quickly deduce the structure of $\mathcal{O}_K$.

Proposition 4.6. *Let K be a number field of degree n.*

i. If there are $\omega_1, \ldots, \omega_n \in K$ such that $\Delta(\omega_i)$ is square-free, then $\mathcal{O}_K = \sum_i \omega_i\mathbb{Z}$.
ii. If there exists $\alpha \in \mathcal{O}_K$ such that $f^{\alpha}_{min}(T)$ has square-free discriminant, then $\mathcal{O}_K = \mathbb{Z}[\alpha]$ and Δ_K equals this discriminant.

5. Dedekind Rings

We zoom out for a moment to discuss some commutative algebra. The importance of this section will be seen in the next section, where we see that $\mathcal{O}_K$ is, in fact, a "Dedekind ring". The most impressive result of this section is that so-called "fractional ideals" of a Dedekind ring can be uniquely factorized into prime ideals.

Definition 5.1. *A commutative ring R is called **Noetherian** if every countable chain of ideals*

$$I_1 \subset I_2 \subset \ldots \tag{5.1}$$

stabilizes.

The key point of the next Lemma is statement (iii), which strongly resembles Zorn's Lemma.

Lemma 5.2. *Let R be a commutative ring. TFAE:*

i. Every R-ideal is finitely generated.
ii. R is Noetherian.
iii. Every non-empty collection of R-ideals contains a maximal element.

Proof. (i) $\implies$ (ii): For any chain of ideals $I_1 \subset I_2 \subset \dots$, their infinite union is also an ideal, which is finitely generated by $a_1, \dots, a_m$, say. Then, each a_i is contained in some I_k. The supremum of these k is where the chain stabilizes.
(ii) $\implies$ (iii): If not, this easily allows us to form an infinitely increasing chain of ideals.
(iii) $\implies$ (i): We want to prove that some ideal I is finitely generated. Assume $I \neq 0$ otherwise the proof is trivial. Consider the set of ideals $J \subset I$ that are finitely generated. If $J \neq I$ then we can easily form an ideal properly containing J, a contradiction. So, $J = I$ and by construction I is finitely generated. □

There is now some terminology that must be stated.

Definition 5.3. *Let $R \subset S$ be an extension of commutative rings. Then, an element $s \in S$ is said to be **integral over** R if there is a monic polynomial $f \in R[T]$ such that $f(s) = 0$. We call R **integrally closed** if every integral element in Frac(R) is contained in R.*

Definition 5.4. *Let R be a commutative ring. The height of a prime ideal $\mathfrak{p} \subset R$ is the supremum of the integers n for which there exists a chain*

$$\mathfrak{p} = \mathfrak{p}_0 \subsetneq \mathfrak{p}_1 \subsetneq \cdots \subsetneq \mathfrak{p}_n \subset R. \tag{5.2}$$

*The **Krull dimension** is the supremum of these n.*

Remark. *If every prime ideal of R is maximal, then we obviously have that R has Krull dimension 1.*

Definition 5.5. *A **Dedekind ring** is a Noetherian, integrally closed domain of Krull dimension at most 1.*

Definition 5.6. *Let K be the field of fractions of R. Then, a fractional ideal of R is an additive subgroup $I \subset K$ such that there exists $a \in K$ such that aI is a non-zero ideal of R.*

We now state a proposition without proof that follows from simple manipulation.

Proposition 5.7. *Let R be a Dedekind ring with field of fractions K. Then,*

i. Every non-zero ideal of R is fractional. A fractional ideal contained in R is an ideal of R.
ii. The set of fractional ideals is closed under set multiplication.
*iii. Fix $a \in K^*$. Then aR is a fractional ideal. These are called **principal**.*
iv. For every fractional ideal I, the set $I^{-1} = \{a \in K : aI \subset R\}$ is a fractional ideal.

The next statement is by far the most important point of this section. This proof sketch is by far the longest contained in these notes.

Theorem 5.8. *Let R be a Dedekind ring and let Id(R) be the set of fractional ideals of R. Then,*

i. The set Id(R) is an abelian group under ideal multiplication. The zero element is R and the inverse of I is I^{-1} as defined in the last proposition.

ii. We have

$$Id(R) \cong \bigoplus_{\mathfrak{p}} \mathbb{Z} \tag{5.3}$$

where $\mathfrak{p}$ *runs over the non-zero prime ideals of* R*.*

Proof. We will assume R is not a field (equivalently, has Krull dimension 1).
(i): It is easy to see that $RI = I$. The inverse element claim will be proved in (ii).
(ii): The proof has six steps.

(1) *Every non-zero ideal of* R *contains a product of non-zero prime ideals of* R*.*
This step represents progress toward the desired result. We want to consider the set of ideals Ω that violate this condition. Hence there is an ideal $I \in \Omega$ such that any $J \supsetneq I$ contains a product of non-zero prime ideals. Examining useful properties of I reveals that I is not a prime ideal, and so there exist $x, y \notin I$ such that $xy \in I$. But then $(I + (x))(I + (y)) \subset I$ contradicting the maximality of I.

(2) *For every ideal* I *with* $0 \neq I \neq R$*, one has that* $R \subsetneq I^{-1}$*.*
It suffices to prove the condition for maximal ideals. Let $\mathfrak{m}$ be a maximal ideal. Let $0 \neq a \in \mathfrak{m}$. Assuming minimality of r, we write $\prod_{i=1}^{r} \mathfrak{p}_i \subset (a)$, where the $\mathbf{p}_i$ are prime ideals. Since $\mathfrak{m}$ is prime, we assume WLOG that $\mathfrak{p}_1 \subset \mathfrak{m}$, and so $\mathfrak{p}_1 = \mathfrak{m}$. By the minimality of r we have some $b \notin (a)$ with $b \in \prod_{i=2}^{r} \mathfrak{p}_i$. Hence, $b/a \notin R$, but $b/a \in \mathfrak{m}^{-1}$ since $b\mathfrak{m} \subset (a)$.

(3) $\mathfrak{m}\mathfrak{m}^{-1} = R$ *for all maximal ideals* $\mathfrak{m} \subset R$*.*
By the above we have $\mathfrak{m} \subset \mathfrak{m}\mathfrak{m}^{-1} \subset R$, where the last inclusion follows since $\mathfrak{m}\mathfrak{m}^{-1}$ is an ideal of R. Now, suppose $\mathfrak{m} = \mathfrak{m}\mathfrak{m}^{-1}$. Then, for $x \in \mathfrak{m}^{-1}$, $x\mathfrak{m} \subset \mathfrak{m}$, and so x is integral. Since R is integrally closed, $\mathfrak{m}^{-1} \subset R$, a contradiction.

(4) $II^{-1} = R$ *for any fractional ideal* I*.*
We start with ideals of R. Let Ω denote the set of such ideals I such that $II^{-1} \neq R$. Let I be maximal with respect to this property. Of course, we have $I \subsetneq \mathfrak{m}$ for some maximal ideal $\mathfrak{m}$. Since $R \subset \mathfrak{m}^{-1}$, $I \subset I\mathfrak{m}^{-1} \subset \mathfrak{m}\mathfrak{m}^{-1} = R$. By an argument replicating the above step, we know that $I \subsetneq I\mathfrak{m}^{-1}$. Using the property of Ω, we have $(I\mathfrak{m}^{-1})(I\mathfrak{m}^{-1}))^{-1} = R$. It is easy from here to show that $II^{-1} = R$, and so Ω must be empty.

