Rings of Algebraic Integers as Dedekind Domains

An Introduction

Horace Fusco, Shuhang Xue (Phone 507-581-6970)

Dr. Mark Krusemeyer
Carleton College
October 16, 2022

Contents

1 Preliminaries

1.1 Norm and Trace

Begin our discussion of the norm of a field extension.

Let $\mathbb{Q} \subseteq F \subseteq \mathbb{C}$ be a field extension where F is an algebraic number field. Suppose $\alpha_1, ..., \alpha_n$ is a basis for F over $\mathbb{Q}$. Now take some element $\alpha \in F$. We can multiply α by each of the basis vectors, and then expand in terms of our basis to get $\alpha\alpha_i = \sum_{1 \le j \le n} q_{ij}\alpha_j$ for some scalars $q_{ij} \in \mathbb{Q}$. For our given element $\alpha \in F$, these scalars form a matrix

$$A_\alpha = \begin{bmatrix} q_{11} & \cdots & q_{1n} \\ \vdots & \ddots & \vdots \\ q_{n1} & \cdots & q_{nn} \end{bmatrix}$$

This matrix is a function of α, and we can use it to define some useful functions of α.

Definition 1.1. For the field extension described above, the *norm* of an element $\alpha \in F$, we define $N_{F|\mathbb{Q}}(\alpha)$ as $\det(A_\alpha)$; and we define $t_{F|\mathbb{Q}}(\alpha)$ as the trace of A_α.

To see that this function is well defined, we need to mention that we are only using the vector space properties of the field extension, and in general the determinant and trace of a matrix are independent of the choice of basis from linear algebra. We should now mention a few other important insights from linear algebra that will be useful later.

Definition 1.2. Continuing to use n for the degree of $\mathbb{Q} \subseteq F$, for a general n-tuple of elements in F, $\alpha_1, ..., \alpha_n$, we define the *discriminant* $\Delta(\alpha_1, ..., \alpha_n)$ by forming a matrix out of $t_{F|\mathbb{Q}}(\alpha_i\alpha_j)$ for each product $\alpha_i\alpha_j$, call it A, and setting $\Delta(\alpha_1, ..., \alpha_n) = \det(A)$.

Remark 1.3. Here, we note that for a splitting field, this general definition agrees with the in-class definition of the norm and trace. However, for non-splitting field (not enough automorphism), they are not equal. One can easily see through the counterexample $\mathbb{Q}(\sqrt[3]{2})$.

Proposition 1.4. *Suppose $\alpha_1, ..., \alpha_n$ and $\beta_1, ..., \beta_n$ are bases for $F \supset \mathbb{Q}$. Let $\alpha_i = \sum_j a_{ij}\beta_j$. Then, $\Delta(\alpha_1, ..., \alpha_n) = \det(a_{ij})^2\Delta(\beta_1, ..., \beta_n)$.*

Proof. We first express a product of two basis vectors $\alpha_i\alpha_k$ using a double sum for the product of their expansions in the β-basis:

$$\alpha_i\alpha_k = \sum_j \sum_l a_{ij}a_{kl}\beta_j\beta_l$$

.

We can take the trace of both sides of this identity when we compute the product for every pair of basis vectors, and form the following matrices

$$A = (t_{F|\mathbb{Q}}(\alpha_i\alpha_j))$$

$$B = (t_{F|\mathbb{Q}}(\beta_j\beta_l))$$

$$C = (a_{ij})$$

We can use the symmetry of the double sum expression above to find $A = C^TBC$. It is known from linear algebra that $\det(C) = \det(C^T)$, so we now have $\det(A) = \det(C)^2\det(B)$. If we apply our definition of discriminant, this expression becomes exactly the desired result. □

1.2 Algebraic Number Fields and Rings of Algebraic Integers

Definition 1.5. For a field extension $\mathbb{Q} \subseteq F \subseteq \mathbb{C}$, we say F is an *algebraic number field* if $|F : \mathbb{C}|$ is finite.

Definition 1.6. We say an element, $c \in \mathbb{C}$ is an *algebraic integer* if c is integral over the ring $\mathbb{Z}$, which is to say if c is the root of monic polynomial with integer coefficients.

It happens that the algebraic integers in the complex numbers form a ring. To see the algebraic numbers (roots of polynomials with integer coefficients that aren't necessarily monic) form a ring, we can use the tower law, and the proof that the algebraic integers form a ring is similar, but in the interest of space we will state this as a proposition without proof.

Proposition 1.7. *The set of algebraic integers, $\Omega \subseteq \mathbb{C}$ is a ring. Furthermore for an extension $\mathbb{Q} \subseteq F \subseteq \mathbb{C}$, the algebraic integers contained in F, denoted $D := F \cap \Omega$ is a ring. We call this ring the* ring of integers *over the algebraic number field F.*

Here, we will have two quick examples on what rings of integers may look like.

Example 1.8.

(i) *$\mathbb{Z}$ the integer ring is a ring of integers.* We trivially observe $\mathbb{Q} \cap \Omega = \mathbb{Z}$; in other words, the elements of $\mathbb{Q}$ with integer coefficient minimal polynomial over Q are exactly integers.

