CLASS NUMBERS OF NUMBER RINGS: EXISTENCE AND COMPUTATIONS

GABRIEL GASTER

Abstract. This paper gives a brief introduction to the theory of algebraic numbers, with an eye toward computing the class numbers of certain number rings. The author adapts the treatments of Madhav Nori (from [1]) and Daniel Marcus (from [2]). None of the following work is original, but the author does include some independent solutions of exercises given by Nori or Marcus. We assume familiarity with the basic theory of fields.

1. A Note on Notation

Throughout, unless explicitly stated, R is assumed to be a commutative integral domain. As is customary, we write $\mathrm{Frac}(R)$ to denote the field of fractions of a domain. By $\mathbb{Z}$, $\mathbb{Q}, \mathbb{R}, \mathbb{C}$ we denote the integers, rationals, reals, and complex numbers, respectively. For R a ring, $R[x]$, read 'R adjoin x', is the polynomial ring in x with coefficients in R.

2. Integral Extensions

In his lectures, Madhav Nori said algebraic number theory is misleadingly named. It is not the application of modern algebraic tools to number theory; it is the study of algebraic numbers. We will mostly, therefore, concern ourselves solely with *number fields*, that is, finite (hence algebraic) extensions of $\mathbb{Q}$.

We recall from our experience with linear algebra that much can be gained by slightly loosening the requirements on the structures in question: by studying modules over a ring one comes across entire phenomena that are otherwise completely obscured when one studies vector spaces over a field. Similarly, here we adapt our understanding of algebraic extensions of a field to suitable extensions of rings, called 'integral.'

Whereas $\mathbb{Z}$ is a 'very nice' ring—in some sense it is the nicest possible ring that is not a field—the integral extensions of $\mathbb{Z}$, called 'number rings,' have surprisingly less structure. Arbitrary number rings, for example, do not even have unique factorization into irreducibles—let alone the property of every ideal being principal. As in other subjects, when we are trying to understand objects of a certain type, we try to group them into types. A natural 'class' of number rings would be the ones that happen to be PIDs. We will define the 'class number' of a ring to measure, in some sense, how badly a certain ring fails to be a PID. We will then show that every number ring has finite class number. In other words, every number ring is 'somewhat close' to being a PID. Finally, we will explicitly calculate the class number of some number rings. This might require some slickness, because in general there is no good way to calculate the class number explicitly.

As we will see, our intuition is to translate statements about algebraic numbers into statements about ideals in the ring of integers. In $\mathbb{Z}$, for example, there is a one-to-one correspondence between numbers and ideals because $\mathbb{Z}$ is a principal ideal domain. This is not true for a ring that is not a principal ideal domain. This trouble aside, we will see in Section 3 that ideals of number rings do factor uniquely into a product of prime ideals. This will allow us to more easily calculate the class number, as we reduce our examination of the ideals of a number ring to the prime ones.

Definition 2.1. Let $R \subset B$ be rings. We say $b \in B$ is *integral over* R if b is the root of a monic polynomial with coefficients in R. If b is integral over $\mathbb{Z}$, we say b is an *algebraic integer*. A ring extension $R \subset S$ is *integral* if every $s \in S$ is integral over R.

Note that when R is a field, this definition coincides exactly with algebraic extensions. That is, algebraic extensions of a field and integral extensions of a field are the same darn thing. We now prove some rudimentary facts about integral numbers.

Theorem 2.2 (Gauss)**.** *Let $f \in \mathbb{Z}[x]$ monic, and $f = gh$ for $g, h \in \mathbb{Q}[x]$ monic. Then $g, h \in \mathbb{Z}[x]$.*

Proof. Let m (respectively, n), be the smallest positive integer so that $mg \in \mathbb{Z}[x]$ (respectively, $nh \in \mathbb{Z}[x]$). If the coefficients of mg have a common factor $d > 1$, then, since g is monic, m is the coefficient of the term with highest degree. Whence d divides m. Then $m > m/d \in \mathbb{N}$ and $(m/d)g \in \mathbb{Z}[x]$, contradicting the minimality of m. Similarly for nh. If $mn > 1$, there is a prime $p \in \mathbb{Z}$ dividing mn. Reducing the equation $mnf = (mg)(nh)$ modulo (p) we see p divides $(mg)(nh)$ whence $p|mg$ or $p|nh$. This contradicts the previous assertion that the coefficients of mg (respectively nh) are relatively prime. □

If b is an algebraic over K, there is a monic polynomial over K with b as a root. In fact, we can pick a monic polynomial of this description with the least possible degree. We call this polynomial *the minimal polynomial of b with respect to K*. N.B. that we can really use the word 'the' with reference to the minimal polynomial: we assume familiarity with the fact that $K[x]$ is a Euclidean Domain when K is a field; from this it follows that the minimal polynomial is unique. Similarly, if b is an algebraic integer, there is a monic polynomial over $\mathbb{Z}$ of minimal degree with b as a root. We call this polynomial *the minimal polynomial of b with respect to $\mathbb{Z}$*. We now go about proving that we can meaningfully use the word 'the'.

Corollary 2.3. If b is an algebraic integer, a minimal polynomial of b with respect to $\mathbb{Z}$ is irreducible over $\mathbb{Q}[x]$.

Proof. Assume not. Then f is the product of $g_1, g_2 \in \mathbb{Q}[x]$,with $\deg(g_i) < \deg(f)$. If g_i has leading coefficient c_i, then $c_1 c_2 = 1$ and we can normalize the g_i so that they are monic. By Gauss' Lemma, $g_i \in \mathbb{Z}[x]$ for $i = 1, 2$. This contradicts the assumption that f has least degree. □

Now that we know that a monic polynomial of least degree having b as a root is irreducible over $\mathbb{Q}$, we have deduced uniqueness: as $\mathbb{Q}[x]$ is a Euclidean domain, any two monic polynomials of least degree with b as a root must divide each other (we are skipping steps in this argument, as the method is routine). So, we can rightfully use

the word 'the'. We may then refine our understanding of the relationship between minimal polynomials over K and over $\mathbb{Z}$.

If b is integral over $\mathbb{Z}$, it is algebraic over $\mathbb{Q}$, so it has a minimal polynomial with respect to $\mathbb{Q}$, $g \in \mathbb{Q}[x]$, and a minimal polynomial with respect to $\mathbb{Z}$, $f \in \mathbb{Z}[x]$. As f is irreducible over $\mathbb{Q}[x]$, the uniqueness of monic irreducible polynomials over $\mathbb{Q}$ shows that $f = g$, hence $g \in \mathbb{Z}[x]$. We can thus 'easily decide' if an algebraic number b is an algebraic integer: given the monic minimal polynomial of b, it has coefficients in $\mathbb{Z}$ if and only if it is integral. We summarize:

Corollary 2.4. If K is a number field, $k \in K$ is an algebraic integer if and only if the irreducible polynomial in $\mathbb{Q}[x]$ lies in $\mathbb{Z}[x]$. In other words, the minimal polynomial over $\mathbb{Z}$ is the same as the minimal polynomial over $\mathbb{Q}$.

Corollary 2.5. A rational algebraic integer is an integer.

Proof. The minimal monic polynomial of $q \in \mathbb{Q}$ is $x - q$. Trivially, $x - q \in \mathbb{Z}[x]$ if and only if $q \in \mathbb{Z}$. □

This property of the integers in their field of fractions is essential, and will come up again. In order to generalize our results about integral elements, we will first come up with several equivalent definitions of integral.

Theorem 2.6. *For $R \subset S$ domains, $b \in S$, the following are equivalent:*

1. *b is integral over R*
2. *$R[b]$ is finitely generated as an R-module*
3. *There is a finitely generated R-module M that is torsion free as an $R[b]$-module.*

Proof. (1)⇒(2) If b is the root of a monic irreducible polynomial over R of degree n, then $R[b]$ is in the R-span of $A = \{1, b, b^2, \ldots, b^{n-1}\}$.

(2)⇒(3) Directly: take $R[b] = M$; since S is a domain, $R[b]$ is a torsion free $R[b]$-module.

(3)⇒(1) Essentially, we use the Cayley-Hamilton Theorem to find the characteristic polynomial of ℓ_b, a monic polynomial over R in b. If M is generated by $\{\alpha_0, \ldots, \alpha_n\}$, then we consider the $R[b]$-endomorphism $\ell_b : M \to M$ given by $\alpha_i \mapsto b\alpha_i$ for all $i \in \{0, \ldots, n\}$, and extend linearly to all of M. Note that ℓ_b is an R-module homomorphism precisely because $R[b]$ is a commutative ring. As M is both an $R[b]$-module and an R-module, ℓ_b is both an $R[b]$-module homomorphism and an R-module homomorphism. This means that we can represent ℓ_b as a matrix (not necessarily uniquely!) with entries in $R[b]$ and with entries in R. As an $R[b]$-module endomorphism, we write ℓ_b as the matrix $b\mathbb{I}$; as an R-module endomorphism, we write ℓ_b as the matrix A with coefficients in R. Without loss of generality, assuming that $b \notin R$, $b\mathbb{I}$ and A are distinct matrices. Therefore $b\mathbb{I} - A$ is not identically the 0 matrix. It is, however, the zero endomorphism. We therefore use the standard determinant trick that is so typical of Cayley-Hamilton. For any $a_0, \ldots, a_n \in R$:

$$\ell_b \begin{pmatrix} a_0 \\ a_1 \\ \vdots \\ a_n \end{pmatrix} = (b\mathbb{I}) \begin{pmatrix} a_0 \\ a_1 \\ \vdots \\ a_n \end{pmatrix} = \begin{pmatrix} ba_0 \\ ba_1 \\ \vdots \\ ba_n \end{pmatrix} = A \begin{pmatrix} a_0 \\ a_1 \\ \vdots \\ a_n \end{pmatrix}$$

We see that $b\mathbb{I} - A$ is the zero endomorphism. Examining the main diagonal of A, (let us name it $a_0, \ldots, a_n$), then $a_i \neq b$. Because M is torsion free as an $R[b]$-module, ℓ_b satisfies its characteristic polynomial. That is, $\det(A - x\mathbb{I})$ gives a polynomial for which 0 is a root. □

We can now use that very helpful theorem to deduce several simple facts.