For general fractional ideals, use the fact that a fractional ideal I satisfies $I = bJ$ for $b \in K^*$ and $J \subset R$ an ideal. Then, $II^{-1} = JJ^{-1}$. So we're done.

(5) *Every fractional ideal is a product of prime ideals with integer exponents.*
Choose an ideal I of R maximal with respect to the property contrary of the above statement. Let $\mathfrak{m}$ be a maximal ideal with $I \subset \mathfrak{m} \subset R$. Following the proof of Step (iii) we reach that $I\mathfrak{m}^{-1}$ is strictly larger than I, and so is a product of prime ideals. So, every ideal of R can be written as a product of prime ideals. Since fractional ideals are of the from $\alpha^{-1}I$ for $\alpha \in R$ and $I \subset R$ an ideal. The result then follows.

(6) *This decomposition into prime ideals is unique.*
A contradiction implies a writing $\prod \mathfrak{p}^{n_\mathfrak{p}}$ with the n's non-zero. So we have a relation $I\mathfrak{p} = R$, implying $I = \mathfrak{p}^{-1}$, which is impossible by Step (ii).

□

We now give an application of the above theorem that generalizes the fact that, in $\mathbb{Z}$, if $\gcd(a, b) = 1$ and ab is an nth power, a and b are both nth powers.

Corollary 5.8.1. *Let* $I_1, \ldots, I_m$ *are non-zero ideals of* R *such that* $I_i + I_j = R$ *when* $i \neq j$*. If* $\prod_{i=1}^{m} I_i = J^n$ *for some ideal* J *of* R*, then each* I_i *is the* n*th power of another ideal of* R*.*

Proof. Decompose the I_i into prime ideals and their exponents, and multiply them all together. By the above theorem, all exponents must be divisible by n. We're now done. □

Note that the ideals of R are precisely those that have prime decomposition $\prod \mathfrak{p}^{n_\mathfrak{p}}$ with the $n's$ non-negative. The second clearly implies the first. Now suppose that an ideal $I = \prod \mathfrak{p}^{n_\mathfrak{p}}$ with at least one of the n's negative. We would obtain a relation $\mathfrak{p} = \mathfrak{p}_1\mathfrak{p}_2 \dots \mathfrak{p}_r$, which is impossible since R has Krull dimension at most 1.

6. Dedekind ζ-Function

As promised in the introduction to the last section, we prove that $\mathcal{O}_K$ is a Dedekind ring.

Proof. Krull dimension at most 1 is satisfied since all prime ideals are maximal in $\mathcal{O}_K$. It is integrally closed since $\mathrm{Frac}(\mathcal{O}_K) = K$. This can be proved just from the fact that K is algebraic over $\mathbb{Q}$. This fact may be proven by observing that for any $\alpha \in K$, the set $1, \alpha, \dots \alpha^{[K:\mathbb{Q}]}$ are linearly dependent. Hence, it remains to prove that $\mathcal{O}_K$ is Noetherian. But this follows from Lemma 5.2(i) and Corollary 4.5.1(i). □

Proposition 6.1. *Let K be a number field and let I and J be non-zero ideals of $\mathcal{O}_K$. Then, $N(IJ) = N(I)N(J)$.*

Proof. Since every ideal can be decomposed into prime ideals, it suffices to prove the result for $I = \mathfrak{p}$ and $J = \mathfrak{q}$, where both are prime ideals. The Chinese Remainder Theorem then tells us that $\mathcal{O}_K/(IJ) = \mathcal{O}_K/I \times \mathcal{O}_K/J$. This proves the result. □

Due to this result, we define the *norm of a fractional ideal* $I = JK^{-1}$ to be $N(I) = N(J)/N(K)$. We present an application of the multiplicativity of the norm.

Proposition 6.2. *Let K be a number field. Then,*

i. For every non-zero prime ideal $\mathfrak{p} \subset \mathcal{O}_K$, there is a unique rational prime p such that $(p) \mid \mathfrak{p}$.

ii. Let $\mathfrak{p}_1^{e_1} \dots \mathfrak{p}_g^{e_g}$ be the prime decomposition of (p) for p a rational prime. Then,

$$\sum_{i=1}^{g} e_i f_i = n, \tag{6.1}$$

where $N(\mathfrak{p}_i) = p^{f_i}$.

iii. For every rational prime p, there are at most n distinct prime ideals of $\mathcal{O}_K$ lying over (p).

iv. There are only finitely many ideals with bounded norm.

Proof. The fourth follows from the third. The third follows from the second. We now prove (i) and (ii).
(i): We can write $\mathfrak{p}I = (p)$. By the multiplicativity of the norm, we're done.
(ii): Follows immediately from the multiplicativity of the norm. □

We now have a lot of definitions. The f_i's are called *inertia indices* and the e_i's are called *ramificiation indices*. In §9, it will be shown that $e_i = 1$ for almost all $\mathfrak{p}_i$. The prime ideals for which $e_i > 1$ are called *ramified*. If $g = n$, we say that p is *totally split*. If $g = 1$, $f_1 = 1$, and $e_1 = n$, we say that p is *totally ramified*. If $g = 1$, $f_1 = n$, and $e_1 = 1$, we say p is *inert*.

Remark. *An alternative definition of the inertia index f_i is $[\mathcal{O}_K/\mathfrak{p}_i : \mathbb{Z}/p\mathbb{Z}]$. These definitions match since this interpretation implies that $N(\mathfrak{p}) = p^{f_i}$.*

Another application of the unique factorization presented in Theorem 5.8(ii) is an analogue of Euler's formula for the Riemann ζ-function.

Definition 6.3. *Let K be a number field. The **Dedekind ζ-function** $\zeta_K(s)$ is given by*

$$\zeta_K(s) = \sum_{I \neq 0} N(I)^{-s}. \tag{6.2}$$

The convergence of this sum is helped from two facts: (1) convergence of $\zeta(s)$ for $\Re(s) > 1$ and (2) for each rational prime p, there are a bounded number of prime ideals lying over (p).

Proposition 6.4. *Let K be a number field. Then,*

$$\zeta_K(s) = \sum_{I \neq 0} N(I)^{-s} = \prod_{\mathfrak{p}} \left(1 - N(\mathfrak{p})^{-s}\right)^{-1}. \tag{6.3}$$

where I runs over the non-zero ideals of O_K and $\mathfrak{p}$ runs over the prime ideals of O_K. Convergence occurs when $\Re(s) > 1$.

Proof. Considering partial sums we may apply the facts (1) and (2) directly preceding the statement of the proposition. Using the fact that $\sum a_i$ converges if and only if $\prod(1 + a_i)$ converges (where $a_i \geq 0$), which of course tells us that $\prod a_i$ converges. We obtain that

$$\prod_{\mathfrak{p}} \left(1 - N(\mathfrak{p})^{-s}\right)^{-1} \tag{6.4}$$

converges. The proof is finished by using unique factorization of prime ideals. We now prove that $\sum a_i$ converges if and only if $\prod(1 + a_i)$ converges. The "if" follows from the fact that the partial sums of $\sum a_i$ are dominated by the partial products of $\prod(1 + a_i)$. The "only if" follows from the fact that $a_i/(\log(1 + a_i))$ is bounded for a_i in a neighborhood of zero and since $a_i \to 0$. □

7. Finitely Generated Abelian Groups

A *free abelian group G* has a $\mathbb{Z}$-basis. It is a *free abelian group of finite rank* if this basis is finite. The cardinality of this basis is called the *rank* of G. In the following theorem, we show that the subgroups of a free abelian group G of finite rank are also free (and therefore finite).