(ii) *The Gaussian integers $\mathbb{Z}[i]$ is a ring of integers.* First, since i has minimal polynomial x^2+1, we note that $\mathbb{Z}[i]$ is a subring of the ring of integer of $\mathbb{Q}(i)$.

Conversely, we let $\alpha = a + bi$ be an element of $\mathbb{Q}(i)$ with $b \neq 0$. We note that it has minimal polynomial $x^2 - 2ax + b^2 + a^2$. Here, to make sure that the minimal polynomial $x^2 - 2ax + b^2 + a^2$ has integer coefficients, at the first sight, it seems that we can let a be a multiple of $1/2$.

However, if a is indeed of fraction expression ($a = k/2$ with k odd), then $b^2 + a^2$ will never be integers. Indeed, we have $a^2 = k^2/4$ with nominator equal to 1 mod 4. Then, b^2 in the cleanest form must have a denominator 4, and a nominator equal to 3 mod 4, which is impossible since $1^2 \equiv 1 \mod 4, 2^2 \equiv 0 \mod 4, 3^2 \equiv 1 \mod 4$, and $0^2 \equiv 0 \mod 4$.

Then, a has to be integer and b has to be integer as well, which completes the proof that $\mathbb{Z}[i]$ is the ring of integers of $\mathbb{Q}(i)$.

In the above two examples, we notice that rings of integers are both finitely generated as a $\mathbb{Z}-$module. Indeed, this observation is true in general. We proceed to prove this fact with the following lemma.

Lemma 1.9. *For $\beta \in F$, there is some integer $b \in \mathbb{Z}$ such that $b\beta \in D$*

Proof. Because the degree $|F : \mathbb{Q}|$ is finite, we know that β satisfies some minimal polynomial $p(X) \in \mathbb{Q}[X]$, where we can multiply through by the product of the denominators of its coefficients to find a polynomial in $\mathbb{Z}[X]$ which still has β as a root. Thus we may assume $p(X) = a_n x^n + a_{n-1}X^{n-1} + ... + a_0 \in \mathbb{Z}[X]$, with $a_n\beta^n + a_{n-1}\beta^{n-1} + ... + a_0 = 0$. The algebraic integers are roots of monic polynomials in $\mathbb{Z}[X]$, so we can multiply this latter expression by a_n^{n-1} to find $(a_n\beta)^n + a_{n-1}(a_n^{n-1}\beta)^{n-1} + ... + a_0 a_n^{n-1} = 0$, and thus that $a_n\beta$ is a root of the monic polynomial $q(X) = X^n + a_{n-1}X^{n-1} + a_{n-2}a_n X^{n-2} + ... + a_0 a_n^{n-1} \in \mathbb{Z}[X]$ and therefore we have our $b := a_n \in Z$ such that $b\beta \in D$. □

Proposition 1.10. *Given an ideal $A \subseteq D$, there is a basis for $F \supseteq \mathbb{Q}$ contained in A.*

Proof. First we take a general basis $\alpha_1, .., \alpha_n$ for F over $\mathbb{Q}$. Then we observe that for each element α_i, by Lemma 1.9 we have an integer b_i such that $\beta_i b_i \in D$. So let $b := \prod b_i$ making $b\alpha_1, ..., b\alpha_n \in D$, and take some element $\alpha \neq 0 \in A$, this gives a new set $\alpha b\alpha_1, ..., \alpha b\alpha_n \in A$ which must also be a basis for F over $\mathbb{Q}$, since we have only multiplied the original basis by the nonzero scalar αb. □

Proposition 1.11. *For an ideal $A \subseteq D$ where $\alpha_1, ..., \alpha_n \in A$ is a basis for $F \supseteq \mathbb{Q}$ such that $|\Delta(\alpha_1, ..., \alpha_n)|$ is minimal. Then $A = \alpha_1\mathbb{Z} + ... + \alpha_n\mathbb{Z}$. In other words, A is a finitely generated $\mathbb{Z}-$module.*

Proof. First, we posit that the absolute value of the discriminant of a basis in A is a non-negative integer (which is believable, but which we won't prove here), so we may choose a specific set of basis elements so that the discriminant is minimal. Specifically, we call this set of basis element $\{\alpha_1, ..., \alpha_n\} \subset A$ with the minimal discriminant.

Next, we let $\alpha \in A$ and write α with respect to the basis of our choice; i.e.,

$$\alpha = \sum_{i=1}^{n} \gamma_i \alpha_i, \text{ where } \gamma_i \in \mathbb{Q}.$$

Then, notice that we need to show that each $\gamma_i \in \mathbb{Z}$. Towards a contradiction, suppose not so that there exists $\gamma_i \notin \mathbb{Z}$. Without loss of the generality, we may assume that $\gamma_1 \in \mathbb{Q} - \mathbb{Z}$.