Fact 2.7. Let $R \subset B$ be domains. Then $\mathcal{O}_B = \{b \in B | b \text{ is integral over } R\}$ is a ring, called the *integral closure of R in B*. When the notation is not confusing, we omit the B and write $\mathcal{O}$.

Proof. It is sufficient to show that, for $a_0, a_1 \in \mathcal{O}$, $a_0 + a_1, a_0a_1 \in \mathcal{O}_B = \mathcal{O}$. From theorem 2.6, we know that $R[a_0]$ is finitely generated by $X = \{x_0, \ldots, x_n\}$, similarly for $R[a_1]$ by $Y = \{y_0, \ldots, y_m\}$. We then simply note that $R[a_0, a_1]$ is torsion free as a module over itself. It is generated by $\{xy \mid x \in X, y \in Y\}$ over R. Therefore $R[a_0, a_1]$ is finitely generated and torsion free as an R module, so it is finitely generated and torsion free as an $R[a_0 + a_1]$-module (respectively, as an $R[a_0a_1]$-module) whence $a_0 + a_1$ (respectively a_0a_1) is integral over R by theorem 2.6. □

In the special case when R is $\mathbb{Z}$ and B is a number field, $\mathcal{O}_B$ is called the *the ring of integers* or a *number ring*.

Example 2.8. As $\sqrt{2}$ and $\sqrt{3}$ are algebraic integers, the previous fact shows that $\sqrt{2} + \sqrt{3} = \alpha$ is also an algebraic integer. Using the algorithm outlined in 2.6, we compute the monic polynomial. First we consider the $\mathbb{Q}$-linear transformation $\ell_\alpha : \mathbb{Q}[\sqrt{2}, \sqrt{3}] \to \mathbb{Q}[\sqrt{2}, \sqrt{3}]$. As $\mathbb{Q}[\sqrt{2}, \sqrt{3}]$ has $\mathbb{Q}$-basis $1, \sqrt{2}, \sqrt{3}, \sqrt{6}$, we see:

$$\begin{array}{rcl@{\qquad}rcl} 1 & \mapsto & \sqrt{2} + \sqrt{3} & \sqrt{3} & \mapsto & 3 + \sqrt{6} \\ \sqrt{2} & \mapsto & 2 + \sqrt{6} & \sqrt{6} & \mapsto & 3\sqrt{2} + 2\sqrt{3} \end{array}$$

Whence,

$$\ell_\alpha = \begin{pmatrix} 0 & 2 & 3 & 0 \\ 1 & 0 & 0 & 3 \\ 1 & 0 & 0 & 2 \\ 0 & 1 & 1 & 0 \end{pmatrix}.$$

Furthermore, we can can also view ℓ_α as an endomorphism of $\mathbb{Z}[\alpha]$-modules. ℓ_α can thus be represented as the matrix $\alpha\mathbb{I}$. Since $\mathbb{Z}[\sqrt{2}, \sqrt{3}]$ is torsion free as a $\mathbb{Z}[\alpha]$-module, $0 = \det(\ell_\alpha - \alpha\mathbb{I}) = \alpha^4 - 10\alpha^2 + 1$.

Fact 2.9. Let $R \subset S \subset T$ be domains. If S is integral over R and T is integral over S, then T is integral over R.

Proof. For all $t \in T$, t is the root of a monic polynomial $a_0 + a_1x + \cdots + x^n \in S[x]$. Furthermore, $R[a_i]$ is a finitely generated, free R-module for all $i \in \{0, \ldots, n-1\}$. Thus $R[a_0, a_1, \ldots, a_n] = A$ is a finitely generated free R-module and $A[t]$ is a finitely generated A-module, hence a finitely generated R module. We can thus conclude that $A[t]$ is a finitely generated free $R[t]$-module, whence t is integral over R. □

Fact 2.10. Given a number field, K, with number ring, $\mathcal{O}$, the field of fractions of $\mathcal{O}$ is K.

Proof. Given $\alpha \in K$, there is $m \in \mathbb{Z}$ so that $m\alpha \in \mathcal{O}$. If the minimal (not necessarily monic) polynomial of α is $f(x) = a_nx^n + \cdots + a_0 \in \mathbb{Z}[x]$, then α is a root of $(a_n)^{n-1}f(x) = g(x)$. But $g(x)$ is a monic polynomial in $a_n\alpha$, whence

$a_n\alpha = \alpha' \in \mathcal{O}$. That is, $\frac{1}{a_n} = q \in \mathbb{Q} \subset \text{Frac}(\mathcal{O})$, the field of fractions of $\mathcal{O}$. Therefore, there is $q, \alpha' \in \text{Frac}(\mathcal{O})$ so that $q\alpha' = \alpha$ for all $\alpha \in K$. Therefore $K \subset \text{Frac}(\mathcal{O})$. □

Now that we know that the integral closure of a ring is a ring, and that integral extensions of integral extensions are integral, we have found an interesting substructure of any algebraic extension K of $\mathbb{Q}$. The integral closure of K over $\mathbb{Z}$, $\mathcal{O}_K$ is a ring and contains all the algebraic integers of K.

Definition 2.11. For a domain R with field of fractions K, a ring $S \subset K$ is *integrally closed* if for any $k \in K \setminus S$, k is not integral over S.

Fact 2.12. Given a number field, K. The integral closure of $\mathbb{Z}$ in K, $\mathcal{O}_K$, is integrally closed.

Proof. If $k \in K$ is integral over $\mathcal{O}$, then by Fact (2.9), k is integral over $\mathbb{Z}$, whence $k \in \mathcal{O}$. □

As number fields are finite extensions of $\mathbb{Q}$, *number rings* are the corresponding integral closures of number fields. What can be said about number rings? Certainly, as subrings of fields, they are domains. Are they principal ideal domains? Are they unique factorization domains? We will see the answer to these questions is, unfortunately, no. What properties do they have? Before moving on to number rings, we will start by giving some properties of the simplest number ring, the integers.

Observation 2.13. $\mathbb{Z}$ is a principal ideal domain.

Observation 2.14. $\mathbb{Z}$ is integrally closed in its field of fractions.

Observation 2.15. Nonzero prime ideals are maximal. (Since, for $p \in \mathbb{Z}$ prime, $\mathbb{Z}/p\mathbb{Z}$ is a field.)

Note that if R is a principal ideal domain, then primes are irreducible. That is, for $0 \neq p \in R$ prime, if there were a proper ideal I containing pR then, as R is a PID, there is $r \in R$ so that $I = rR \supset pR$. This means that there is $x \in R$ so that $rx = p$. Since $rR \neq R$, $r \notin R^\times$. Whence, x must be a unit, since p is irreducible. Then $rR = pR$ and pR is maximal. We have shown that, in a principal ideal domain, nonzero primes are maximal. Thus, Observation 2.13 ⇒ Observation 2.15. In fact, in general, unique factorization domains are integrally closed in their field of fractions.

We stated that number rings are not principal ideal domains; in general, they are not even unique factorization domains. It is time for some examples.

Example 2.16. For d a square free integer, $\mathbb{Q}\left[\sqrt{d}\right]$ is a number field with ring of integers

$$\begin{aligned} \mathbb{Z}\left[\sqrt{d}\right] \quad &\text{if} \quad d \equiv 2 \text{ or } 3 \pmod 4 \\ \mathbb{Z}\left[\frac{1+\sqrt{d}}{2}\right] \quad &\text{if} \quad d \equiv 1 \pmod 4 . \end{aligned}$$

This amounts to calculations. For completeness, we include the calculations; reader be advised—you are more likely to understand this if you figure it out yourself. What follows is not the shortest proof, but it is the proof that one finds if one sets out naively.

Proof. As $\mathbb{Q}\left[\sqrt{d}\right]$ is a quadratic extension spanned by 1, $\sqrt{d}$, for any $\alpha \in \mathbb{Q}\left[\sqrt{d}\right]$, $\alpha = a+b\sqrt{d}$ for $a, b \in \mathbb{Q}$. Then α is the root of $(x-(a+b\sqrt{d}))(x-(a-b\sqrt{d})) = x^2 - 2ax + a^2 - b^2 d$. By Fact (2.4), α is an algebraic integer if and only if $2a, a^2 - b^2 d \in \mathbb{Z}$. As $2a = m \in \mathbb{Z}$, this means that $4b^2 d \equiv m^2 \pmod 4$.

What remains to be shown, is that this implies that if $d \equiv 1 \pmod 4$ then $2b \in \mathbb{Z}$ and $2a \equiv 2b \pmod 2$ and if $d \equiv 2, 3 \pmod 4$ then $a, b \in \mathbb{Z}$.

If $d \equiv 1 \pmod 4$ and m is even then $a \in \mathbb{Z}$ so $4b^2 \in 4\mathbb{Z}$, whence $b^2 \in \mathbb{Z}$ and $b \in \mathbb{Q}$. Because rational algebraic integers are integers, $b \in \mathbb{Z}$. Furthermore, $a, b \in \mathbb{Z}$ means that $2a \equiv 2b \equiv 0 \pmod 4$. If m is not even, then $1 \equiv 4b^2 \pmod 4$ so $4b^2 \in \mathbb{Z}$. Thus $2b \in \mathbb{Z}$ and $2b \equiv 1 \equiv 2a \pmod 4$.

We have shown that $\alpha \in \mathbb{Z}\left[\frac{1+\sqrt{d}}{2}\right]$. Furthermore, $\frac{1+\sqrt{d}}{2}$ is an algebraic integer, as it is the root of $x^2 - x + \frac{1-d}{4}$. This completes the case when $d \equiv 1 \pmod 4$.

If $d \equiv 3 \pmod 4$ then $m^2 \equiv 12b^2 \pmod 4$. Then $a \notin \mathbb{Z}$ if and only if $m \notin 2\mathbb{Z}$ if and only if $1 \equiv 12b^2 \pmod 4$ i.e. $3 \equiv 4b^2 \pmod 4$. So $4b^2 \in \mathbb{Z}$ means that $(2b)^2 \in \mathbb{Z}$ whence $2b \in \mathbb{Z}$. But then $(2b)^2 \equiv 3 \pmod 4$ which is impossible for $2b \in \mathbb{Z}$. Similarly for $d \equiv 2 \pmod 4$ because $1 \equiv 8b^2 \pmod 4$ means that $8b^2 \in \mathbb{Z}$, i.e. $(2b)^2 \in \frac{1}{2}\mathbb{Z}$. Since $\frac{1}{2}$ is not a square, $(2b)^2 \in \mathbb{Z}$; whence $2b \in \mathbb{Z}$. But then $(2b)^2 \equiv 0$ or $1 \pmod 4$ implies $8b^2 \equiv 0$ or $2 \pmod 4$; a contradiction.