Theorem 7.1. *Let G be a free abelian group of rank n and let $H \subset G$ be a subgroup. Then,*

i. The group H is free of rank $m \leq n$.
ii. There exists a $\mathbb{Z}$-basis $\{e_1, \ldots, e_n\}$ of G and $a_1, \ldots, a_m \in \mathbb{Z}$ such that $a_1 \mid a_2 \mid \cdots \mid a_m$ and $\{a_1 e_1, \ldots, a_m e_m\}$ is a basis for H. These a_i are determined uniquely.

Proof. We start with (i). Assume $H \neq 0$ otherwise the proof is trivial. Since $H \neq 0$, there exists a homomorphism $\varphi : G \to \mathbb{Z}$ and $h \in H$ such that $\varphi(h) > 0$ (this uses (1) the identification of G with $\mathbb{Z}^n$ and (2) the isomorphism $\mathrm{Hom}(\mathbb{Z}^n, \mathbb{Z}) \simeq \mathbb{Z}^n$.

The condition on a_1 in the statement of (i) leads us to construct integers based upon some kind of minimality condition. With homomorphisms in mind, we construct the following set:

$$\{\varphi(h) : \varphi \in \mathrm{Hom}(G, \mathbb{Z}), h \in H\} \subset \mathbb{Z}. \tag{7.1}$$

The previous paragraph tells us this set is non-empty, and it is easy to see that it is an ideal of $\mathbb{Z}$. Choose the minimal element a_1 of this set and choose a homomorphism ψ and $h \in H$ such that $\psi(h) = a_1$. By minimality arguments it is easy to show that a_1 divides $\varphi(h)$. By the identification

of the homomorphisms $G \to \mathbb{Z}$, we have that a_1 divides all coordinates of h. Define $e_1 = h/a_1 \in G$. The observation that $\psi(e_1) = 1$ allows us to conclude the following decompositions:

$$G = \mathbb{Z} \cdot e_1 \oplus \ker(\psi) \tag{7.2}$$

$$H = \mathbb{Z} \cdot a_1 e_1 \oplus (\ker(\psi) \cap H). \tag{7.3}$$

A nice induction finishes the proof of (i).

For (ii) we also use induction. For $n = 0$ it is obviously true. For $n > 0$, $\ker(\psi)$ is free by (i) and has rank $n - 1$ by the above decomposition of G. Induction tells us that there exists a basis $e_2, \ldots, e_n$ for $\ker(\psi)$ and integers $a_2 \mid \cdots \mid a_m$ such that $a_2 e_2, \ldots, a_m e_m$ is a basis for $\ker(\psi) \cap H$. It remains to show that $a_1 \mid a_2$ and the uniqueness of the a_i. For the former, assume $m > 1$, otherwise it is vacuously true. In this case, we exploit the minimality of a_1 to prove the result. Also, the construction of each a_i relies on being the smallest positive integer of some fixed set that ultimately depends on H. This proves uniqueness. □

Corollary 7.1.1. *We have the following:*

i. For any finitely generated abelian group A there exist unique integers $r \geq 0$ and $a_1, \ldots, a_t \in \mathbb{Z}_{>1}$ with $a_1 \mid \cdots \mid a_t$ such that

$$A \simeq \mathbb{Z}^r \times \left(\prod \mathbb{Z}/a_i\mathbb{Z} \right). \tag{7.4}$$

ii. If G is a free group of finite rank, then for $H \subset G$ a subgroup, we have $[G : H] < +\infty$ if and only if rank(G) = rank(H).

Proof. (i): We have an obvious surjection $\theta : \mathbb{Z}^n \to A$. We can reach an expression of the desired form by using the First Isomorphism Theorem. Apply the above theorem to $H = \ker \theta$ and $G = \mathbb{Z}^n$ to finish.
(ii): Consider the quotient G/H. It has rank rank(G) − rank(H). A group of non-zero rank has infinitely many elements. Hence, rank(G) = rank(H). □

Corollary 7.1.2. *Let $M \in \mathbb{Z}^{n \times n}$. Let $G = \mathbb{Z}^n$ and $H = M(G) \subset G$. Then,*

(1) $[G : H] < +\infty$ *if and only* $\det M \neq 0$.
(2) If $\det M \neq 0$, $[G : H] = |\det M|$.

Proof. Use the previous corollary for a near immediate proof of (i). For (ii), we observe that the index is $\prod a_i$. Let f be the linear map defined by M, and let M' be the matrix of f with respect $e_1, \ldots, e_n$. Applying the theorem, we see that M' is in fact diagonal with the ith diagonal entry being a_i. This concludes the proof. □

The next quantity introduced in the next corollary will be of importance in §9.

Corollary 7.1.3. *Let f be an integral monic irreducible polynomial. Let α denote a zero of f and let $K = \mathbb{Q}(\alpha)$. Then,*

$$disc(f) = [\mathcal{O}_F : \mathbb{Z}[\alpha]]^2 \cdot \Delta_K. \tag{7.5}$$

Proof. Let M map a $\mathbb{Z}$-basis $\omega_1, \ldots \omega_n$ of $\mathcal{O}_K$ to $1, \alpha, \ldots, \alpha^{n-1}$. Then, by Proposition 3.4(iii),

$$(\det(M))^2 \Delta_K = \Delta(1, \alpha, \ldots, \alpha^{n-1}) \tag{7.6}$$

Applying Proposition 3.6 and Corollary 7.1.2 then finishes the job. □

This final corollary is simple but useful as it unpackages information about a principal ideal to its generating element.

Corollary 7.1.4. *Let K be a number field and let $0 \neq \alpha \in O_K$. Then,*

$$N((\alpha)) = |N(\alpha)|. \tag{7.7}$$

Proof. By definition, $|N(\alpha)| = |\det(M_\alpha)|$. An application of Corollary 7.1.2 finishes the proof. □

8. Lattices

We will see in this section that O_K and its group of units are both lattices in some sense. We start with the definition of a lattice (or more specifically, a $\mathbb{Z}$-lattice.

Definition 8.1. *Let V be a vector space over $\mathbb{R}$. A subset $L \subset V$ is called a $\mathbb{Z}$-**lattice** if there exist $e_1, \dots e_n \in L$ such that*

(1) $L = \sum_i \mathbb{Z} e_i$
(2) The e_i are linearly independent.

Remark. *In this section we will use the extra condition that the e_i are actually a basis for V. But this assumption is not generally upheld in practice (see* [HB84, Lemma 1]*, for instance).*

We start with our first critical result of this section.

Proposition 8.2. *Recall the map $\Phi : K \to K \otimes \mathbb{R} = \mathbb{R}^{r_1} \times \mathbb{C}^{r_2}$. Then, $\Phi(O_K)$ is a lattice in the codomain.*

Proof. We have that Φ maps a $\mathbb{Q}$-basis of K to an $\mathbb{R}$-basis of $\mathbb{R}^{r_1} \times \mathbb{C}^{r_2}$. So, every $\mathbb{Z}$-base of O_K is mapped an $\mathbb{R}$-basis of $\mathbb{R}^{r_1} \times \mathbb{C}^{r_2}$. So, condition (ii) of Definition 8.1 is clear. Finally, because Φ is the amalgam of embeddings (in particular, homomorphisms) $\varphi_i : K \to \mathbb{C}$, we can conclude condition (i) in Definition 8.1. □

Proposition 8.3. *Let L and V be as before. TFAE:*

i. L is a lattice.
ii. L is discrete and cocompact.
iii. L generates V over $\mathbb{R}$ and for every bounded set $B \subset V$, one has that $\#(B \cap L) < +\infty$.