Then, we may truncate the integer part of γ_1 to write $\gamma_1 = m + \theta$, where $m \in \mathbb{Z}$ and $0 < \theta < 1$. With m, we may create another basis in A of F over $\mathbb{Q}$, namely $\beta_1 = \alpha - m\alpha_1, \beta_2 = \alpha_2, ..., \beta_n = \alpha_n$. We claim that $\beta_1, ..., \beta_n$ is a basis of F over $\mathbb{Q}$. Indeed, the linear independence of $\beta_2, ..., \beta_n$ is clear by assumption. To see that β_1 is linearly independent from other $\beta_i' s$, we suppose not so that there exists $c_i \in F$ not all nontrivial so that

$$c_1(\alpha - m\alpha_1) + c_2\alpha_2 + ... + c_n\alpha_n = 0.$$

Then, we can distribute α into its linear combination of α_i to obtain the contradiction that $\alpha_1, ..., \alpha_n$ are linearly dependent. Thus, the claim is proved with the straightforward observation that $\beta_1 = \alpha - m\alpha_1 \in A$.

Furthermore, we need to find the matrix of change of basis, namely $\{a_{ij}\}$ mentioned in Proposition 1.4. Indeed, we note that $\beta_1 = \theta\alpha_1 + \gamma_1\alpha_2 + ... + \gamma_n\alpha_n$ so that the first row is $(\theta \;\; \gamma_1 \;\; \gamma_2 \;\; ... \;\; \gamma_n)$. For any other $\beta_i = \alpha_i$, the $i - th$ has 1 at the $i - th$ column and 0 anywhere else. Thus, we notice that the determinate of this upper-diagonal matrix $\{a_{ij}\}$ is exactly θ.

Finally, we apply Proposition 1.4 to notice that $\Delta(\beta_1, ..., \beta_n) = \theta^2\Delta(\alpha_1, ..., \alpha_n) < \Delta(\alpha_1, ..., \alpha_n)$, since $0 < \theta < 1$, which is the desired contradiction with the choice of $\alpha_1, ..., \alpha_n$ minimizing the discriminant. □

With the above proposition, we know that all rings of integers are finitely generated $\mathbb{Z}-$module. However, we don't know the number of generators and what those generators look like. In the next example, we see that the rings of integers of $\mathbb{Q}(\sqrt{5})$ and $\mathbb{Q}(\sqrt{-5})$ have completely different forms.

Example 1.12. Further examples of rings of integers.

(i) For $F = \mathbb{Q}(\sqrt{5})$, $D = \mathbb{Z}[\frac{1+\sqrt{5}}{2}]$.

Proof. We first note that $\frac{1+\sqrt{5}}{2} \in \Omega \cap F$ since $x^2 - x - 1$ is its minimal polynomial.

Conversely, we see that since $\{1, \sqrt{5}\}$ is a basis of F over $\mathbb{Q}$, we write an arbitrary element of F as $\alpha = a + b\sqrt{5}$, with $b \neq 0$. Then, α has minimal polynomial $x^2 - 2ax + (a^2 - 5b^2)$. Notice that first for $-2a \in \mathbb{Z}$, we let a be an integral multiple of $1/2$. Then, it follows that any b as an integral multiple of $1/2$ will always make sure $a^2 - 5b^2 \in \mathbb{Z}$ by looking at the nominator mod 4 similar to the proof of $\mathbb{Z}[i]$ is a ring of integer. Thus, we conclude that $D = \mathbb{Z}[\frac{1+\sqrt{5}}{2}]$. □

(ii) For $F = \mathbb{Q}(\sqrt{-5})$, $D = \mathbb{Z}[\sqrt{-5}]$.

Proof. We note that similarly, the containment of $\mathbb{Z}[\sqrt{-5}] \subset D$ is trivial. Conversely, for any element of F as $\alpha = a + b\sqrt{-5}$, with $b \neq 0$, it has minimal polynomial $x^2 - 2ax + a^2 + 5b^2$. Note that if $a = k/2$, where k is some odd integer, we have $5b^2 \equiv 1 \mod 4$, which implies that the term $a^2 + 5b^2$ is never in $\mathbb{Z}$. Therefore, it has to be the case that $a \in \mathbb{Z}$ and correspondingly $b \in \mathbb{Z}$. Thus, we conclude that $D = \mathbb{Z}[\sqrt{-5}]$. □

Proposition 1.13. *If $A \subseteq D$ is an ideal then $A \cap \mathbb{Z}$ is nonempty.*

Proof. If we take some $\alpha \neq 0 \in A \subset D$, α is an algebraic integer and therefore must satisfy some monic polynomial over $\mathbb{Z}$, in other words there exist $a_{n-1}, ..., a_0 \in \mathbb{Z}$ such that $\alpha^n + a_{n-1}\alpha^{n-1} + ... + a_0 = 0 \in A$. Then, since we are in a field, we may multiply a^{-1} to both sides of the above equation so that without loss of generality, we may assume $a_0 \neq 0$. Notice now we may move a_0 to the other side to see that $a_0 \in A \cap \mathbb{Z}$. □

Proposition 1.14. *Show if A is a ideal of D, then D/A is finite.*

Proof. To show D/A is finite, we instead look at a principle ideal $\langle a \rangle \subset A$, where $a \in A \cap \mathbb{Z}$, obtained from Proposition 1.13. We notice that there is a canonical surjective homomorphism from $D/\langle a \rangle \to D/A$. Thus, it suffices to show $D/\langle a \rangle$ is finite.