For $d \equiv 3 \pmod 4$, if $a \in \mathbb{Z}$ then m is even and $0 \equiv 12b^2 \pmod 4$. Then $3b^2 \in 4\mathbb{Z}$ so $b^2 \in \frac{4}{3}\mathbb{Z}$ implies $b^2 \in 4\mathbb{Z}$ whence $b \in 2\mathbb{Z}$. Similarly for $d \equiv 2 \pmod 4$: $a \in \mathbb{Z}$ implies that $0 \equiv 8b^2 \pmod 4$, whence $2b \in \mathbb{Z}$. If $b \notin \mathbb{Z}$, then $2b$ is odd, whence $(2b)^2 \equiv 1 \pmod 4$. But this would imply $0 \equiv 8b^2 \equiv 2 \pmod 4$, a contradiction.

In all cases, we have shown $a, b \in \mathbb{Z}$, whence $\alpha \in \mathbb{Z}\left[\sqrt{d}\right]$. Lastly, $\sqrt{d}$ is obviously integral over $\mathbb{Z}$. This completes the proof. □

We would naturally like to derive properties of these number rings. For $d > 0$, we call $\mathcal{O}_{\mathbb{Q}[\sqrt{d}]}$ a real quadratic number ring; likewise, when $d < 0$, $\mathcal{O}_{\mathbb{Q}[\sqrt{d}]}$ is an imaginary quadratic number ring.

Fact 2.17. $\mathcal{O}_{\mathbb{Q}[\sqrt{-5}]} = \mathbb{Z}\left[\sqrt{-5}\right]$ is not a unique factorization domain.

This will become clear, once we determine some primes in $\mathbb{Z}\left[\sqrt{-5}\right]$. In order to do that without causing too much of a headache, we will first develop some tools to analyze the structure of number rings. Using the determinant trick from the proof of Theorem 2.6, we consider the following.

Definition 2.18. For a field F, and for B a finite dimensional F-algebra, for a fixed $\alpha \in B$ we consider the F-algebra homomorphism $r_\alpha : B \to B$ given by $x \mapsto x\alpha$ for all $x \in B$. We then define the *norm* of α (relative to F), $N_{B/F}(\alpha) = \det_F(r_\alpha)$. If no confusions arise, for simplicity, we write $N_F(\alpha)$ or even $N(\alpha)$.

Fact 2.19. The norm is multiplicative.

This is immediate, as the determinant is. One might ask if $\det(r_\alpha) = \det(\ell_\alpha)$ for all $\alpha \in B$. Generally speaking, if the F-algebra is not commutative, this might not be the case. We will show, however, that if the F-algebra is simultaneously a division algebra, they are equal. First though, we have an example.

Example 2.20. Recalling the algebraic integer $\sqrt{2}+\sqrt{3} = \alpha$ from example 2.8, we compute $N_{\mathbb{Q}}(\alpha)$. This amounts to taking the determinant of the linear transformation in 2.8, or, because we are lazy, simply plugging in 0 for the minimal polynomial of α in the determinant already computed. Then $N(\alpha) = 1$, the constant term of the monic polynomial of α. The way that we arrived at this computation reveals that this is not a coincidence—it suggests a deeper phenomenon. We also note that $N(\sqrt{2}+\sqrt{3}) \in \mathbb{Z}^\times$ and, indeed, $\sqrt{2}+\sqrt{3} \in \mathcal{O}^\times$.

Claim 2.21. *Let B be a division algebra over F a field with $\dim_F(B) = n$. Given $b \in B$ with minimal monic polynomial $f \in F[x]$, $f(x) = x^r + a_1x^{r-1} + \cdots + a_r$, $\det(r_b) = \left((-1)^r a_r\right)^{n/r}$. In particular, $\det(r_b) = \det(\ell_b)$.*

Proof. Let $L = F[b]$. Then $\dim_F L = r$ and $F \subset L \subset B$. Then L is a finite dimensional integral domain (since B is a division algebra), whence L is a division algebra, making B an L-vector space. This shows $r|n$.

The ring L has F-basis $1, b, b^2, \ldots, b^{r-1}$. Let B have L-basis $1 = v_1, v_2, \ldots, v_{r/n}$. Then $r_b|_L = r'_b$ is an F-algebra endomorphism. In fact, we can easily calculate the determinant of r'_b : because b is a primitive element, r'_b acts very nicely on the basis formed by powers of b.

$$r'_b = \begin{pmatrix} 0 & 0 & 0 & \cdots & a_r \\ 1 & 0 & 0 & \cdots & a_{r-1} \\ 0 & 1 & 0 & \cdots & a_{r-2} \\ \vdots & & & \ddots & \\ 0 & 0 & \cdots & 1 & a_0 \end{pmatrix} \tag{2.1}$$

so that

$$\det(r'_b) = (-1)^{r-2} \det \begin{pmatrix} a_r & 0 & 0 & \cdots & 0 \\ a_{r-1} & 1 & 0 & \cdots & 0 \\ a_{r-2} & 0 & 1 & \cdots & 0 \\ \vdots & & & \ddots & \\ a_0 & 0 & 0 & \cdots & 1 \end{pmatrix} = (-1)^r a_r$$

We can extend this calculation to r_b, as we have a nice F-basis of B which decomposes B into n/r invariant subspaces of dimension r. Pick the basis $\{a_i b^j | i \in \{1, \ldots, r/n\}, j \in \{0, \ldots, r-1\}\}$, then

$$r_b = \begin{pmatrix} \square & 0 & 0 \\ 0 & \ddots & 0 \\ 0 & 0 & \square \end{pmatrix}$$

where $\square$ denotes the matrix previously associated to r'_b. A simple linear algebra trick gives $\det(r_b) = \left(\det(r'_b)\right)^{n/r}$, whence the claim. $\square$

Observation 2.22. The usual norm in $\mathbb{C}$ of an element $a + bi$, for $a, b \in \mathbb{R}$, is given by $a^2 + b^2$ which happens to equal the product of the complex conjugates

$(a+bi)(a-bi)$. Thus the norm as defined in 2.18 coincides with the one we know (and love).

The following is immediate from the calculation of claim 2.21.

Corollary 2.23. Let K be a number field with integral closure $\mathcal{O}$ with respect to $\mathbb{Z}$. Then for $a \in \mathcal{O}$, $N_{K/F}(a) \in \mathbb{Z}$.

Corollary 2.24. For α algebraic over F, a field, $N_{F[\alpha]/F}(\alpha)$ is the product of the conjugates of α.

Proof. The minimal monic polynomial of α, $f(x) = \prod_{\sigma \in \mathrm{Emb}_{\overline{F}}(F[\alpha])} (x - \sigma(\alpha))$, whence the constant term of f is the product of the conjugates, $= (-1)^r \prod_\sigma (\sigma(\alpha))$. □

Corollary 2.25. With K and $\mathcal{O}$ and a as before, $N(a) = \pm 1$ if and only if $a \in \mathcal{O}^\times$.

Proof. If $N(a) = \pm 1$ then the minimal monic polynomial over $\mathbb{Z}$ of a has constant term ± 1. For all $\gamma \in \mathrm{Emb}_{\overline{\mathbb{Q}}} L$, $0 = \gamma(f(b)) = f(\gamma(b))$ shows that $\gamma(b) \in \mathcal{O}$. But the product of the conjugates of b is precisely the constant term of f, i.e. ± 1. If $a \in \mathcal{O}^\times$, then there is $a^{-1} \in \mathcal{O}$ so that $N(a)N(a^{-1}) = N(1) = 1$, i.e. $N(a) \in \mathbb{Z}^\times$. □

With this extra machinery, we can now return to the problem of (2.17). Observing that $a + b\sqrt{-5}$ is conjugate to $a - b\sqrt{-5}$ over $\mathbb{Q}$, we see that $N(a + b\sqrt{-5}) = a^2 - 5b^2$. We then conclude that $\mathbb{Z}\left[\sqrt{-5}\right]$ has no elements of norm 2 or 3. If $a + b\sqrt{-5} \in \mathbb{Z}\left[\sqrt{-5}\right]$ had norm 2, then $a^2 - 5b^2 \equiv a^2 - b^2 \equiv 2 \pmod 4$, an impossibility. Likewise $a^2 - 5b^2 \equiv a^2 \equiv 3 \pmod 5$ is impossible. We then conclude that $2, 3, (1+\sqrt{-5}), (1-\sqrt{-5})$ are irreducible. As no algebraic integers in $\mathbb{Z}\left[\sqrt{-5}\right]$ have norm 2 or 3, there are no nonunit algebraic integers whose product has norm $4, 6$ or 9. However, this means that $6 = 2 \cdot 3 = (1 + \sqrt{-5})(1 - \sqrt{-5})$ cannot be written uniquely as the product of irreducibles.

3. Number Rings

We have seen what can go wrong with number rings. Now we would like to come up with some properties that number rings do have. We return to the observations about the integers from 2.15.

Definition 3.1. A *noetherian module* is one in which every submodule is finitely generated. A *noetherian ring* R is a noetherian R-module.

Theorem 3.2. *The following are equivalent.*

1. *A module M is noetherian, i.e. every submodule is finitely generated.*
2. *M has the ascending chain condition on submodules.*
3. *Every nonempty set of submodules of M has a maximal element.*

Proof. (1) ⇒ (2) If $I_1 \subset I_2 \subset \cdots$ is an infinite chain of submodules of M, then $\bigcup_{n\in\mathbb{N}} I_n = I$ is a submodule of R, hence finitely generated: $I = Rv_1 + \cdots + Rv_k$. For all $i \in \{1, \ldots, k\}$ there is $I_{j_i} \subset R$ so that $v_i \in I_{j_i}$. Therefore $\max_{i\in\{1,\ldots,k\}}(j_i) = j$ and $I_j = I$, whence the chain stabilizes.