Proof. (i) $\implies$ (ii): L must be discrete. The projection $V \to V/L$ is continuous and $\sum_i e_i[0,1]$ maps to V/L. The former is compact, and so therefore is the latter.
(ii) $\implies$ (iii): Let W be the subspace generated by L. The natural map $V/L \to V/W$ is continuous and the former is compact, so the latter is also compact. Therefore, $W = V$. Next, if B is bounded then $B \cap L$ is bounded and closed, hence compact. A discrete topological space is compact if and only if it is finite.
(iii) $\implies$ (i): With $B = \sum_i e_i[0,1]$, we can write

$$L = \bigcup_{x \in B \cap L} (x + \sum_i e_i \mathbb{Z}) \tag{8.1}$$

where the $e_1, \dots e_n \in L$ form a basis for V. So, the index $[L : \sum_i e_i \mathbb{Z}]$ is finite and so $mL \subset \sum_{i=1^n} e_i \mathbb{Z}$ for some positive integer m. We also know that mL is free and of rank n. So, L is free of rank n. This proves the implication. □

Corollary 8.3.1. *Let K be a number field. The image of a fractional ideal I under Φ is a lattice.*

Proof. By consideration of the minimal polynomial over $\mathbb{Q}$ of $\alpha \in K^*$, there exists $n \in \mathbb{Z}_{\neq 0}$ such that nI is an ideal. Let $0 \neq m \in nI$ be an integer. Knowing that $\Phi(\mathcal{O}_K)$ is a lattice, we write:

$$\frac{m}{n}\mathcal{O}_K \subset I \subset \frac{1}{n}\mathcal{O}_K. \tag{8.2}$$

Cocompactness follows from consideration of the first inclusion. Discreteness comes from the second inclusion. □

Define the *covolume* of the lattice L as the volume of the fundmanetal domain $\sum_i e_i[0,1] \subset V$.

Proposition 8.4. *Let K be a number field of degree n. Let r_1 and r_2 be the number of real and non-conjugate complex embeddings of K.*

(1) The covolume of the lattice $\Phi(\mathcal{O}_K)$ in $K \otimes \mathbb{R}$ is given by

$$covol(\mathcal{O}_K) = 2^{-r_2}|\Delta_K|^{1/2}. \tag{8.3}$$

(2) Let I be a fractional ideal, the covolume of I in $K \otimes \mathbb{R}$ is given by

$$covol(I) = N(I)2^{-r_2}|\Delta_K|^{1/2}. \tag{8.4}$$

Proof. (i): Let $\omega_1, \ldots, \omega_n$ be a $\mathbb{Z}$-basis for $\mathcal{O}_K$. With the identification of $\mathbb{C}$ with $\mathbb{R}^2$, we obtain a matrix M for Φ. It is well-known that $|\det M|$ yields the covolume, and so computing it yields the result.
(ii): Pass from fractional ideal to ideal of $\mathcal{O}_K$ by considering mI for some $0 \neq m \in \mathbb{Z}$. Because mI has finite index in $\mathcal{O}_K$, we let A be the matrix of a linear transform such that $A(\mathcal{O}_F) = mI$. Then, $|\det A| = [\mathcal{O}_K : mI] = N(mI) = m^n N(I)$ by the theory in §7. Finally, by using the relation between determinant and covolume, we obtain the result. □

9. Discriminants and Ramification

As stated in the discussion following Proposition 4.3, it is usually not true that $\mathcal{O}_K = \mathbb{Z}[\alpha]$ for some $\alpha \in \mathcal{O}_K$. In this section we seek to gain a greater understanding of this failure via analysis of the index $[\mathcal{O}_K : \mathbb{Z}[\alpha]]$. Of course if the index is 1, there is no failure. To make the analysis more concrete, we will take α to be such that $K = \mathbb{Q}(\alpha)$. This will not be too great a restriction though, since if $\mathcal{O}_K = \mathbb{Z}[\alpha]$, then $K = \mathbb{Q}(\alpha)$. We start with the Factorization Lemma.

Theorem 9.1 (Factorization Lemma)**.** *Suppose $f \in \mathbb{Z}[T]$ is an irreducible polynomial. Let α denote a zero of f and let $K = \mathbb{Q}(\alpha)$. Let p be a rational prime not dividing $[\mathcal{O}_K : \mathbb{Z}[\alpha]]$. Suppose the polynomial f factors in $\mathbb{F}_p$ as $f(T) = \prod_{i=1}^{g} h_g(T)^{e_g}$, where the h_i are distinct and irreducible modulo p. Let $g_i \in \mathbb{Z}[T]$ be a polynomial reducing to h_i modulo p. Then, $\mathfrak{p}_i = (g_i(\alpha), p)$ is a prime ideal of $\mathcal{O}_K$ with $N(\mathfrak{p}_i) = p^{\deg h_i}$, the $\mathfrak{p}_i$ are distinct, and*

$$p\mathcal{O}_K = \prod_{i=1}^{g} \mathfrak{p}_i^{e_i}. \tag{9.1}$$

Proof. We will leave the reader to fill in some gaps in the proof. Let $d = [\mathcal{O}_K : \mathbb{Z}[\alpha]]$. We first get a handle on the problem by deducing some easy facts. First we have that

$$\mathbb{Z}[\alpha]/(g_i(\alpha), p) \simeq (\mathbb{Z}[T]/f(T))/(g_i(T), p) \simeq \mathbb{F}_p[T]/(h_i(T)) \simeq \mathbb{F}_{p^{\deg h_i}}. \tag{9.2}$$

Next, we want to prove that $\mathcal{O}_K/\mathfrak{p}_i$ is a field. By the definition of the index, we know that $d\mathcal{O}_K \subset \mathbb{Z}[\alpha]$. So a multiplication by d map $M_d : \mathcal{O}_K/\mathfrak{p}_i \to \mathbb{Z}[\alpha]/(g_i(\alpha), p)$ is considered. But of course by the previous discussion, this map is not always surjective. So, this map does not yet work to show

that $\mathcal{O}_K/\mathfrak{p}_i$ is a field. We must identify something that is able to separate $M_d(x)$ and $M_d(y)$ in the codomain for certain $x, y \in \mathcal{O}_K$.

It is important to note at this point that if we deduce some isomorphism $\mathcal{O}_K/\mathfrak{p}_i \to \mathbb{Z}[\alpha]/(g_i(\alpha), p)$, then the trickiest remaining step to be proven is that $g_i(\alpha) \notin (g_j(\alpha), p)$ for $i \neq j$. Other steps fall out naturally from consideration of the norm of the $\mathfrak{p}_i$.

We first prove the aforementioned step somewhat brazenly. If $g_i(\alpha) \cong g_j(\alpha) \pmod{p\mathcal{O}_K}$, then we can write $g_i(\alpha) = g_j(\alpha) + p\beta$ for $\beta \in \mathcal{O}_K$. Since $d\mathcal{O}_K \subset \mathbb{Z}[\alpha]$, we have $g_i(\alpha) = g_j(\alpha) + (p/d)\gamma$ for some $\gamma \in \mathbb{Z}[\alpha]$. We rewrite $\gamma = \delta(\alpha)$ so that $\gcd(dg_i(T), dg_j(T) + p\delta(T)) \neq 1$ in $\mathbb{Z}[T]$. Reducing modulo p, we would obtain that $\gcd(dh_i(T), dh_j(T)) = 1$ in $\mathbb{F}_p[T]$, contradicting the hypothesis of the Theorem since $p \nmid d$.