First, we appeal to Proposition 1.11 to write down $D = \alpha_1\mathbb{Z} + \alpha_2\mathbb{Z} + ... + \alpha_n\mathbb{Z}$, where $\alpha_i \in D$. Let an arbitrary element $\omega \in D$. Note since $\alpha_1, ..., \alpha_n$ is also a basis of F over $\mathbb{Q}$, we can write $\omega = \sum m_i\alpha_i$, where $m_i \in \mathbb{Z}$. Then, we note that for each m_i, we may consider m_i modulo a with remainder as an integer; i.e., write $m_i = n_i a + q_i$, where $0 \leq q_i < a$ is an integer (this is the division with remainder in the ring of integers).

Then, we notice that in $D/\langle a \rangle$,

$$\overline{\omega} = \overline{\sum m_i\alpha_i} = \sum q_i\alpha_i + \langle a \rangle.$$

So far, it is already clear that for each coset in $D/\langle a \rangle$, there is an element of $\{\sum q_i\alpha_i \mid 0 \leq q_i < a, q_i \in \mathbb{Z}\}$ inside. We further claim that in each coset, there is exactly one element from $\{\sum q_i\alpha_i \mid 0 \leq q_i < a, q_i \in \mathbb{Z}\}$. In other words, $\{\sum q_i\alpha_i \mid 0 \leq q_i < a, q_i \in \mathbb{Z}\}$ is the set of representatives for cosets in $D/\langle a \rangle$.

Note that if $\sum q_i\alpha_i$ and $\sum q_i'\alpha_i$ are in the same coset, by definition, we have $\sum(q_i - q_i')\alpha_i = a\beta$ for $\exists \beta \in D$. Then, we note that since $\alpha_i's$ are linearly independent, $q_i - q_i'$ must be divisible by a. Recall here that $0 \leq q_i, q_i' < a$ so that it must be $q_i = q_i'$, which completes the proof of the claim.

In conclusion, we know that the set of representatives of coset of $\{\sum q_i\alpha_i \mid 0 \leq q_i < a, q_i \in \mathbb{Z}\}$ has finite cardinality a^n, which implies that D/A is finite. □

Definition 1.15. We say a ring is *Noetherian* if every ascending chain of ideals $A_1 \subseteq A_2 \subseteq A_3 \subseteq ...$ has some natural number $N \in \mathbb{N}$ such that $A_n = A_{n+1}$ for all $n \geq N$.

Lemma 1.16. *The ring of integers $D \subseteq F$ of an algebraic number field is a Noetherian ring.*

Proof. This follows directly from the fact that D/A is finite. Indeed, by the one-to-one correspondence between ideals containing A and ideals of D/A, we note that there are finitely many ideals containing A. □

Lemma 1.17. *Every prime ideal of D is maximal.*

Proof. Take some prime ideal $P \subseteq D$. We have by Lemma 1.14 that D/P is finite, making it a finite integral domain. For any element $a \neq 0$ in a finite integral domain, by the pigeonhole principle the sequence $1, a, a^2, a^3, ...$ must eventually repeat a value, so there exist $n < m \in \mathbb{N}$ such that $a^n = a^m$, but since we have cancellation in an integral domain, it must be that $1 = a^{m-n}$ where $m - n \geq 2$, but this means that a has the inverse a^{m-n-1}, so all finite integral domains are fields, thus D/P is a field and therefore P is maximal in D. □

Note here that using Kummer's theorem on commutative algebra, which states that a noetherian normal domain with all prime ideals being maximal is Dedekind, we can directly conclude that rings of integers has unique prime ideal factorization. However, the fact of rings of integers are normal (integrally closed) is nontrivial. Instead, we directly show the existence and uniqueness of factorization into prime ideals by studying the class number.

2 Existence of factorizations into prime ideals

2.1 Failure of unique prime factorizations in D

In this subsection, we show the failure of prime factorization in the ring of integers $\mathbb{Z}[\sqrt{-5}]$ (checked in Example 1.12). But first, we generalize our context to rings of form $\mathbb{Q}[\sqrt{d}]$ with $d \in \mathbb{Z}$ square free. Then, utilizing the norm, we prove a few lemmas to understand the units and irreducible elements in those rings.

Lemma 2.1. *For $x \in \mathbb{Z}[\sqrt{d}]$ where d is a square-free integer, $N(x) = \pm 1$ if and only if x is a unit.*

Proof. If x is a unit, then there exists some $y \in \mathbb{Z}[\sqrt{d}]$ such that $xy = 1$, then $N(x)N(y) = N(xy) = N(1) = 1$. Since $N(x), N(y)$ are both integers, the only possibility are $N(x) = \pm 1$.