(2) ⇒ (3) If M has the ascending chain condition on submodules, then given a nonempty set of submodules $\{I \subset R\} = A$, we will assume there is no maximal submodule. As $I_1 \in A$ is not maximal, there is $I_2 \in A$ strictly containing I_1. Inductively, if $I_k \in A$ is not maximal, there is $I_{k+1} \in A$ strictly containing I_k.

There is thus a strictly ascending chain of submodules. By assumption, the chain terminates, contradicting the strict ascent of the chain—whence there is a maximal submodule in A.

(3) $\Rightarrow$ (1) Assume, toward a contradiction, that there is a nonfinitely generated submodule $I \subset R$. Then let $A = \{J \subset R | J \subset I,\ J \text{ finitely generated}\}$. If A had a maximal element J, then, as I is not finitely generated, there is $x \in I/J$. $J \neq J + xR \in A$ contradicts the maximality of J. □

Corollary 3.3. A submodule of a noetherian module M is noetherian.

Proof. It is sufficient to show that a submodule $A \subset M$ is noetherian according to definition (2) of Theorem 3.2. Given any ascending chain of submodules of A, it is also an ascending chain of submodule in R, whence the chain stabilizes. □

Note that the definition of a noetherian ring can be equivalently reformulated by replacing the word 'module' with 'ring' and the word 'submodule' with 'ideal' in 3.2.

Corollary 3.4. A quotient module M/N of a noetherian module M is noetherian.

Proof. Let $\pi : M \to M/N$ be the quotient map. Much as in 3.3, any ascending chain of submodules $A_i \subset M/N$ pulls back to an ascending chain of submodules $\pi^{-1}(A_i) \subset M$, since $\pi^{-1}(A_i)$ stabilizes, so do A_i. □

Fact 3.5. Given M, an R-module, with submodule $N \subset M$ so that N and M/N are noetherian, then M is noetherian.

Proof. [1] Given a submodule $A \subset M$, then $N \cap A = B \subset N$ is a submodule of N, hence it is finitely generated, i.e. there are $a_1, \ldots, a_n \in M$ so that $B = Ra_1 \oplus \cdots \oplus Ra_n$. Let $\pi : M \to M/N$ be the natural projection. Then $\pi(A) \subset M/N$ is a submodule, hence it is finitely generated by $b_1, \ldots, b_m$. Then there are $c_1, \ldots, c_m \in M$ so that $\pi(c_i) = b_i$ for each $i \in \{1, \ldots, m\}$. Now, as M/N is generated by b_i, for every $s \in M$, $\pi(s) = \sum_{i=1}^{m} \alpha_i b_i$, so $s = \sum_{i=1}^{m} \alpha_i c_i + y$ for some $y \in B$. Then for every $x \in A$ there is a $y \in B$ so that $x - y$ is in the R-span of $c_1, \ldots, c_m$, whence $A = Ra_1 \oplus \cdots \oplus Ra_n \oplus Rc_1 \oplus \cdots \oplus Rc_m$. □

Corollary 3.6. For R a noetherian ring, if M is a noetherian R-module with the structure of a ring, then it is a noetherian ring.

Proof. Since any M-submodule of M is also a R-submodule, an ascending chain of M-submodules must stabilize. □

Here, we use the trace-form, which we'll define as the trace of the linear map that is multiplication on the left.

Definition 3.7. For $x \in L$ a finite extension of K, the *trace of x with respect to* L/K is $\mathrm{Tr}_{L/K}(x) = \mathrm{tr}_K(\ell_x)$, the trace of the multiplication-by-x linear map.

As in the calculation of the norm (2.21), we have the following fact.

Fact 3.8. For L/K separable, $\mathrm{Tr}_{L/K}(x) = \sum_{\sigma \in \mathrm{Emb}_{\overline{K}}(L)} \sigma(x)$

[1] This proof is directly from [4].

Proof. For $x \in K$, $\mathrm{Tr}_{L/K}(x) = \deg(L/K)x$, verifying the fact on K. For $x \in L$ with minimal polynomial $x^n + a_{n-1}x^{n-1} + \cdots + a_0$, consider $K[x] = F$ with basis $1, x, \ldots, x^{n-1}$. Then $\ell_x \in \mathrm{End}_K(F)$. With the basis chosen, we refer to equation 2.1 on page 7 to conclude that $\mathrm{tr}(\ell_x) = a_{n-1}$, which is the sum of the conjugates of x. Allowing $\ell_x \in \mathrm{End}_K(L)$, we see $\mathrm{Tr}_{L/K}(\ell_x) = [L : F] \sum_{\sigma \in \mathrm{Emb}_{\overline{K}}(L)} \sigma(x)$, finishing the proof. □

Corollary 3.9. For x integral over a PID R, $\mathrm{tr}(x) \in R$. In particular, we care for the case when $R = \mathbb{Z}$.

Proof. Let $f(x) = x^n + a_{n-1} + \cdots + a_0 \in R[x]$ be the monic polynomial of x; $\mathrm{tr}(x) = a_{n-1} \in R$. □

From Fact 3.8, we conclude that the trace is additive and scalars pull out. Therefore, $(x, y) \mapsto \mathrm{Tr}(xy)$ is a symmetric bilinear form, called the trace form. We now cite Lang [3], Theorem 5.2, which gives

Fact 3.10. For L/K a finite extension, L/K is separable if and only if the trace-form $(x, y) \mapsto \mathrm{Tr}_{L/K}(xy)$ is nondegenerate, i.e. if and only if the map $L \to L^*$, the dual vector space over K, by $v \mapsto \mathrm{tr}_v \in L^*$, $\mathrm{tr}_v(x) = \mathrm{tr}(vx)$, is an isomorphism of K-vector spaces.

Obviously every PID is noetherian, as each ideal is, in fact, generated by one element (i.e. every ideal is principal). We showed, however, that some number rings are not principal ideal domains. Have no fear though, we will show that all number rings are noetherian.

Definition 3.11. For R a PID, K its field of fractions, L a finite extension of K, a ring $A \subset K$ is an *R-order of L* if the following conditions hold:

(1) $A \supset R$
(2) A is finitely generated as an R-module
(3) For every $k \in K$ there is $0 \neq c \in R$ so that $ck \in A$.

Observation 3.12. From before, we saw that a ring of integers is an order. We also saw that for any order A, $A \subset \mathcal{O}_L$. We will use this necessary condition of $\mathcal{O}_L$ to show that it is noetherian.

Fact 3.13. For R a PID, K its field of fractions, L a finite extension of K, there is an order $R \subset A \subset K$.

Proof. Pick a K basis of L, $S = \{w_1, \ldots, w_n\}$. As L is a K-algebra, $w_i w_j \in L$, let $a_{i,j,k} \in K$ so that $w_i w_j = \sum_{k=1}^n a_{i,j,k} w_k$. As there are finitely many $a_{i,j,k} \in K$, there is $c \in R \backslash 0$ so that $ca_{i,j,k} \in R$ for all $i, j, k \in \{1, \ldots, n\}$. Because $(cw_i)(cw_j) = \sum_{k=1}^n (ca_{i,j,k})(cw_k)$, $A' = Rcw_1 \oplus \cdots \oplus Rcw_n$ is a finitely generated R-module which is also closed under multiplication. If we let $A = R \oplus A'$, it is clear that A contains R and is finitely generated. Furthermore, for $k \in L$, write $k = \sum_{i=1}^n a_i w_i$ for $a_i \in K$. Then, because K is the field of fractions of R, there is $0 \neq r \in R$ so that $ra_i \in R$ for all $i \in \{1, \ldots, n\}$. Then $rk \in Rw_1 \oplus \cdots \oplus Rw_2$, whence $crk \in A' \subset A$. □

Observation 3.14. For R a PID, K its field of fractions, L a finite extension of K, if A is an R-order then the field of fractions $\mathrm{Frac}(A) = L$.

Proof. Given $k \in L$, there is $0 \neq c \in R$ so that $0 \neq ck \in A$. Clearly $K \subset \mathrm{Frac}(A)$, so $\frac{1}{c} \in \mathrm{Frac}(A) \Rightarrow k \in \mathrm{Frac}(A)$. □

Observation 3.15. The rank of a $\mathbb{Z}$-order A of a number field K is at least the dimension of the number field.

Proof. For every $k \in K$, there is $r \in \mathbb{Z}$ so that $rk \in A$. We conclude the generating set $v_1, \ldots, v_n$ of A spans K. □

Claim 3.16. *For R a PID with field of fractions K, and a finite separable extension L/K, $\mathcal{O}_L$ is a noetherian ring.*

Proof. Pick A an R-order of L with R-basis $v_1, \ldots, v_n$. Because A is an order, $v_1, \ldots, v_n$ form a K-basis of L. As L/K is finite and separable, the trace form is nondegenerate, whence the tr_{v_i} form a K-basis of L^*, the K-vectorspace dual to L, according to notation from 3.10. Furthermore, there is a basis $v^i \in L$ so that $\mathrm{tr}_{v_i}(v^j) = \delta_{i,j}$. Consider $A^\perp = \{x \in L |\ \mathrm{tr}(\alpha x) \in R \ \forall\ \alpha \in A\}$. Because the trace is linear, $A^\perp$ is an R-module. Then for any $\alpha \in \mathcal{O}_L$ and $x \in A \subset \mathcal{O}_L$, as $\alpha x \in \mathcal{O}_L$, the Corollary 3.9 shows that $\mathcal{O}_L \subset A^\perp$. To show $\mathcal{O}_L$ is noetherian, it is thus sufficient to show that $A^\perp$ is noetherian, by 3.3. If $x \in A^\perp$, let $x = q_1 v^1 + \cdots + q_n v^n$ for $q_i \in K$. Then, for any $v_i \in A$, $\mathrm{tr}(v_i x) = q_i \in R$. This proves that $A^\perp \subset Rv^1 \oplus \cdots \oplus Rv^n$ is a finitely generated R-module, hence a noetherian R-module. In fact, $\mathrm{tr}(v_i v^j) \in R$ shows that $A^\perp = Rv^1 \oplus \cdots \oplus Rv^n$. By Corollary 3.6, $\mathcal{O}_L \subset A^\perp$ is a noetherian ring. □

In fact, we can improve this proof to bound the index $[\mathcal{O}_L : A]$. We consider the matrix $M = \left(\mathrm{tr}(v_i v_j)|_{i,j=1}^n\right)$, the associated matrix to the symmetric bilinear form. For $w_1, w_2 \in L$, letting $\vec{w_1}, \vec{w_2}$ denote the column vector according to the v_i basis, we see $\mathrm{tr}(w_1 w_2) = \vec{w_1}^{\mathrm{T}}(M)\vec{w_2}$.