We now go back to rectifying the problem with M_d. We apply the fact that $\gcd(p, d) = 1$. In algebraic terms, this means we can find $a, b \in \mathbb{Z}$ such that $ap + bd = 1$. We realize that this can solve the issue of injectivity by replacing M_d with M_{bd}. To see this, choose $x, y \in \mathcal{O}_K/$ such that $x \neq y$. Then, $bd(x - y) = (1 - ap)(x - y) \cong x - y \pmod{p}$, which means that x and y reduce to the same class modulo $\mathfrak{p}_i$. Moreover, M_{bd} is also surjective! Indeed, $x = (ap + bd)x \cong bdx \pmod{p}$. It only remains to show that M_{bd} is a homomorphism, which is an easy check. Thus, we have an isomorphism, and our proof sketch is complete. □

We continue our exploration of the index $[\mathcal{O}_K : \mathbb{Z}[\alpha]]$. Digging around, we try applying it to monic Eistenstein polynomials of a prime p. Recall that this means p divides all coefficients except the leading coefficient, and p^2 doesn't divide the constant term.

Proposition 9.2. *Let p be a prime and let $f \in \mathbb{Z}[T]$ be an Eisenstein polynomial for the prime p. Let α be a zero of f and let $K = \mathbb{Q}(\alpha)$. Then, $p \nmid [\mathcal{O}_K : \mathbb{Z}[\alpha]]$.*

Remark. *The key idea behind this Proposition can be attributed to the Sylow theorems. We make this clear in the proof below.*

Proof. Write $f(T) = T^n + a_{n-1}T^{n-1} + \cdots + a_0$. Suppose $p \mid [\mathcal{O}_K : \mathbb{Z}[\alpha]]$. Then, there exists an element $x \in \mathcal{O}_K \setminus \mathbb{Z}[\alpha]$ such that $px = \sum_{i=0}^{n-1} b_i\alpha^i$ where $b_i \in \mathbb{Z}$ (this is where Sylow's First Theorem is used). Replacing α with T, write the polynomial on the right-hand side as $k(T)$. We come back to this in a moment.

We have the relation

$$-a_0 = \alpha^n + a_{n-1}\alpha^{n-1} + \cdots + a_1\alpha. \tag{9.3}$$

Note that $p \mid \alpha^n$ since every other term on both sides is divisible by p. We are close to deducing that $p\alpha$ divides a_0. If this happens, we can write $b_0 := a_0/p$, and since f is Eisenstein, $p \nmid b_0$. Hence it remains to prove $p \mid \alpha$ in $\mathcal{O}_K$, which would contradict the fact that f is Eisenstein. This is where return to the end of the first paragraph.

The polynomial $k(T)$ has the property that $k(\alpha) \in p\mathcal{O}_K$. So we consider the set I of all such polynomials (in $\mathbb{F}_p[T]$, not $\mathbb{Z}[T]$, since we are considering values modulo $p\mathcal{O}_K$). It is easy to verify that I is an ideal which contains $k(T)$. The fact that f is Eisenstein tells us that $T^n \in I$. Hence $(T^n) \subsetneq I$. If we could produce the condition $p \mid \alpha^{n-1}$, then in the above paragraph, we would have been done. Fortunately, that's exactly what we have. The condition that $(T^n) \subsetneq I$ implies that $T^{n-1} \in I$.

Remark. *To see this, induct on $n \geq 1$. Clearly, it holds for $n = 1$. Now, suppose $(T^k) \subsetneq I$. If $I = \mathbb{F}_p[T]$, we're done. Otherwise, it contains no constant polynomials and so we have $T(T^{k-1}) \subsetneq (T)I'$ for some ideal I' of $\mathbb{F}_p[T]$. It must be true then that $(T^{k-1}) \subsetneq I'$, so $T^{k-2} \in I'$, and so $T^{k-1} \in I$.*

Hence, $p \mid \alpha^{n-1}$ and we are done. □

We illustrate a powerful use of this technique in the following theorem.

Theorem 9.3. *Let $K = \mathbb{Q}(\zeta_{p^n})$ where $\zeta_{p^n} = e^{2\pi i/p^n}$. Then, $\mathcal{O}_K = \mathbb{Z}[\zeta_{p^n}]$.*

Proof. Let $q = p^n$. Then $\mathbb{Z}[\zeta_q] \subset \mathcal{O}_K$. Then, $\mathrm{disc}(\Phi_q)$ is a power of p. So, if $[\mathcal{O}_K : \mathbb{Z}[\zeta_q]] \neq 1$, then $p \mid [\mathcal{O}_K : \mathbb{Z}[\zeta_q]$ by Corollary 7.1.3. Then,

$$\Phi_q(T) = \sum_{i=1}^{p-1} T^{(p-i)p^{n-1}}. \tag{9.4}$$

After some computation we see that $\Phi_q(T+1)$ is an Eisenstein polynomial for p, and the by the Proposition, we're done. □

We state the last two results without proof. The proof of the first result uses Sylow's first theorem and some motivated ideals as was used in the proof of Proposition 9.3. The proof of the second is better reserved for a course on commutative algebra.

Theorem 9.4 (Dedekind's Criterion)**.** *Suppose α is an algebraic integer with minimum polynomial $f \in \mathbb{Z}[T]$ over $\mathbb{Q}$. Let $K = \mathbb{Q}(\alpha)$. For p a rational prime, let $\overline{f} = \prod_{i=1}^{g} \overline{f_i}^{e_i}$ be the decomposition of f in $\mathbb{F}_p[T]$ into distinct irreducible polynomials modulo p. Then, $p \mid [\mathcal{O}_K : \mathbb{Z}[\alpha]]$ if and only if there exists an index j such that $e_j \geq 2$ and*

$$\left(\frac{\overline{f}(T) - \prod_i \overline{f_i}(T)^{e_i}}{p} \right) \subset (\overline{f_j}) \tag{9.5}$$

where the ideals are understood to be in $\mathbb{F}_p[T]$.

Theorem 9.5 (Dedekind, 1920)**.** *Let K be a number field and p a rational prime. Then, p is ramified in K if and only if $p \mid \Delta_K$.*

10. Minkowski's Theorem

The most important finiteness results of algebraic number theory will be introduced in this section. In particular, we prove that the class group is finite. We begin with an account of Minkowski's "Geometry of Numbers".

Theorem 10.1 (Minkowski's Convex Body Theorem)**.** *Let $V = \mathbb{R}^n$ be a real vector space and $L \subset V$ a lattice. Let X be a bounded, convex, symmetric subset of V. If $vol(X) > 2^n covol(L)$, then there exists a non-zero vector $\lambda \in L \cap X$.*

Proof. It is easy to see that $\mathrm{vol}(X) > \mathrm{vol}(V/2L)$. So, the projection $X \to V/2L$ cannot be injective. This follows by a Pigeonhole Principle style argument. Let $e_1, \ldots e_n$ be a basis for L and let

$$\mathcal{S} = \{ \sum_i [a_i, a_i + 1] e_i : a_i \in \mathbb{Z} \}. \tag{10.1}$$

Then, we clearly have the following (finite) sum:

$$\sum_{S \in \mathcal{S}} \mathrm{vol}(S \cap X) = \mathrm{vol}(X) > \mathrm{vol}(V/2L). \tag{10.2}$$

Injectivity would hence be absurd as the projection $S \cap X \to V/2L$ is measure-preserving. So, there are two points $x_1 \neq x_2 \in X$ which have the same image in $V/2L$. The proof is finished by an

appeal to symmetry and then to convexity using the fact that $1/2 + 1/2 = 1$ (this is why there is an exponent of 2 in the statement of the theorem!). □

The next lemma introduces the volume of a strange region, but makes sense upon consideration of the AM-GM inequality used in the proof of the next theorem.