On the other hand, for $x = s + t\sqrt{d} \in \mathbb{Z}[\sqrt{d}]$, if $N(x) = \pm 1$, by definition of the norm function, $(s + t\sqrt{d})(s - t\sqrt{d}) = N(x) = \pm 1$. Therefore, we have $x \cdot \bar{x} = 1$, where $\bar{x} = s - t\sqrt{d}$. Thus, we proved that x is a unit. □

Lemma 2.2. *If $d < -1$, then $\mathbb{Z}[\sqrt{d}]$ only has units ± 1.*

Proof. When $d < -1$, it suffices to solve $s^2 + lt^2 = \pm 1$, where $l = |d| > 0$. Note that the since the left hand side is positive, the right hand side can never equal to -1. Thus, by solving $s^2 + lt^2 = 1$, we deduce that $u = \pm 1$. □

Lemma 2.3. *$1 + \sqrt{-5}$ and $1 - \sqrt{-5}$ are irreducible in $\mathbb{Z}[\sqrt{-5}]$.*

Proof. The proof for $1 + \sqrt{-5}$ is almost the same to the proof for $1 - \sqrt{-5}$. Here, we only prove $1 + \sqrt{-5}$ is irreducible.

Let $a, b \in \mathbb{Z}[\sqrt{-5}]$ such that $ab = 1 + \sqrt{-5}$. Then, $N(1 + \sqrt{-5}) = 6 = N(ab) = N(a)N(b)$. Notice $N(a)$ may only be $1, 2, 3$ or 6 since the norm in $\mathbb{Z}[\sqrt{-5}]$ is positive in general. However, $N(a) \neq 2$ or 3 because the corresponding Diophantine equation $s^2 + 5t^2 = 2$, or 3 has no integer solutions. Then, either $N(a) = 1$, which implies that a is a unit, or $N(a) = 6$, which implies that b is a unit. □

Proposition 2.4. *The domain $\mathbb{Z}[\sqrt{-5}]$ is not a unique factorization domain (UFD).*

Proof. In domain $\mathbb{Z}[\sqrt{-5}]$, we observe that the element 6 has two factorizations:

$$6 = 2 \cdot 3, \qquad 6 = (1 + \sqrt{-5})(1 - \sqrt{-5}).$$

As we proved in the last lemma, $1+\sqrt{-5}$ and $1-\sqrt{-5}$ are both irreducible elements in $\mathbb{Z}[\sqrt{-5}]$. Similarly, we can show that 2 and 3 are irreducible. As an instance, let $a, b \in \mathbb{Z}[\sqrt{-5}]$ such that $2 = ab$. Then, $N(2) = 4 = N(ab) = N(a)N(b)$. Notice $N(a)$ may only be 1,2, or 4 since the norm in $\mathbb{Z}[\sqrt{-5}]$ is positive in general. However, $N(a) \neq 2$ because the corresponding Diophantine equation $s^2 + 5t^2 = 2$ has no integer solutions. Then, either $N(a) = 1$, which implies that a is a unit, or $N(a) = 4$, which implies that b is a unit.

Similarly, we use the same steps to show that 3 is also irreducible in $\mathbb{Z}[\sqrt{-5}]$. Finally, recall that the only units in $\mathbb{Z}[\sqrt{-5}]$ are ± 1. By taking the products with units, it's clear that $2, 3, 1 + \sqrt{-5}$, and $1 - \sqrt{-5}$ are not each others' associates.

Hence, $\mathbb{Z}[\sqrt{-5}]$ is not a unique factorization domain (UFD). □

2.2 Ideal Multiplication

Instead of looking at the prime factorization of elements, we look at the prime ideal factorization of ideals. In this subsection, we first aim to understand how to multiply ideals together, and deduce some important properties of ideal multiplication in rings of integers.

Definition 2.5. The **product** IJ of ideals I and J is defined to be the set of all sums of elements of the form ab, with $a \in I$ and $b \in J$; that is,

$$IJ = \{a_1b_1 + a_2b_2 + ... + a_nb_n | n \geq 1, a_k \in I, b_k \in J\}.$$

Followed from the definition, it's easy to check that the product IJ is an ideal since it's closed under subtraction and multiplication from the domain. To proceed with our program, we must state the following unobjectionable fact, whose proof would take us slightly beyond the scope of our project. We will then prove a lemma which will will aid our understanding of how ideal multiplication works in the ring D.

Note 2.6. For an ideal $A \subseteq D$ and an element $\beta \in F$, if $\beta A \subseteq A$ then $\beta \in D$.

Lemma 2.7. *For ideals $A, B \subseteq D$ such that $A = AB$, we have $B = D$.*

Proof. We can appeal to Proposition 1.11 to say that A consists of integral linear combinations of some set of elements $\alpha_1, ..., \alpha_n \in A$. Since $A = AB$, we can find elements $b_j \in B$ such that $\alpha_i = \sum_j b_{ij}\alpha_j$. We can from the matrix $B = (b_{ij} - \delta_{ij})$ where $\delta_{ij} = 1$ if $i = j$ and $\delta_{ij} = 0$ otherwise. The sums above become the matrix expression

$$B \begin{bmatrix} \alpha_1 \\ \alpha_2 \\ \vdots \\ \alpha_n \end{bmatrix} = 0$$

in other words $\det(B) = 0$, and if we write out the algebra of this expression, we find the sum of 1 and many elements in B is zero, so $1 \in B$ and therefore $B = D$.