Definition 3.17. The *discriminant* of a finite separable extension L/K is the determinant of the trace-form matrix.

Improvement 3.18. Given R a PID with field of fractions K, a finite separable extension L/K with discriminant d, and an R-order A of L, $[\mathcal{O}_L : A] \leq d$.

Proof. As before, $A = Rv_1 \oplus \cdots \oplus Rv_n$. We seek to compute the basis v^i used in the previous proof. We want a basis v^i so that $\mathrm{tr}(v^i v_j) = \delta_{i,j}$, i.e. we want $\vec{v^i}^{\mathrm{T}}(M)\vec{v_j} = \delta_{i,j}$. This means $\vec{v^i}^{\mathrm{T}}(M) = \vec{v_i}^{\mathrm{T}}$, or $(M)^{\mathrm{T}}\ \vec{v^j} = \vec{v_i}$. This amounts to computing the inverse matrix, for which we invoke the useful Cramer's Rule: let N be the matrix of minors of M^{T}, then $NM^{\mathrm{T}} = \det(M)\mathbb{I}$, where $\mathbb{I}$ is the identity matrix. In particular, N has entries that are polynomials in the coefficients of M, hence N has entries in R.

$$\begin{aligned}
(M)^{\mathrm{T}}\vec{v^j} &= \vec{v_i} \\
N(M)^{\mathrm{T}}\vec{v^j} &= N\vec{v_i} \\
\det(M)\vec{v^j} &= N\vec{v_i} \\
\vec{v^j} &= \frac{1}{\det(M)} N\vec{v_i} \in \frac{1}{d}A
\end{aligned}$$

Then $A \subset \mathcal{O}_L \subset \bigoplus_{i=1}^n Rv^i \subset \frac{1}{d}A$, whence $[\mathcal{O}_L : A] \leq \det(M) = d$. □

Fact 3.19. In number rings, ideals have finite index.

Proof. For $\mathcal{O}$ a number ring of number field K, I an ideal, let $0 \neq \alpha \in I$. Since K is a domain, $N(\alpha) \neq 0$. We have already seen in corollary 2.23, that $N(\alpha) = m \in \mathbb{Z}$. Then let β be the product of the nontrivial conjugates of α; in (2.24) we showed that $\alpha\beta = m$, whence $\beta \in K$. Since β is integral over $\mathbb{Z}$ and in K, $\beta \in \mathcal{O}$, whence $\alpha\beta = m \in I$, and $Rm \subset I$. The quotient $R/(Rm)$ has exactly $m^{\deg K/\mathbb{Q}}$ elements: since R is a free $\mathbb{Z}$-module of rank $\deg K/\mathbb{Q}$, $\frac{\left(\bigoplus_{i=1}^{\deg K/\mathbb{Q}} \mathbb{Z}\right)}{m\left(\bigoplus_{i=1}^{\deg K/\mathbb{Q}} \mathbb{Z}\right)} \simeq \bigoplus_{i=1}^{\deg K/\mathbb{Q}} \mathbb{Z}/m\mathbb{Z}$. Then $|R/I| < |R/(Rm)|$, R/I divides $R/(Rm)$. □

Definition 3.20. The *norm of an ideal* $I \triangleleft R$ of a domain is the index $[R : I]$ of the ideal in the ring, denoted $\|I\|$.

Observation 3.21. For principal ideals of a number ring, $Rx \triangleleft R$, $\|Rx\| = |R/Rx| = N(x)$, this follows because $\ell_x : R \to Rx$ and $\det(\ell_x) = |R/Rx|$. More generally, the norm of an element of an ideal as defined in 2.18 divides the norm of an ideal containing that element. 3.19 shows that ideals have finite norm. That the index of ideals is multiplicative shows the norm of ideals to be multiplicative.

Corollary 3.22. In number rings, nonzero primes are maximal.

Proof. For P a prime ideal of $\mathcal{O}$, $\mathcal{O}/P$ is an integral domain. In fact, by (3.19), it is a finite integral domain i.e. a field, whence P is maximal. □

These properties alone turn out to be quite stringent: from these we can deduce much about our ring. For that reason, it makes sense to name this class of rings.

Definition 3.23. A domain R with the following properties is called a *Dedekind domain*:

(1) R is noetherian.
(2) Every nonzero prime is maximal.
(3) R is integrally closed in its field of fractions.

Corollary 3.24. Every number ring is a Dedekind domain.

Proof. We have shown 1 in claim 3.16 and 2 in 3.22. From 2.10 and 2.12, 3 is immediate. □

We are now in good shape to prove some key facts about Dedekind domains. And, the best part is that every time we prove something about a Dedekind domain, we prove something about number rings!

Fact 3.25. In a Dedekind domain, D, every ideal contains a product of prime ideals.

Proof. If not, then there is a nonempty set of ideals that contain no products of primes. This set has a maximal member I by definition 3 of a noetherian ring. As I is not prime (otherwise it would not be in the set of ideals containing no products of primes), there are $a, b \in R/I$ so that $ab \in I$, whence $Ra + I$, $Rb + I$ are ideals that are both strictly bigger than I, i.e. containing a product of prime ideals. On the other hand, $(Ra+I)(Rb+I) = R^2ab+RaI+RbI+I^2 \subset I$, contains a product of primes. □

That is a cool fact about number rings that we, otherwise, did not know. If we think of the simplest Dedekind domain ($\mathbb{Z}$), then the previous fact is stupid-easy as $\mathbb{Z}$ is a PID.

Lemma 3.26. *For $A \subsetneq D$ an ideal of a Dedekind domain with field of fractions K, there is $\psi \in K \backslash D$ so that $\psi A \subset D$.*

Before we prove this Lemma, we state it in terms of $\mathbb{Z}$ for concreteness: given a proper ideal $(n\mathbb{Z})$, $n \in \mathbb{Z}$, there is a nonintegral fraction $q \in \mathbb{Q}/\mathbb{Z}$ so that $q(n\mathbb{Z}) \subset \mathbb{Z}$. Naturally, we would think to take $\frac{1}{n} = q \notin \mathbb{Z}$ because n is not a unit. In the case where the Dedekind domain in question is not a principal ideal domain, this will not be so straightforward.

Proof of Lemma. We will examine $0 \neq a \in A$. Then $Da \triangleleft D$ means that Da contains a product of prime ideals: in particular there is a minimal n so that $P_1 \cdots P_n \subset Da$. Furthermore, there is a maximal (hence prime) ideal $I \supset A \supset P_1 \cdots P_n$. If $P_i \not\subset I$ for all $i \in \{1, \ldots, n\}$ then there would be an n-tuple $(a_1, \ldots, a_n)$ so that $a_i \notin I$ and $a_1 \cdots a_n \in I$, contrary to the primality of I. Therefore there is a $P_i \subset I$; without loss of generality, let $P_1 \subset I$. Because, in Dedekind domains, prime ideals are maximal, $P_1 = I$. Then, as Da cannot contain a product of fewer than n primes, $P_2 \cdots P_n \backslash Da$ is nonempty. Let $b \in P_2 \cdots P_n \backslash Da$, then $\psi = b/a \in K$. Since $\psi a \notin Da$, $\psi \notin D$. Furthermore, since $P_1 \supset A$, for all $\alpha \in A$, $b\alpha \in P_1 \cdots P_n \subset Da$ whence $b\alpha$ is a multiple of a and $\psi\alpha = b\alpha/a \in R$. □

Claim 3.27. *For every ideal $I \triangleleft D$ a Dedekind domain, there is an ideal $I' \triangleleft D$ so that II' is principal.*

Proof. Let $0 \neq \alpha \in I$. Then $I' = \{\psi \in D | \psi I \subset D\alpha\}$ is an ideal: if $a_1, a_2 \in J$ then $(a_1 + a_2)I = a_1 I + a_2 I \subset D\alpha$ and, for all $b \in D$, $b(a_1 I) \subset b(D\alpha) \subset D\alpha$. Since $\alpha \in I'$, I' is a nonzero ideal and $II' \subset D\alpha$. Then $A = \frac{1}{\alpha} II' \subset D$ is an ideal because D is commutative.

There are then two possibilities: either $A = D$ or $A \subsetneq D$. If $A = D$, then $II' = D\alpha$, whence the claim. If $A \subsetneq D$, then by 3.26 there is $\psi \in K \backslash D$ so that $\psi A \subset D$. Since $\alpha \in I$, $I' \subset A$ and $\psi I' \subset \psi A \subset D$. Also, $\psi A = \psi \frac{1}{\alpha} II' \subset D$ means that $\psi II' \subset D\alpha$, whence, for all $j \in I'$, $\psi(jI) \subset D\alpha$ shows that $\psi j \in I'$.

I' now looks surprisingly like a $D[\psi]$ module. Since I' is finitely generated as a D-module—because D is a Dedekind domain—it is finitely generated as a $D[\psi]$-module, whence ψ is integral over D by property 3 of 2.6. Then, by the integral closure of Dedekind domains, $\psi \in D$, contradicting 3.26. □

Corollary 3.28 (Cancellation Law)**.** If $A, B, C \triangleleft D$, a Dedekind domain, $AB = AC \Rightarrow B = C$.

Proof. By Claim 3.27 there is $A' \triangleleft D$ so that $A'A$ is principal, so there is $\alpha \in D$ such that $A'A = \alpha D$ and $(\alpha D)B = (\alpha D)C$. Trivially: for every $a_1 \in (\alpha D)B$ there is $a_2 \in (\alpha D)C$ so that $a_1 = a_2$. Then there is $d_1, d_2 \in D$ and $b \in B$, $c \in C$ so that $a_1 = \alpha d_1 b$ and $a_2 = \alpha d_2 c$. If K is the field of fractions of D, there is $\frac{1}{\alpha d_1}, \frac{1}{\alpha d_2} \in K$ so that $a_1 = a_2 \ \Rightarrow b = c$. □

As we have a suitable cancellation law in multiplication of ideals, we know what it means for ideals to *divide one another*. If A, B are ideals of some domain R, then we say A divides B (written $A|B$) if there is $r \in R$ so that $rA = B$.