Lemma 10.2. *Let K be a number field of degree n and let r_1 and r_2 be the usual parameters. For $R \geq 0$, set*

$$W(r_1, r_2, R) = \{(x_1, \dots, x_{r_1}, y_1, \dots y_{r_2} : |x_1| + |x_{r_1}| + 2|y_1| + \cdots + 2|y_{r_2}| \leq R\}. \tag{10.3}$$

Then,

$$vol(W(r_1, r_2, R)) = 2^{r_1} \left(\frac{\pi}{2}\right)^{r_2} \frac{R^n}{n!}. \tag{10.4}$$

Theorem 10.3 (Minkowski)**.** *Let K be a number field with r_1 real embeddings and $2r_2$ complex ones. Then, every non-zero ideal I of $\mathcal{O}_K$ contains an element x with*

$$|N(x)| \leq \frac{n!}{n^n} \left(\frac{4}{\pi}\right)^{r_2} |\Delta_K|^{1/2} N(I). \tag{10.5}$$

Proof. Let $X(R)$ be the set introduced in the previous lemma. It is bounded, convex, symmetric, and closed. An application of Minkowski's Convex Body Theorem followed by applying AM-GM concludes the proof. □

The key statement of the following corollary is statement (iv).

Corollary 10.3.1. *Let K be a number field of degree n.*

(1) We have

$$|\Delta_K| \geq \left(\frac{n^n}{n!} \left(\frac{\pi}{4}\right)^{r_2}\right)^2. \tag{10.6}$$

(2) We have $|\Delta_K| > 1$ for $K \neq \mathbb{Q}$.

(3) Every ideal class contains an ideal I with

$$|N(I)| \leq \frac{n!}{n^n} \left(\frac{4}{\pi}\right)^{r_2} |\Delta_K|^{1/2}. \tag{10.7}$$

(4) The class group of $\mathcal{O}_K$ is finite.

Proof.

Remark. *The theme here is to combine finiteness results. For that, one naturally tries to utilize Proposition 6.2(iii,iv).*

(i): By Theorem 5.8(ii), we can combine the fact that $(x) \subset I$ (where x and I are as in the above theorem) with Proposition 6.1 to conclude that $|N((x))| = |N(x)| \leq N(I)$. A little algebraic manipulation yields the desired statement.
(ii): Follows from (i) and consideration of the lower bound of $n^n/n!$.
(iii): Every ideal class contains an integral ideal.
(iv): Apply Proposition 6.2(iv) and (iii). □

Remark. *We can use Stirling's formula for large n to obtain a stricter lower bound.*

We conclude this section with a result of Hermite.

Corollary 10.3.2. *For any integer Δ, there are only finitely number field K, up to isomorphism, with $|\Delta_K| = \Delta$.*

Proof. Corollary 10.3.1(ii) tells us we can assume K has fixed degree. Then, with consideration of the lattice structure of $\mathcal{O}_K$ in $K \otimes \mathbb{R}$ and Minkowski's Convex Body Theorem, we claim that there exists an element $\alpha \in \mathcal{O}_K$ such that $K = \mathbb{Q}(\alpha)$ and $|\varphi_i(\alpha)| < 1 + \sqrt{\Delta}$ for all embeddings $\varphi : F \to \mathbb{C}$.

It is natural then to consider the box

$$B = \{(x_1, \dots, x_{r_1+r_2}) : |x_1| < 1 + \sqrt{\Delta}, |x_i| < 1 \text{ for } i \neq 1\} \tag{10.8}$$

since it has volume $2^{r_1}\pi^{r_2}(1 + \sqrt{\Delta})^{\kappa} > 2^n \text{covol}(\mathcal{O}_K)$ since $\kappa = 1$ if $r_1 > 0$ and $\kappa = 2$ if $r_1 = 0$. Thus, we obtain an $\Phi(\alpha) \in B \cap \Phi(\mathcal{O}_K)$ by Minkowski's Convex Body Theorem. Because the characteristic polynomial of α is an integral polynomial that is a power of the (irreducible) minimal polynomial for α, then $|\varphi_1(\alpha)| > 1$ while $|\varphi_i(\alpha)| < 1$ for all other $i \neq 1$. So, f^{α}_{char} has a root of multiplicity 1, and by Proposition 3.2(ii), $K = \mathbb{Q}(\alpha)$. This proves the claim.

To finish, we consider how many possible f there can be. If α is as in the claim, then the $\varphi_i(\alpha)$ are bounded in size by $1 + \sqrt{\Delta}$. Because the coefficients of the minimal polynomial of f (which is also the characteristic polynomial) are elementary symmetric polynomials in the $\varphi_i(\alpha)$, there is a constant $b(n, \Delta)$ such that the coefficients a_j of f have $|a_j| \leq b(n, \Delta)$. Since the a_j are integers, this finishes the proof. □

11. Dirichlet's Unit Theorem

We introduce modified absolute values on $\mathbb{R}$ and $\mathbb{C}$: $\|x\| = |x|$ if $x \in \mathbb{R}$ and $\|x\| = |x|^2$ if $x \in \mathbb{C} \setminus \mathbb{R}$.

Definition 11.1. *Let K be a number field of degree n with r_1 real embeddings and $2r_2$ complex embeddings. Let the homomorphism $\Psi : \mathcal{O}_K^* \to \mathbb{R}^{r_1+r_2}$ given by*

$$\Psi(\epsilon) = (\log \|\varphi_1(\epsilon)\|, \dots \log \|\varphi_{r_1+r_2}(\epsilon)\|). \tag{11.1}$$

with the standard chosen embeddings (first the real ones, then non-conjugate complex ones).

The structure for the remainder of this section is as follows: we will introduce two auxilliary lemmas to supplement the main theorem of Dirichlet. As a corollary, we shall deduce Dirichlet's Unit Theorem. We will then conclude with a discussion on the regulator of a number field.

Lemma 11.2. *Let K be a number field of degree n. Let $\varphi_1, \dots \varphi_{r_1}$ be the real embeddings of K and let $\varphi_{r_1+1}, \dots, \varphi_{r_1+r_2}$ be a set of non-conjugate complex embeddings of K. For each index $1 \leq i \leq r_1 + r_2$, there exists a sequence $\{\alpha_i\}$ of non-zero $\mathcal{O}_K$ elements such that $|N(\alpha_j)| \leq |\Delta_K|^{1/2} + 1$ and*

$$\|\varphi_j(\alpha_1)\| > \|\varphi_j(\alpha_2)\| \dots \tag{11.2}$$

for all $j \neq i$.

Proof. We normalize α_1 to 1. We now proceed inductively. Suppose $\alpha_1, \dots, \alpha_m$ have been defined satisfying the inequalities in the theorem. As with other Geometry of Numbers proofs, we construct a box. And we want it to have volume exceeding $2^n \text{covol}(\mathcal{O}_K) = 2^{r_1+r_2}|\Delta_K|^{1/2} < 2^{r_1}\pi^{r_2}|\Delta_K|^{1/2}$. We don't need control over i, so we will control $\|\varphi_j\|$ for $j \neq i$. In this vain, let $\beta_j = \frac{1}{2}\|\varphi_j(\alpha_m)\|$ and β_i be defined by $\prod_k \beta_k = |\Delta_K|^{1/2} + 1$.