□

Corollary 2.8. *For ideals $A, B \subseteq D$ and some $\omega \in D$ that satisfies $\langle\omega\rangle A = BA$, then $\langle\omega\rangle = B$.*

Proof. Since $\langle\omega\rangle A = BA$, if we take $\beta \in B$ and $\alpha \in A$, then we have some $a \in A$ with $\beta\alpha = \omega a$, in which case $\frac{\beta}{\omega}\alpha = a \in A$, so $\frac{\beta}{\omega}A \subset A$, and by the note above, this means $\frac{\beta}{\omega} \in D$. Consequentially, $B \subset \langle\omega\rangle$ which means $\frac{1}{\omega}B$ is an ideal in D. Now manipulating the given expression we have $A = \frac{1}{\omega}BA$, so by Lemma 2.7 we know $\frac{1}{\omega}B = D$ and subsequently $B = \langle\omega\rangle$. □

We will now define an equivalence relation on the set of ideals in the ring of integers in an algebraic number field.

Note 2.9. For two ideals A and B in the ring of integers D of an algebraic number field, the relation $A \sim B$ where A and B are related if there exists two nonzero $\alpha, \beta \in D$ with $< \alpha > A =< \beta > B$, is an equivalence relation.

Definition 2.10. The equivalence classes of the relation $\sim$ are called *ideal classes*, and the number of ideal classes is called the *class number* of F and is denoted h_F.

2.3 Finite class number of F

Before proving the following lemma, we first note the this is a generalization of a Euclidean function. Recall that a Euclidean function f on an integral domain R satisfies that for any element $a, b \neq 0 \in R$, there must exist $q, r \in R$ such that $a = bq + r$ with $f(a - bq) > f(r)$.

In our case, the generalization is weak in the sense that instead of requiring using a itself, we may use a scalar multiple (up to some scale dependent on F) of a. In the proof of the following lemma, since the norm we defined earlier is an n-dimensional notion, we exploit the distance in n-space, where n is the degree of F over $\mathbb{Q}$.

Lemma 2.11. *For some algebraic number field F, there is a positive integer $M \subseteq \mathbb{Z}$ with the following property. For $\alpha, \beta \in D$ with $\beta \neq 0$, there is some integer $1 \leq t \leq M$ and an element $\omega \in D$ such that $|N(t\alpha - \omega\beta)| < |N(\beta)|$*

Proof. We first use the multiplicative property derived by viewing N as a homomorphism between multiplicative groups. Then, to prove the desired result, we can name $\gamma = \alpha\beta^{-1}$ so that it suffices to show $|N(t\gamma - \omega)| < 1$ under the desired condition. A warning here is that γ may not necessarily in D since β^{-1} may not necessarily in D. Thus, in the following, we assume γ to be an arbitrary element of F.

We start by writing D as a finitely generated $\mathbb{Z}-$module; i.e., $D = \alpha_1\mathbb{Z} + ... + \alpha_n\mathbb{Z}$ (from Proposition 1.11). Then, we first try to find a universal bound on $|N(\gamma)|$ for $\gamma \in F$. Note that we can write $\gamma = \sum \gamma_i\alpha_i$ in term of the basis with $\gamma_i \in \mathbb{Q}$ so that we have the following bounds:

$$|N(\gamma)| = \left|\prod_i(\sum_i \gamma_i\alpha_i^{(j)})\right| \leq C(\max_i \gamma_i)^n, \tag{1}$$

where $C = \prod_j(\sum_i |\alpha_i^{(j)}|)$ by triangle inequality. To our convenience, we choose integer $m > \sqrt[n]{C}$ and let $M = m^n$.

Then, we split γ into integer parts and fractional parts. Particularly, we may write $\gamma_i = a_i + b_i$, where $a_i \in \mathbb{Z}, 0 \leq b_i < 1$. Thus, by defining

$$[\gamma] = \sum_i a_i\alpha_i, \quad \{\gamma\} = \sum_i b_i\alpha_i,$$

we obtain $\gamma = [\gamma] + \{\gamma\}$, where $[\gamma] \in D$ and $\{\gamma\}$ has rational coefficients between 0 and 1.

Here, we formalize the geometric intuition we discussed before. Define the coordinate map $\phi : F \to \mathbb{R}^n$ such that $\phi(\gamma) = (\gamma_1, \gamma_2, ..., \gamma_3)$. Then, we note that by construction, $\phi(\{\gamma\})$ is mapped inside the unit $n-$cube. We partition the unit $n-$cube into m^n sub-n-cubes with length $1/m$ on each side (easily verify that the volume is preserved so that the partition is well-defined). Then, we have for each $1 \leq k \leq m^n + 1$, we have a corresponding point $\phi(\{k\gamma\})$ inside the unit n-cube by construction (when $k = m^n + 1$, it is still inside the unit cube since m is chosen to be an integer). Next, by the pigeon-hole principle, we note that there are at least two points lie in the same sub-n-cube (including the boundary). Let's denote the corresponding elements in F as $h\gamma$ and $l\gamma$. Without loss of generality, we may assume that $h > l$. Let $t = h - l \leq m^n$ and observe

$$t\gamma = h\gamma - l\gamma = \omega + \delta,$$

where $\omega \in D$ and δ must has absolute value less than or equal to $1/m$ since two points are assumed to be in the same sub-n-cube.