Corollary 3.29. For D a Dedekind domain, if $A, B \triangleleft D$ then $A|B$ if and only if $A \supset B$. This is often rephrased simply as: in Dedekind domains, to divide is precisely to contain.

Proof. Trivially, $A|B$ means that for every $a \in A$ and $b \in B$ there is $c \in D$ so that $ac = b$, whence $b \in A$ and $B \subset A$. On the other hand, if $A \supset B$, then for some $\alpha \in D$ there is $A' \triangleleft D$ so that $AA' = D\alpha$ and $BA' \subset D\alpha$. We then see that $C = \frac{1}{\alpha}BA' \subset D$. Exactly as in the proof of Claim 3.27, C is in fact an ideal. Then $AC = B$. □

Elucidating the structure of Dedekind domains, we are now set to prove a very pleasing result, which (partially) offsets the unpleasantness that there are number rings that are not unique factorization domains.

Theorem 3.30. *Every (proper) ideal in a Dedekind domain D is uniquely representable as a product of prime ideals.*

While it is not true, that unique factorization domains are Dedekind in general, this theorem shows that in some sense a Dedekind domain can be worked with in a similar fashion as a UFD. This theorem is encouraging in that it enables us to work effectively with ideals of number rings.

Proof. Proof of TheoremWe proceed exactly as in the proof of the fundamental theorem of arithmetic (that $\mathbb{Z}$ is a UFD): first we show every ideal is the product of primes. We consider the (nonempty) collection S of proper ideals of D which are not representable as a product of primes. Since D is noetherian, S has a maximal element $M \subsetneq D$. M is contained in a maximal (hence prime) ideal P. By Corollary 3.29, P divides M and there is ideal $Q \triangleleft D$ so that $M = PQ$. Similarly, Q divides M so $Q \supset M$: we see, from the Cancellation Law 3.28, that $Q \supsetneq M$: if $Q = M$ then $DM = DQ \Rightarrow D = P$, contradicting the primality of P. As $Q \supsetneq M$, $Q \notin S$, whence Q is a product of primes. But $M = PQ$ shows that M is also, in fact, a product of primes, contradicting $M \in S$.

Note that the proof has used the same arguments employed in the fundamental theorem of arithmetic.

We still must show that the representation of an ideal as a product of prime ideals is unique. Suppose not: then there is a minimal $r \in \mathbb{N}$ so that there are equivalent products of prime ideals $P_1 \cdots P_r = Q_1 \cdots Q_s$ for $P_i \neq Q_j$ for some $i \in \{1, \ldots, r\}$, $j \in \{1, \ldots, s\}$. We conclude that $P_1 \supset Q_1 \cdots Q_s$, and, precisely as in the proof of Lemma 3.26, there is $Q_i \subset P_1$; without loss of generality $Q_1 \subset P_1$. Because P_1 is a prime ideal, it is maximal by property 2, hence $P_1 = Q_1$. From the Cancellation Law 3.28, we see $P_2 \ldots P_r = Q_2 \ldots Q_s$, contradicting the minimality of r. □

Corollary 3.31. A number ring has unique factorization into prime ideals.

We finish this section with a nice application of this fact to our understanding of the ideals of a number ring. This will come up again later, when we talk about how number rings are 'almost' principal ideal domains.

Fact 3.32. For any $n \in \mathbb{N}$, there are finitely many ideals I in $\mathcal{O}$ so that $\|I\| = n$.

Proof. The norm is multiplicative and takes integer values. Furthermore, primes ideals take values strictly greater than 1. Because ideals in number rings have unique factorization into primes, we most simply prove there are finitely many prime ideals with norm $\leq n$. For $x \in I$, any ideal, x satisfies an (irreducible) monic polynomial with coefficients in $\mathbb{Z}$, whence the constant term of the polynomial is nonzero, i.e. $x^r + a_{r-1} + \cdots + a_0 = 0$ for $a_i \in \mathbb{Z}$, $a_0 \neq 0$. Then $a_0 = x^r + \cdots + a_1 x \in I$,

whence $I \cap \mathbb{Z} \neq 0$. Therefore, if P is a (proper) prime ideal in $\mathcal{O}$, it contains a nonzero integer $a_0 \in P$. Say $a_0 = p_1^{l_1} p_2^{l_2} \cdots p_e^{l_e}$ the prime factorization of a_0 in $\mathbb{Z}$. Then, by definition of primality, there is a $p_i \in P$. If P contained another prime integer q, then P contains their $\mathbb{Z}$-span, namely, 1, contradicting the primality of P. Therefore a prime ideal contains only one integer prime. Since $\|P\| \geq 2$, its prime factorization must be the power of a prime, i.e. $\|P\| = p^t$ for $t \in \mathbb{N}$. Then $p\mathcal{O}$ factors $\prod_{i=1}^{s} P_i^{a_i}$. If an ideal has norm a power of p, then it contains p. To divide is to contain implies that the ideal divides $p\mathcal{O}$. But there are only s such prime ideals. □

4. Ideal Classes

Now that we have seen that some number rings are not principal ideal domains, we would like some way of measuring how much $\mathbb{Z}\left[\sqrt{-5}\right]$ is not a PID. In the integral closure of a number field, we see that, all (nonzero) principal ideals are a scalar of one another—i.e. there is an element in the number field that appropriately scales any (nonzero) principal ideal to any other. This does not seem like it should be true for ideals in general—if an ideal were a scalar of a principal ideal, it would be principal. With this in mind we partition the set of ideals into classes under the following relation.

Definition 4.1. For number field K with ring of integers $\mathcal{O}_K = \mathcal{O}$, two nonzero ideals $I_1, I_2 \triangleleft \mathcal{O}$ are *principally equivalent*, denoted $\sim$, if there is $\alpha \in K$ so that $I_1\alpha = I_2$. The *class number* of a ring of integers (or of a number field) is the number of ideal classes under right principal equivalence.

Fact 4.2. Right principal equivalence is an equivalence relation.

Proof. Obviously every ideal is principally equivalent to itself. As we only concern ourselves with nonzero ideals, $I_1\alpha = I_2$ means that $\alpha \in K^\times$, whence $\alpha^{-1} \in K$ and $I_2\alpha^{-1} = I_1$. $I_1 \sim I_2 \sim I_3$ so that $I_1\alpha_1 = I_2$ and $I_2\alpha_2 = I_3$ implies $I_1\alpha_1\alpha_2 = I_3$. □

Observation 4.3. For a number field, the class number is 1 if and only if the corresponding number ring is a principal ideal domain.

Proof. If the class number is 1, then there is $\alpha \in K$ so that every ideal is equivalent to the nonproper ideal R, whence the ideal is $R\alpha$. If the number ring is a principal ideal domain, then for all nonzero ideals $R\alpha_1$, $R\alpha_2$ there is $q = \frac{\alpha_1}{\alpha_2} \in K$ so that $R\alpha_2 k = R\alpha_1$. □

Fact 4.4. The set of ideal classes of a ring of integers $\mathcal{O}$ forms a group under multiplication.

Proof. It must be checked is that multiplication is well defined on the equivalence classes. For $I_1, I_2, J \triangleleft \mathcal{O}$ so that $I_1 \sim I_2$, we must show $I_1 \cdot J \sim I_2 \cdot J$. If $\alpha \in K$ so that $I_1\alpha = I_2$, then $(I_1\alpha) \cdot J = I_2 \cdot J$. As $\mathcal{O}$ is a commutative ring, $(I_1\alpha) \cdot J = (I_1 \cdot J)\alpha$. We also note the nonproper ideal $\mathcal{O} \sim I$ for any principal ideal I, whence the set has an identity element. By Claim 3.27, this commutative monoid is a group. □

There are more nice properties of this abelian group. We will see that the ideal classes in fact form a finite abelian group. For finiteness, we need to do a bit of work. First we examine the embeddings of a number ring in $\mathbb{R}$ and in $\mathbb{C}$, and then we use what we know about ideal classes of Dedekind domains (namely, that they

are generated by prime ideals) to bound the number of distinct ideal classes. We will make use of an analytic result due to Minkowski about lattices to deduce some facts about an arbitrary number ring.

Before we define an abstract lattice, let us consider a concrete embedding of $\mathbb{Q}\left[\sqrt{2}\right]$, for this will give us an embedding of $\mathbb{Z}\left[\sqrt{2}\right]$. As $\mathbb{Q}\left[\sqrt{2}\right]$ is a quadratic number field, there are precisely two embeddings of it in $\mathbb{C}$. Because both of these embeddings are actually contained in $\mathbb{R}$, it makes sense to embed $\mathbb{Z}\left[\sqrt{2}\right]$ into $\mathbb{R}^2$.

Observation 4.5. The embedding $\varphi : \mathbb{Z}\left[\sqrt{2}\right] \to \mathbb{R}^2$ by $a + b\sqrt{2} \mapsto (a + b\sqrt{2}, a - b\sqrt{2})$ preserves the norm of an element. We see that the image of $\mathbb{Z}\left[\sqrt{2}\right]$ forms a discrete subgroup of $\mathbb{R}^2$; also the index $\left[\mathbb{Z}^2 : \mathbb{Z}\left[\sqrt{2}\right]\right]$ is finite.

More generally, for a number field K of degree n, there are n embeddings $K \to \mathbb{C}$. For every embedding σ, if $i : \mathbb{C} \to \mathbb{C}$ is complex conjugation, then $i \cdot \sigma$ is another embedding. Furthermore, $i \cdot \sigma = \sigma$ if and only if $\sigma(K) \subset \mathbb{R}$. Therefore there are an even number r' of complex embeddings (i.e. not contained in $\mathbb{R}$). Let $2r_2 = r'$ and let r_1 be the number of embeddings $\sigma_1, \dots, \sigma_{r_1}$ so that $\sigma_i(K) \subset \mathbb{R}$. If we write the complex embeddings $(\sigma_{r_1+1}, \dots, \sigma_{r_1+2r_2})$ so that $i \cdot \sigma_i = \sigma_{i+r_2}$ for $i \in \{r_1+1, \dots, r_1+r_2\}$, then the every (ordered) list of embeddings $(\sigma_1, \dots, \sigma_{r_1+2r_2})$ is in one to one correspondence with the (ordered) list of embeddings $\sigma_1, \dots, \sigma_{r_1+r_2}$. We can thus consider the injective ring homomorphism $\sigma : K \to \mathbb{R}^{r_1} \times \mathbb{C}^{2r_2}$ by $x \mapsto (\sigma_1(x), \dots, \sigma_{r_1+r_2}(x))$.