Now consider the box

$$B = \{(x_1, \dots, x_{r_1+r_2} : \|x_k\| \leq \beta_k\}. \tag{11.3}$$

It has volume exceeding $2^n \mathrm{covol}(\mathcal{O}_K)$. So, by Minkowski's Convex Body Theorem, we obtain a non-zero element in $B \cap \Phi(\mathcal{O}_K$, which we write as α_{m+1}, because it actually works! □

We omit the proof of the following lemma as it is elementary linear algebra.

Lemma 11.3. *Let $(a_{ij})_{i,j}$ be a real $m \times m$ matrix. Suppose that $a_{ij} < 0$ when $i \neq j$ and $\sum_j a_{ij} > 0$ for all i. Then, $(a_i j)_{i,j}$ has rank m.*

As promised, we now go over Dirichlet's theorem (with proof).

Theorem 11.4. *Recall the definition of Ψ at the beginning of this section. Then,*

i. The kernel of Ψ is finite and equal to μ_K, the group of the roots of unity of K.

ii. $\Psi(\mathcal{O}_K)$ is a lattice in the space

$$H = \{(x_1, \ldots, x_{r_1+r_2}) \in \mathbb{R}^{r_1+r_2} : \sum x_i = 0\} \tag{11.4}$$

which is of codimension 1 in $\mathbb{R}^{r_1+r_2}$.

Proof. It is easy to show that $\mu_K \subset \ker(\Psi)$. For the opposite inclusion, we prove that Ψ has finite kernel. This is enough to show that $\ker(\Psi) = \mu_K$. We now investigate properties of an element $\epsilon \in \ker(\Psi)$.

Obviously, one has $\|\varphi(\epsilon)\| = 1$ for all embeddings $\varphi : K \to \mathbb{C}$. Not for a second forgetting the geometry of the situation and combining it with the above control on φ, we conclude that $\Phi(\ker(\Psi)) \subset B = \{(x_1, \ldots, x_{r_1}, y_1, \ldots, y_{r_2}) : |x_i|, |y_i| \leq 1\}$, which of course has bounded volume. Trivially, $\Phi(\ker(\Psi)) \subset B \cap \Phi(\mathcal{O}_K)$, the right side of which by Proposition 8.2 is finite. Since Φ is injective, we're done with (i).

Moving to (ii), we start with the fact that a unit $\epsilon \in \mathcal{O}_K^*$ has $N(\epsilon) = \pm 1$. So,

$$1 = N(\epsilon) = \prod_{i=1}^{r_1+r_2} \|\varphi_i(\epsilon)\| \tag{11.5}$$

and this implies that $\mathrm{im}(\Psi) \subset H$.

We next prove that $\Psi(\mathcal{O}_K^*)$ is discrete. Again, we exploit the lattice structure of $\Phi(\mathcal{O}_K)$. It is an easy exercise to check that if for any bounded set B we have $\Psi(\mathcal{O}_K^*) \cap B$ is finite, then $\Psi(\mathcal{O}_K^*)$ is discrete. Let $B' = \{(x_1, \ldots, x_{r_1+r_2}) \in \mathbb{R}^{r_1+r_2} : |x_i| \leq R\}$ with R so large such that $B \subset B'$. An element $\epsilon \in \mathcal{O}_K^*$ that is mapped into B' is also mapped by Φ to a bounded box in $K \otimes \mathbb{R}$. That concludes this step. We have now shown that $\Psi(\mathcal{O}_K^*)$ is a lattice in $\mathbb{R}^{r_1+r_2}$.

It remains to show that $\Psi(\mathcal{O}_K^*)$ spans H. The question then, is how we produce a basis for $\Psi(\mathcal{O}_K^*)$. We target numbers of the form $\log \|\varphi_j(\epsilon_i)\|$, as this has the form of Ψ. Using Lemma 11.2 we can find units ϵ_i such that $\|\varphi_j(\epsilon_i)\| < 1$ for $j \neq i$. Noting that the condition in Lemma 11.3 can easily be replaced with $\sum_j a_{ij} < 0$. So, any $(r_1 + r_2 - 1) \times (r_1 + r_2 - 1)$ minor of the matrix $(a_{ij})_{i,j}$ with $a_{ij} = \log \|\varphi_j(\epsilon_i)\|$. Therefore, the rank of (a_{ij}) is $r_1 + r_2 - 1$, so we're done. □

Dirichlet's Unit Theorem is then an easy corollary.

Corollary 11.4.1. *Let K, r_1 and r_2 be as usual. Then, there exist a set of **fundamental units** $\epsilon_1, \ldots \epsilon_{r_1+r_2-1}$ such that*

$$\mathcal{O}_K^* = \{\zeta \prod_{k=1}^{r_1+r_2-1} \epsilon_k^{n_k} : \zeta \in \mu_K, n_k \in \mathbb{Z}\}. \tag{11.6}$$

We now define the regulator.

Definition 11.5. *Let K be a number field of degree n and let $\varphi_1, \ldots, \varphi_{r_1+r_2}$ be the homomorphisms used in the map Φ. The* ***regulator*** *R_K of K is defined to be*

$$R_K = \left|\det(\log \|\varphi_j(\epsilon_i)\|)_{i,j}\right| \tag{11.7}$$

where j skips any φ_k.

Proposition 11.6. *The covolume of $\Psi(\mathcal{O}_K^*)$ in H (as defined in Theorem 11.4(ii)) equals $\sqrt{r_1 + r_2} \cdot R_K$.*

Proof. Consider the vector $\xi = (r_1 + r_2)^{1/2}(1, \ldots, 1) \in \mathbb{R}^{r_1+r_2}$, which is unit. We then use the interpretation of covolume as the determinant of a linear transform and use the fact that $\sum_{i=1}^{r_1+r_2} \log \|\varphi_i(\epsilon_k)\| = 0$, which shows it doesn't matter what row is deleted in the definition of R_K. An expansion by minors yields the result. □

12. The Class Number Formula

Recall the definition of the Dedekind ζ-function with respect to K:

$$\zeta_K(s) = \sum_{I \neq 0} N(I)^{-s}. \tag{12.1}$$

In this section we generalize the fact that $\zeta_{\mathbb{Q}}$ has a simple pole at $s = 1$ with residue 1 with a proof of the following theorem, the proof of which relies on lemmas to be introduced afterward:

Theorem 12.1 (Class Number Formula)**.** *The K be a number field and let $\zeta_K(s)$ be defined as above. Then,*

$$\lim_{s \to 1} \zeta_K(s) = \frac{2^{r_1}(2\pi)^{r_2} h_K R_K}{w_K |\Delta_K|^{1/2}}, \tag{12.2}$$

where r_1, r_2, R_K, and Δ_K are as in previous sections, h_K is the class number of K, and w_K is the number of roots of unity in K.

Proof. We split the infinite sum $\zeta_K(s)$ into sums over ideal classes:

$$\zeta_K(s) = \sum_{C \in \mathrm{Cl}(O_K)} \sum_{J \in C} N(J)^{-s}. \tag{12.3}$$

Because we are working over ideal classes, $JI = (\alpha)$ for some fixed ideal $I \in C^{-1}$ and $\alpha \in K$. Then, $(\alpha) \subset I$. Hence,

$$\sum_{J \in C} N(J)^{-s} = N(I)^s \sum_{(\alpha) \subset I} |N(\alpha)|^{-s}. \tag{12.4}$$

With the sum controlled in terms of an ideal I, we may descend into $K \otimes \mathbb{R}$ and utilize theorems from the Geometry of Numbers developed in previous sections. Extend Ψ from $\mathcal{O}_K^*$ to $K \otimes \mathbb{R}$ in the natural way, and using Proposition 3.2(iii) we extend the norm $N : K \to \mathbb{R}$ to $K \otimes \mathbb{R}$ via

$$N(x_1, \ldots, x_{r_1}, z_1, \ldots z_{r_2}) = |x_1| \ldots |x_{r_1}| \cdot |z_1|^2 \ldots |z_{r_2}|^2. \tag{12.5}$$

The norm is homogeneous, as it should be.