Finally, we check that the with the above choice of ω and δ, we must have the desired

$$|N(t\gamma - \omega)| = |N(\delta)| \leq C(1/m)^n = C/m^n < 1.$$

□

Theorem 2.12. *The class number of an algebraic number field F is finite.*

Proof. Let A be an ideal in D. Then, since for nonzero element of A, the norm is a positive integer, we may take $\beta \neq 0 \in A$ such that $|N(\beta)|$ is minimal.

Then, by Proposition 2.11, we note that for any $\alpha \in A$, we have $1 \leq t \leq M$ such that $|N(t\alpha - \omega\beta)| < |N(\beta)|$. Therefore, it has to be the case that $t\alpha - \omega\beta = 0$ (intuitively when β has minimal functional value, it "divides" any element). Then, we note that for any $1 \leq t \leq M$, we have $t\alpha \in \langle\beta\rangle$, which implies $M!\alpha \in \langle\beta\rangle$.

Next, we try to find all equivalent ideals to A by looking at the equivalent ideals containing the "smallest" element. Define $B = \langle\beta^{-1}\rangle M!A \subset D$ and note that $\langle\beta\rangle B = M!A$. Notice that by choice, $\beta \in A$ so that $M!\beta \in \langle\beta\rangle B$, which implies that $M! \in B$ so that $\langle M!\rangle \subset B$. We recall that D is noetherian so that there are only finitely many ideals containing $\langle M!\rangle$, which implies that there are only finitely many candidates for $B \sim A$. Finally, because $\sim$ is an equivalent relation on the set of ideals of D, we note that the finiteness of B implies that the class number h_F is finite. □

2.4 Factoring Ideals

After proving the class number h_F of an algebraic number field F is finite, we can immediate exploit the "finiteness" of ideals, just like how one proves a finite integral domain is a field, a finite field has the Frobenius automorphism, and so on. In our case, we prove that every ideal raised to a power is principal.

Proposition 2.13. *For any ideal $A \subset D$, there is an integer k, $1 \leq k \leq h_F$, such that A^k is principal.*

Proof. First, we let $A \subset D$ be an arbitrary ideal. Consider the set $\{A^i \mid 1 \leq i \leq h_F + 1\}$ and note that there are at least two ideals in this set that are equivalent.

Then, without loss of generality, let's say that A^m is equivalent to A^n with $1 \leq n < m \leq h_F$. By definition, there exists $\alpha, \beta \in D$ such that

$$\langle\alpha\rangle A^n = \langle\beta\rangle A^m.$$

We let $B = A^{m-n} := A^k$ $(k = m - n)$ and claim that B is a principal ideal. First, we note the equality $\langle\alpha\rangle A^n = \langle\beta\rangle BA^n$. Then, we may move β to the other side so that $\langle\alpha\beta^{-1}\rangle A^n \subset BA^n$. Note that then $\langle\alpha\beta^{-1}\rangle A^n \subset A^n$ so we can conclude $\alpha\beta^{-1} \in D$ by definition of an ideal.

Here, we obtain the crucial equality of ideals:

$$\langle\alpha\beta^{-1}\rangle A^n = BA^n.$$

By Corollary 2.8, we finally conclude $B = \langle\alpha\beta^{-1}\rangle$ as desired.

□

Remark 2.14. Indeed, the set of ideal classes form a group with ideal multiplication. Then, the above Proposition implies that every class of ideal $\bar{A}$ has inverse $\bar{A}^{k-1}$ because the product of those is the trivial ideal class (principle ideals).

With the machinery we have built so far, we are ready to prove the generalized version of Corollary 2.8, which serves as a crucial stepping stone for giving the factorization of ideals into prime ones.

Proposition 2.15. *If A, B, C are ideals, and $AB = AC$, then $B = C$.*

Proof. Given ideals A, B, C of D and assume $AB = AC$. Then, we first recall from the last proposition that there exists $1 \leq k \leq h_F$ such that A^k is principle. Thus, we multiply A^{k-1} to the left on both sides of the equation to obtain

$$\langle\omega\rangle B = \langle\omega\rangle C.$$

Here, we note that for any $b \in B$, $\omega b \in \langle\omega\rangle C$. Thus, there exists $c \in C$ such that $\omega b = \omega c$. After multiplying ω^{-1} on both sides, we conclude that $b = c$, which implies $b \in C$. Similarly, we use a symmetric argument to conclude $B = C$. □

The next proposition is about the existence of an ideal "factor" to facilitate the proof of prime ideal factorization.

Proposition 2.16. *If A, B are ideals of D such that $B \supset A$, then there exists an ideal C such that $A = BC$.*

Proof. Recall that there exists $1 \leq k \leq h_F$ such that $B^k = \langle\omega\rangle$. Then, from $A \subset B$, we have $B^{k-1}A \subset \langle\omega\rangle$.