Definition 4.6. We call σ the *canonical embedding of a number field.*

As an $\mathbb{R}$-normed vectorspace, $\mathbb{R}^{r_1} \times \mathbb{C}^{r_2} \simeq \mathbb{R}^n$. Therefore the canonical embedding of a number field can be considered as lying in the Banach space $\mathbb{R}^n$.

Definition 4.7. A *lattice* $\Gamma \subset \mathbb{R}^n$ is an additive subgroup which is discrete and in which $\mathbb{R}^n/\Gamma$ is compact with respect to the quotient topology.

Just as we saw in observation 3.12, that $\mathbb{Z}\left[\sqrt{2}\right]$ was a $\mathbb{Z}$ order of $\mathbb{Q}\left[\sqrt{2}\right]$, we will see that the image of $\mathbb{Z}\left[\sqrt{2}\right]$ is a lattice of $\mathbb{R}^2$. We would like that every number ring of a number field of degree n embeds to a lattice of R^n.

Claim 4.8. *$\Gamma < \mathbb{R}^n$ is a lattice if and only if there is $v_1, \dots, v_n \in \mathbb{R}^n$ so that $\Gamma = \mathbb{Z}v_1 \oplus \cdots \oplus \mathbb{Z}v_n$.*

Proof. $\Leftarrow$ Clearly Γ is an additive discrete subgroup. $\bigoplus_{i=1}^{n} ([0,1]v_i) = C$ is compact because it is a closed and bounded subset of $\mathbb{R}^n$. Since $\pi : \mathbb{R}^n \to \mathbb{R}^n/\Gamma$ is continuous, $\pi(C)$ is compact. $\pi(C) = \mathbb{R}^n/\Gamma$ shows the quotient is compact.

$\Rightarrow$ We induct on n. If $\Gamma < \mathbb{R}$ a lattice, then Γ has a positive element (otherwise $\mathbb{R}/\Gamma$ would not be compact). If the positive elements of Γ are not well ordered then any positive element $v \in \Gamma$ has infinitely many positive members of Γ less than it. By compactness, there is a limit point of Γ, contradicting the discreteness of Γ. Therefore the positive elements of Γ are well-ordered.

Let $v \in \Gamma$ be the least positive element. Then $\mathbb{Z}v \subset \Gamma$. If $w \in \Gamma \backslash \mathbb{Z}v$, then $\mathbb{Z}w \subset \Gamma$. Using the Euclidean Algorithm, there is $q, r \in \mathbb{N}$ so that $r < v$ and $w = qv + r$. Then $r \in \Gamma$ contradicts v as the least lattice point.

Γ contains a basis for $\mathbb{R}^n$ as an $\mathbb{R}$-vector space. If not, there is a vector $v \in \mathbb{R}^n$ so that $\mathbb{R}v$ is disjoint from Γ. Then, by discreteness, Γ is bounded away from $\mathbb{R}$, whence there is a cylinder of infinite length which injects isometrically into $\mathbb{R}^n/\Gamma$, showing that the quotient is not compact.

Assume the statement holds for $n-1$. Γ contains a basis for a subspace $A \simeq \mathbb{R}^{n-1}$. Then $A \cap \Gamma = A_1$ is a lattice, whence there is $v_1, \ldots, v_{n-1}$ so that $A_1 = \mathbb{Z}v_1 \oplus \cdots \oplus \mathbb{Z}v_{n-1}$. Let λ be the orthogonal complement of A. Consider the projection $\pi : \Gamma \to \lambda$. Write $A_2 = \lambda \cap \Gamma$. We will show this projection is discrete, first though, we'll show Γ is finitely generated.

Pick $w_1, \ldots, w_n \in \Gamma$ an $\mathbb{R}$-basis of $\mathbb{R}^n$. Then for $\gamma \in \Gamma$, there are $\alpha_i \in \mathbb{R}$ so that $\gamma = \sum_{i=1}^n \alpha_i w_i$. As is standard, we write $\{\alpha_i\}$ to denote the fractional part of α_i. Then if $\alpha_i \notin \mathbb{Q}$, for all $p \in \mathbb{N}$, $\sum_{i=1}^n \{p\alpha_i\} w_i \in \bigoplus_{i=1}^n [0,1] w_i$, the (compact) unit cube. As the intersection of a compact set and a discrete set is finite, there are finitely many $\sum_{i=1}^n \{p\alpha_i\} w_i$. Therefore, there are distinct $p, q \in \mathbb{Z}$ so that $\{p\alpha_i\} = \{q\alpha_i\}$ i.e. there are $m, n \in \mathbb{Z}$ so that $p\alpha_i - m = q\alpha_i - n$ whence $\alpha_i \in \mathbb{Q}$. We conclude $\Gamma \subset \mathbb{Q}w_1 \oplus \cdots \oplus \mathbb{Q}w_n$ and there is a countable generating set $A = \{a_{i,j}/b_{i,j} w_i\}$ of Γ with $a_{i,j}, b_{i,j} \in \mathbb{Z}$, and $a_{i,j}, b_{i,j}$ relatively prime. We can further specify that $a_{i,j} < b_{i,j}$, as we know $w_i \in \Gamma$. But, again, $A \subset \bigoplus_{i=1}^n [0,1] w_i$, whence A is finite.

$\pi(\Gamma)$ is discrete. If not, there is a sequence x_n in $A_1 \oplus A_2$ so that 0 is a limit point of $\pi(x_n)$. Then, for every $n \in \mathbb{N}$, we can translate x_n so that the A_1 component is zero. Therefore 0 is a limit point of Γ, contradicting discreteness. Hence $\pi(\Gamma)$ is in fact a lattice of λ.

Then there is $v_n \in \Gamma$ so that $\pi(v_n)$ is closest to 0, whence by the above argument $\mathbb{Z}\pi(v_n) = \pi(\Gamma)$. Therefore Γ is contained in the $\mathbb{Z}$ span of $v_1, \ldots, v_n$. □

We imagine the lattice to be a tessellation of an n-parallelepiped. Thus it makes sense to define the volume of the lattice to be the volume of that parallelepiped. Allow μ to denote the Lebesgue measure on $\mathbb{R}^n$.

Definition 4.9. $F \subset \mathbb{R}^n$ is a *fundamental set* of Γ if F is measurable and the natural map $\coprod_{\gamma \in \Gamma} F + \gamma \to \mathbb{R}^n$ is a bijection.

As every lattice has a $\mathbb{Z}$-basis, it also has a fundamental set, e.g. take $F = [0,1]v_1 \oplus \cdots \oplus [0,1]v_n$.

Fact 4.10. If F_1, F_2 are fundamental sets for Γ then $\mu(F_1) = \mu(F_2)$

Proof. For any measurable $S \subset \mathbb{R}^n$, $S = \coprod_{\gamma \in \Gamma} (F_1 + \gamma) \cap S$. Thus

$$\mu(S) = \mu\left(\sum_{\gamma \in \Gamma} (F_1 + \gamma) \cap S\right) = \mu\left(\sum_{\gamma \in \Gamma} F_1 \cap (S - \gamma)\right) \tag{4.1}$$

$$\text{Then} \qquad \mu(F_2) = \mu\left(\sum_{\gamma \in \Gamma} F_1 \cap (F_2 - \gamma)\right)$$

$$\text{and, by } \gamma \mapsto -\gamma, \qquad = \mu\left(\sum_{\gamma \in \Gamma} F_1 \cap (F_2 + \gamma)\right) = \mu(F_1). \qquad \square$$

Now we know that it makes sense to define the volume of a lattice $\mu(\mathbb{R}^n/\Gamma)$ as the measure of its fundamental set.

Definition 4.11. Given number field K with $\mathbb{Q}$-basis $v_1, \ldots, v_n$, the *discriminant* of K is $\left(|\det(\sigma_i(v_j))_{i,j=1}^n|\right)^2$.

Fact 4.12. A $\mathbb{Z}$-order, A, of an n dimensional number field K embeds in $\mathbb{R}^n$ as a lattice. Furthermore, if d is the discriminant of K, then $\mu(\sigma(A)) = 2^{-r_2}\sqrt{|d|}$.

Proof. Given a $\mathbb{Z}$-order, A, of a number field K, from observation 3.15 we see that A is a Z-module of rank n: let $v_1, \dots, v_n$ be the generating set of A. Consider the canonical embedding of K, $\sigma K \to \mathbb{R}^n$. Considering the matrix of σ according to the generating set,

$$\sigma = \begin{pmatrix} \sigma_1(v_1) & \dots & \sigma_1(v_n) \\ \vdots & & \vdots \\ \sigma_{r_1}(v_1) & \dots & \sigma_{r_1}(v_n) \\ \Re(\sigma_{r_1+1}(v_1)) & \dots & \Re(\sigma_{r_1+1}(v_n)) \\ \Im(\sigma_{r_1+1}(v_1)) & \dots & \Im(\sigma_{r_1+1}(v_n)) \\ \vdots & & \vdots \\ \Re(\sigma_{r_1+r_2}(v_1)) & \dots & \Re(\sigma_{r_1+r_2}(v_n)) \\ \Im(\sigma_{r_1+r_2}(v_1)) & \dots & \Im(\sigma_{r_1+r_2}(v_n)) \end{pmatrix} = M$$

With $\Re(z)$ (respectively $\Im$) denoting the real (respectively imaginary) projection of $z \in \mathbb{C}$, we note $\Re(z) = \frac{1}{2}(z + \bar{z})$, and $\Im(z) = \frac{1}{2i}(z - \bar{z})$. By the alternating multi-linearity of the determinant, $\det(M) = (2i)^{-r_2}\det(\sigma_i(v_j))_{i,j=1}^n$. By the linear independence of characters of a group, we see $\det(\sigma_i(v_j))_{i,j=1}^n \neq 0$, hence $\{\sigma(v_1), \dots, \sigma(v_n)\}$ is a linearly independent set in $\mathbb{R}^n$. Then, by claim 4.8, we see $\sigma(A) = \mathbb{Z}(\sigma(v_1) \oplus \dots \oplus \mathbb{Z}(\sigma(v_n)$ is a lattice of $\mathbb{R}^n$. Furthermore, noting the volume of lattice is the determinant of the embedding finishes the proof. □

Corollary 4.13. A number ring of a number field with r_2 $\mathbb{C}$-embeddings not contained in $\mathbb{R}$, being a $\mathbb{Z}$-order of a number field, embeds to a lattice with volume $2^{-r_2}\sqrt{|d|}$.