Continuing in the style of the Geometry of Numbers, choose a basis $E = \{\Psi(\epsilon_i)\}_{i=1}^{r_1+r_2-1} \cup \{\mathbf{v}\}$ where $\mathbf{v}$ has its first r_1 entries equal to 1 and the rest equal to 2. The reason for this choice of $\mathbf{v}$ will become apparent in later lemmas.

Consider the subset $\Gamma \subset K \otimes \mathbb{R}$ consisting of $\mathbf{x} \in K \otimes \mathbb{R}$ such that the coordinates ξ_i of $\Psi(\mathbf{x})$ with respect to the basis E satisfy $0 \leq \xi_i < 1$ for $1 \leq i \leq r_1 + r_2 - 1$ and such that the first coordinate x_1 of $\mathbf{x}$ satisfies $0 \leq \arg(x_1) < 2\pi/w_F$. Using Lemma 12.2, we can decompose the inner sum of

Equation 12.4. It is easy to verify that Γ is a cone and doesn't contain $\mathbf{0}$. Since we also have that $\Gamma_1 = \{\gamma \in \Gamma : |N(\gamma)| \leq 1\}$ is bounded, we may apply Lemmas 12.3 and 12.4 to get the result. □

Lemma 12.2. *Let K be a number field and let Γ be as defined in the proof of the Theorem. For a fractional ideal I of K we then have that*

$$\sum_{(\alpha)\subset I} |N(\alpha)|^{-s} = \sum_{\alpha \in I \cap \Gamma} |N(\alpha)|^{-s}. \tag{12.6}$$

Proof. The reason for the choice of Γ is that we can write $\mathbf{x} \in (K \otimes \mathbb{R})^*$ as $\mathbf{x} = \epsilon \cdot \gamma$ where $\epsilon \in O_K^*$ and $\gamma \in \Gamma$. We first note that given any $\mathbf{x}$, we can choose ϵ such that $\Psi(\epsilon^{-1}\mathbf{x})$ has its first $r_1 + r_2 - 1$ coordinates with respect to E in the interval $[0, 1)$. This follows from Dirichlet's Unit Theorem. Furthermore, we can do this uniquely.

Showing that this representation exists is just a matter of choosing a correct root of unity. Uniqueness is a bit more complicated. Suppose that $\epsilon\gamma = \epsilon'\gamma'$. Of course, this implies $\epsilon \neq \epsilon'$. If ϵ/ϵ' is contained in the free part of O_K^*, then $\epsilon/\epsilon' \notin \Gamma$, a contradiction. So, ϵ and ϵ' differ in their torsion. So, $\epsilon/\epsilon' \in \ker(\Psi)$. Then, since the first arguments of γ and γ' are contained in $[0, 2\pi/w_K)$, we conclude that $\epsilon = \epsilon'$.

With this, the lemma follows from the fact that for any $(\alpha) \subset I$, $N(\alpha) = N(\Phi(\alpha))$. Since $\Phi(\alpha)$ then has the unique decomposition as above and since $|N(\epsilon)| = 1$, the result follows. □

Lemma 12.3. *Let L be a lattice in $\mathbb{R}^n$ and let $\Gamma \subset \mathbb{R}^n$ be a cone. Let N be a homogeneous polynomial of degree n not vanishing on Γ. Let $\Gamma_1 = \{\gamma \in \Gamma : |N(\gamma)| \leq 1\}$ and assume it is bounded with finite volume. Then,*

$$\lim_{s\to 1}(s-1)\sum_{x \in L\cap\Gamma} |N(x)|^{-s} = \frac{vol(\Gamma_1)}{covol(L)}. \tag{12.7}$$

Proof. We tacitly utilize measure theory here to deduce that we can find a covering of Γ_1 by a countable almost disjoint union of parallelotopes of the shape (possibly scaled down) of the fundamental domain of L. The proof of [SS09, Chapter 1, Theorem 1.4] can be adapted in our case to produce such a covering (given more technical measure theoretic results). Set $\nu(r) = \#\left(\frac{1}{r}L \cap \Gamma_1\right) = \#\{x \in L : |N(x)| \leq r^n\}$. Let $n(r)$ be the number of fundamental domains of $\frac{1}{r}L$ strictly contained inside Γ_1. Then by Stein and Shakarchi's construction,

$$\mathrm{vol}(\Gamma_1) = \lim_{r\to\infty} n(r)\mathrm{covol}\left(\frac{1}{r}L\right) = \lim_{r\to\infty} \nu(r)\mathrm{covol}\left(\frac{1}{r}L\right). \tag{12.8}$$

Equivalently,

$$\lim_{r\to\infty} \frac{\nu(r)}{r^n} = \frac{\mathrm{vol}(\Gamma_1)}{\mathrm{covol}(L)}. \tag{12.9}$$

The desired final form of the equation is in sight. For ease of notation we enumerate the vectors in $\Gamma \cap L$ and sum them in that order. We also sort them so that

$$0 < |N(\mathbf{x}_1)| \leq |N(\mathbf{x}_2)| \leq \dots. \tag{12.10}$$

Multiplication applications of the squeeze principle suffice to carry this proof to its end. It starts by noting that, by setting $r_k = |N(\mathbf{x}_k)|^{1/n}$, we actually have that $k \leq \nu(r_k)$ and that $\nu(r_k - \epsilon) \leq k - 1 < k$ for any $\epsilon > 0$. □

Lemma 12.4. *Let K be a number field and let Γ be the cone defined in the Theorem. Then,*

$$vol(\Gamma_1) = \frac{2^{r_1}\pi^{r_2}R_K}{w_K}. \tag{12.11}$$

Proof. In the definition of Γ_1, if we drop the condition on the first coordinate ($0 \leq \arg(x_1) < 2\pi/w_K$), then $\mathrm{vol}(\Gamma_1)$ is increased by a factor of w_F. If we require the real coordinates to be positive, we cut the volume by a factor of 2^{r_1}. The remainder of the proof is standard calculus: introducing a volume integral, and then using change of variable to shift to integration by the ξ_i. The Jacobian of this transformation has determinant which produces the factor of R_K in the lemma. Identifying $\mathbb{C}$ with $\mathbb{R}^2$ produces the factor of π^{r_2}. □

References

[Bro09] Timothy D Browning, *Quantitative arithmetic of projective varieties*, vol. 277, Springer Science & Business Media, 2009.

[DF04] David Steven Dummit and Richard M Foote, *Abstract algebra*, vol. 3, Wiley Hoboken, 2004.

[HB84] DR Heath-Brown, *Diophantine approximation with square-free numbers*, Mathematische Zeitschrift **187** (1984), no. 3, 335–344.

[Sch03] René Schoof, *Algebraic number theory*, `http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.168.6261&rep=rep1&type=pdf`, 2003, Online; accessed August 11, 2020.

[SS09] Elias M Stein and Rami Shakarchi, *Real analysis: measure theory, integration, and hilbert spaces*, Princeton University Press, 2009.

[Wil95] Andrew Wiles, *Modular elliptic curves and fermat's last theorem*, Annals of mathematics **141** (1995), no. 3, 443–551.

Email address: `asz2115@columbia.edu`