Then, we let $C := \langle\omega^{-1}\rangle B^{k-1}A$ and observe that C is an ideal from $\langle\omega^{-1}\rangle B^{k-1}A \subset D$. Immediately, we verify that

$$BC = B\langle\omega^{-1}\rangle B^{k-1}A = \langle\omega\rangle\langle\omega^{-1}\rangle A = A,$$

by straightforward element chasing. □

Proposition 2.17. *Every proper ideal in D can be written as a product of prime ideals.*

Proof. Let A be a proper ideal. Recall that from Zorn's lemma, A must be contained in a maximal ideal P_1 (even without Zorn's lemma, since D/A is finite, A must be contained in a maximal ideal). Then, from the last proposition on finding factors, we note that there exists an ideal B_1 such that $A = P_1 B_1$.

Then, consider two situation. If $B_1 = D$, then we are done since $A = P_1$.

If B_1 is a proper ideal of D, then we can further break down B_1 into $B_1 = P_2 B_2$ and consider whether B_2 is a proper ideal of D. Notice that this process must terminate since with this process, we have a chain of ascending ideals $A \subsetneq B_1 \subsetneq B_2$. By D being noetherian, we note that at some $n \in \mathbb{N}$, $B_n = D$. Finally, we can observe that

$$A = \prod_{1 \leq i \leq n} P_i.$$

Thus, every proper ideal in D can be written as a product of prime ideals. □

3 Uniqueness of Factorization into Prime Ideals

We are now close to being able to show the factorization into prime ideals proved above is unique. To this end we must establish a definition.

Definition 3.1. For a prime ideal P and another ideal A, we define its order under P, $\text{Ord}_P(A)$ to be the unique non-negative integer such that $A \subset P^t$ and $A \not\subset P^{t+1}$

We might suspect this integer is well defined because the chain $P \supset P^2 \supset P^3 \supset ...$ features only proper containments, since if $PP^i = P^i$ we can write $P^i = DP^i$ and conclude by Proposition 2.15 that $P = D$. We now establish a few preliminary facts about the order of an ideal.

Proposition 3.2. *Let P be a prime ideal.*

(i) $\text{Ord}_P(P) = 1$.

(ii) For some other prime ideal $P' \neq P$, $\text{Ord}_P(P') = 0$.

(iii) For two ideals $A, B \subset D$, we have $\text{Ord}_P(AB) = \text{Ord}_P(A) + \text{Ord}_P(B)$.

Proof. The first claim is more or less by definition, and because we know $P^2 \subsetneq P$. The second claim is derived from the fact that the prime ideals in D are maximal, and therefore $P' \not\subset P$. For the third claim, we must invoke Proposition 2.16, letting $t = \text{Ord}_P(A)$ and $t' = \text{Ord}_P(B)$ so that $A \subset P^t$ and $B \subset P^{t'}$ implies there exist ideals A_1, B_1 where $A = P^t A_1$ and $B = P^{t'} B_1$. Furthermore if, for instance, $A_1 \subset P$, then by the same Proposition we could pull out another factor of P, and find that $A = P^{t+1} A_2 \subset P^{t+1}$ which contradicts the definition of order. Thus $A_1 \not\subset P$ and similarly $B_1 \not\subset P$.

Now we have $AB = P^{t+t'} A_1 B_1 \subset P^{t+t'}$, and if $AB \subset P^{t+t'+1}$, then we can lean on the same proposition again to assert that $P^{t+t'} A_1 B_1 = AB = P^{t+t'+1} C = P^{t+t'} PC$ on which we can use Proposition 2.15 to argue $A_1 B_1 = PC \subset P$, and then by the primeness of P that either $A_1 \subset P$ or $B_1 \subset P$, and we have shown this not to be true. So indeed, $\text{Ord}_P(AB) = t + t' = \text{Ord}_P(A) + \text{Ord}_P(B)$. □

We now have everything we need to prove the uniqueness of a prime ideal factorization in D. We can express a finite product of ideals in the following way, $\prod P^{a(P)}$, ranging over every prime ideal in D, where $a(P)$ is some integer exponent for each P such all but finitely many of the $a(P)$ are zero. We have seen already that for every ideal A, there exists such an expression for A.

Theorem 3.3. *For every ideal $A \subset D$, expressing A as a product of prime ideals $A = \prod P^{a(P)}$, we have the $a(P)$ are uniquely determined by $a(P) = \mathrm{Ord}_P(A)$, and therefor this product representation is unique.*

Proof. Let $A = \prod P^{a(P)}$ For some prime ideal P', take the order under P' of both sides, giving

$$\mathrm{Ord}_{P'}(A) = \sum \mathrm{Ord}_{P'}(P^{a(P)}) = \sum a(P)\mathrm{Ord}_{P'}(P)$$

where we have applied the Proposition 3.2 to split apart the product and pull down the exponents. Now by the same proposition, $\mathrm{Ord}_{P'}(P) = 0$ for all $P \neq P'$ and $\mathrm{Ord}_{P'}(P') = 1$, so finally $\mathrm{Ord}_{P'}(A) = a(P')$ and we are done.

□

References

[1] Kenneth Ireland, Michael Rosen. A Classical Introduction to Modern Number Theory (1990). Chapter 6,12, and 13. Graduate Texts in Mathematics. Springer Science and Business Media, New York.

[2] Thomas W. Hungerford: Abstract Algebra: An Introduction Second Edition (1996). 2nd Edition.