Now that we have calculated the volume of the lattice into which a number ring embeds, we would like to calculate the volume of the lattice into which an ideal of a number ring embeds. We will then use this calculation to deduce the finiteness of the ideal class group.

Corollary 4.14. An ideal of a number ring, $I \triangleleft R$, embeds to a lattice $\|I\|$ the size of the number ring.

Proof. An ideal of a number ring will embed to a rank n torsion-free $\mathbb{Z}$-module, hence a lattice, by the preceding fact 4.12. The image of I under the embedding into $\mathbb{R}^n$ will still have index $[R : I]$: we can then find a fundamental set of the lattice of I composed of $[R : I]$ copies of the fundamental set of the lattice of R. □

Lemma 4.15 (Minkowski)**.** *For a lattice $\Gamma < \mathbb{R}^n$, if $C \subset \mathbb{R}^n$ a symmetric convex measurable subset with $\mu(C) > 2^n\mu(\mathbb{R}^n/\Gamma)$, then $C \cap \Gamma$ is nonzero.*

Proof. Clearly $\mu(\frac{1}{2}C) = \frac{1}{2^n}\mu(C) > \mu(\mathbb{R}^n/\Gamma)$. For $F \subset \mathbb{R}^n$, a fundamental set, and $S = \frac{1}{2}C$, we can apply the computation of (4.1) of fact 4.10.

$$\mu(F) < \mu(\frac{1}{2}C) \quad = \quad \sum_{\gamma\in\Gamma} \mu(F \cap (\frac{1}{2}C - \gamma))$$

From this we conclude that the $\mu(F \cap (\frac{1}{2}C - \gamma))$ are not disjoint—hence there are distinct $\gamma_1, \gamma_2 \in \Gamma$ so that $F \cap (\frac{1}{2}C - \gamma_1) \cap (\frac{1}{2}C - \gamma_2) \neq \emptyset$. In particular, there

are $c_1, c_2 \in C$ so that $\frac{1}{2}c_1 - \gamma_1 = \frac{1}{2}c_2 - \gamma_2$. As C is symmetric, $-c_2 \in C$; and as C is convex, $\frac{1}{2}(c_1 + (-c_2)) = c \in C$. But $0 \neq c = \gamma_2 - \gamma_1 \in \Gamma$, completing the lemma. □

It has been shown that embedding an ideal of a number ring of an n-dimensional number field into $\mathbb{R}^n$ gives a lattice. We have, furthermore, calculated the volume of the lattice in terms of the index of the ideal and the volume of the lattice of the number ring, which has been explicitly calculated. If we can show that there is an ideal in every ideal class of relatively small index, we can bound the size of the lattices of the ideal classes. We then, will only have to show that there are finitely many ideals of a given index. To do this, we must calculate the volume of a convex, symmetric subset of $\mathbb{R}^n$ of diameter $t \in \mathbb{R}$.

Observation 4.16. For $r_1, r_2 \in \mathbb{N}$ so that $r_1 + 2r_2 = n$ and $t \in \mathbb{R}$, the set $B_t = \{(x_1, \ldots, x_{r_1}, y_1, z_1, \ldots, y_{r_2}, z_{r_2}) \in \mathbb{R}^n | \sum_{i=1}^{r_1} |x_i| + \sum_{j=1}^{r_2} \sqrt{y_1^2 + z_1^2} \leq t\} \subset \mathbb{R}^n$ is convex and symmetric. Furthermore, $\mu(B_t) = 2^{r_1} \left(\frac{\pi}{2}\right)^{r_2} \frac{t^n}{n!}$.

Proof Sketch. Convexity and symmetry follow, as the ball around the origin of radius t in $\mathbb{R}^{r_1} \times \mathbb{C}^{r_2}$ is convex and symmetric. The volume of the ball is an elementary exercise in multi-variable calculus. □

Lemma 4.17. *For K a number field of degree n with r_1 real embeddings and r_2 complex embeddings, with number ring $\mathcal{O}$, d the absolute value of the discriminant, and $0 \neq I \triangleleft \mathcal{O}$, then there is $0 \neq x \in I$ so that*

$$|N(x)| \leq \left(\frac{4}{\pi}\right)^{r_2} \frac{n!}{n^n} \sqrt{|d|} \|I\| \tag{4.2}$$

Proof. Given the canonical embedding of K, σ, we consider the ball of radius $t \in \mathbb{R}$ around the origin, B_t from 4.16. We make the ball big enough so that a nonzero lattice point of I is guaranteed to be in B_t, by Minkowski's Lemma 4.15. That is, there is $t \in \mathbb{R}$ so that $\mu(B_t) = 2^n(\mu(\sigma(I))$. We have calculated $\mu(B_t)$ and $\mu(\sigma(I))$:

$$2^{r_1} \left(\frac{\pi}{2}\right)^{r_2} \frac{t^n}{n!} = 2^n 2^{-r_2} \sqrt{|d|} \|I\|.$$

We conclude that $t^n = 2^{n-r_1} \pi^{-r_2} n! \sqrt{|d|} \|I\|$. Applying Minkowski's Lemma, there is $0 \neq x \in I$ so that $\sigma(x) \in B_t$. Furthermore, $|N(x)| = \prod_{\sigma_i \in \mathrm{Emb}_{\mathbb{C}}(K)} |\sigma_i(x)| = \prod_{i=1}^{r_1} |\sigma_i(x)| \prod_{j=1}^{r_2} |\sigma_j(x)|^2$. By the arithmetic-geometric mean inequality, we see $|N(x)|^{\frac{1}{n}} \leq \frac{1}{n} \sum_{i=1}^{r_1} |\sigma_i(x)| + \frac{2}{n} \sum_{j=1}^{r_2} |\sigma_j(x)| \leq \frac{t}{n}$, since $x \in B_t$. Therefore, $|N(x)| \leq \left(\frac{t}{n}\right)^n$, and $|N(x)| \leq n^{-n} 2^{n-r_1} \pi^{-r_2} n! \sqrt{|d|} \|I\|$. We have shown that x has sufficiently small norm. □

Corollary 4.18. With notation as above, for every ideal class $\mathfrak{a}$ of $\mathcal{O}$, there is an $I \in \mathfrak{a}$ so that $\|I\| \leq \left(\frac{4}{\pi}\right)^{r_2} \frac{n!}{n^n} \sqrt{|d|}$.

Proof. Consider $I \in \mathfrak{a}^{-1}$. We can scale I by $k \in K$ so that $I' = (kI)^{-1} \subset \mathcal{O}$; note: kI may not be in $\mathcal{O}$. In fact, if $I \subsetneq \mathcal{O}$, then $k \notin \mathcal{O}$, $k^{-1} \in \mathcal{O}$ and $k\mathcal{O} \supset \mathcal{O}$. Then we say $\|II'\| = 1$. By lemma 4.17, there is $0 \neq x \in I'$ so that x has minimal norm; it is guaranteed to be small as in 4.2. Then $J = xI' \in \mathfrak{a}$, and $\|J\| = N(x)\|I'\| \leq \left(\frac{4}{\pi}\right)^{r_2} \frac{n!}{n^n} \sqrt{|d|} \|I\| \|I'\| = \left(\frac{4}{\pi}\right)^{r_2} \frac{n!}{n^n} \sqrt{|d|} \|II'\|$. We conclude $\|I'\| \leq \left(\frac{4}{\pi}\right)^{r_2} \frac{n!}{n^n} \sqrt{|d|}$, whence we have found an ideal of small norm in $\mathfrak{a}$. □

Theorem 4.19. *A number ring has finite class number.*

Proof. By corollary 4.17, every ideal class contains an ideal of norm less than some positive integer. We now recall fact 3.32, that there are only finitely many ideals of a given norm. This combined shows there can be only finitely many ideal classes. □

We finish the exposition with a brief calculation, demonstrating the strength of the afore built machinery.

Fact 4.20. $\mathbb{Z}\left[\frac{1+\sqrt{17}}{2}\right]$, the number ring of $\mathbb{Q}\left[\sqrt{17}\right]$, is a PID.

Proof. The discriminant of this field is 17 and Minkowski's bound gives us that in every equivalence class, there is an ideal of norm $\leq \frac{1}{2}\sqrt{17} \sim 2.06$. Therefore, we only need to consider ideals of norm 2. We naively factor 2:

$$2 = \frac{17-9}{4} = \frac{(3-\sqrt{17})}{2}\frac{(3+\sqrt{17})}{2}$$

That $\frac{(3+\sqrt{17})}{2}$ has norm 2 implies it is irreducible. Given a prime ideal of norm 2, it would contain 2, hence it would contain $\frac{(3\pm\sqrt{17})}{2}$. But a prime ideal containing $\frac{(3\pm\sqrt{17})}{2}$ and having the same index as the principal ideal $\left(\frac{(3\pm\sqrt{17})}{2}\right)$ means that the prime ideal was principal. Therefore all prime ideals are principal. □

References

[1] M. Nori. Notes from lectures on Algebraic Number Theory, 2007. University of Chicago.

[2] D. Marcus. *Number Fields*. Springer-Verlag, 1977, New York.

[3] S. Lang. *Algebra*. Springer-Verlag, 2002, New York. Rev. 3rd ed.

[4] W. Stein. *A Brief Introduction to Classical and Adelic Algebraic Number Theory*. http://modular.fas.harvard.edu/papers/ant/html/node11.html.

[5] P. Samuel. *Algebraic Theory of Numbers*. Kershaw Publishing Co. 1971, London. trans. A. Silberger.