Factorization of Primes, Primes, Primes: Elements, Ideals, and in Extensions

By

Peter Bonventre

****

Advisor: Karl Zimmermann

Submitted in partial fulfillment
of the requirements for
Honors in the Department of Mathematics

UNION COLLEGE

June, 2011

Abstract

It is often taken it for granted that all positive whole numbers except 0 and 1 can be factored uniquely into primes. However, if K is a finite extension of the rational numbers, and $\mathfrak{O}_K$ its ring of integers, it is not always the case that non-zero, non-unit elements of $\mathfrak{O}_K$ factor uniquely. We do find, though, that the proper ideals of $\mathfrak{O}_K$ do always factor uniquely into prime ideals. This result allows us to extend many properties of the integers to these rings. If we a finite extension L of K and $\mathfrak{O}_L$ of $\mathfrak{O}_K$, we find that prime ideals of $\mathfrak{O}_K$ need not remain prime when they are extended into $\mathfrak{O}_L$; instead, they can split into a product of prime ideals of $\mathfrak{O}_L$ in a very structured way. If L is a normal extension of K, we can use Galois theory to further study this splitting by considering the intermediate fields of K and L, as well as quotient rings of the associated rings of integers. In this paper, we will introduce these topics of algebraic number theory, prove that unique factorization of ideals holds using two different methods, and observe the patterns that arise in the splitting of prime ideals.

.

Contents

Chapter 1

Background

In grade school, once we have grasped how to manipulate numbers and use basic arithmetic, one of the first concepts we learn about is factorization of whole numbers. We can take any whole number and find a collection of these special, irreducible, "prime" numbers that when multiplied together yield our original number. Moreover, we are told that, for any whole number, this factorization into prime numbers is unique. This is a very powerful result that is exploited greatly in many fields of number theory.

More specifically, the field of algebraic number theory can be described, simply, as the study of numbers viewed algebraically. In this paper, we will be considering finite extensions of the rational numbers, referred to as number fields, and a specific subring of these fields called either the associated ring of integers or associated number ring. We will attempt to extend the properties of the integers and rationals to these number rings and number fields, respectively. In general, we find that many properties are the same and still apply: for example, the usual binary operations still make sense and work as we expect them to. The important counterexample highlighted in this paper is unique factorization of elements in the ring of integers. Unlike the regular integers, there are examples of number rings where elements have multiple factorizations into irreducibles, and thus factorization is not unique. Without uniqueness of factorization, many ideas, such as the greatest common divisor among others, no longer have a meaningful definition.

The field of algebraic number theory gained much of its prominence in attempts to prove Fermat's Last Theorem: the equation $a^n + b^n = c^n$, where $n \in \mathbb{Z}$, has no integral solutions

for a, b, and c when n is greater than 2 and $abc \neq 0$. A supposed proof was worked out in the 1800s, but it assumed certain rings of integers were unique factorization domains, which was soon shown to be a faulty assumption. Fermat's Last Theorem was finally proved in 1995 in a several hundred page paper, and involved topics ranging from algebraic geometry to elliptic curves to modular groups [For more information on the story of this proof, see Stewart and Tall [7]]. We will not go into details of all, or any, of these highly advanced topics. Instead, we will concentrate on the ideas of factorization at the beginning of the hunt for this elusive proof.

In this paper, we give an introduction to algebraic number theory, with a focus on various types of factorization in algebraic number structures. In this first chapter, we will define the terms and concepts that are necessary background for our main results. In the last section of Chapter 1 we will briefly look at the factorization of elements in number rings, and show that unique factorization cannot be taken for granted; importantly, this will require clarification of the difference between a prime number and an irreducible number. In Chapter 2 we look at a similar situation, where instead of factoring elements of a ring of integers, we are factoring ideals in that ring; we will show that in this case all ideas factor uniquely into prime ideals. Finally, in Chapter 3 we will look at towers of number structures, and observe how primes behave as they are extended through different Galois extensions.

Many of the results and discussions in this paper are based on two major works, *Number Fields* by D.A. Marcus [5] and *Algebraic Number Theory and Fermat's Last Theorem* by I. Stewart and D. Tall [7]. For our discussion, we will assume some knowledge of ring theory, specifically topics concerning ideals and quotient rings, as well as comfort with field and Galois theory. For a good introduction to these subjects, see Herstein [3], Stewart [6], or Howie [4].

1.1 Elements

The number structures we would like to consider are composed of very specific types of elements. In this section, we will define these elements, as well as some of their basic

properties.

We start with a distinction which is trivial in the integers:

Definition 1.1. An non-unit element α in a ring R is *irreducible in* R if whenever we have $\alpha = \beta\gamma$ for $\beta, \gamma \in R$, then either β or γ is a unit.

Definition 1.2. We say a non-zero, non-unit element α is *prime in* R if whenever $\alpha|\beta\gamma$, then $\alpha|\beta$ or $\alpha|\gamma$.

The following proposition follows easily:

Proposition 1.3. *Every prime element of a ring R is irreducible* [see Stewart and Tall [7] p.87].

Example 1.4. Note that in the integers, all irreducibles are also prime. This is why we typically say both of these properties define "prime" integers. We will eventually construct extensions of the integers in which this distinction becomes significant.

1.1.1 Algebraic Numbers and Algebraic Integers

We will now define and consider two particular types of complex numbers which play a major role in algebraic number theory, each of which satisfies a certain type of polynomial.

Definition 1.5. A complex number α is an *algebraic number* if it satisfies a polynomial with coefficients in $\mathbb{Q}$. The set of algebraic numbers is denoted $\mathbb{A}$.

For example, all rational numbers and integers q are clearly algebraic since they satisfy the polynomial $x - q$. Further, we can easily see that any algebraic number also satisfies a polynomial in $\mathbb{Z}$.

Moreover, the set of all algebraic numbers is a field:

Proposition 1.6. *The set of algebraic numbers $\mathbb{A}$ is a subfield of $\mathbb{C}$* [for details, see Stewart and Tall [7] p.36].

A stronger condition must hold if a complex number is to be in our second class of elements, an algebraic *integer*:

Definition 1.7. The complex number θ is an *algebraic integer* if it satisfies a monic polynomial with coefficients in $\mathbb{Z}$. The set of algebraic integers is denoted $\mathbb{B}$.

For example, we have that $\theta_1 = \sqrt{-5}$ is an algebraic integer since it satisfies the polynomial $t^2 + 5$; similarly $\theta_2 = \frac{1}{2}(1 + \sqrt{5})$ is an algebraic integer since it satisfies $t^2 - \theta - 1$. However, the rational number $\theta_3 = 22/7$ is *not* an algebraic integer, since it only satisfies polynomials such as $7t - 22$ or $t - 22/7$; it does not satisfy any monic polynomials over the integers.

Clearly any algebraic integer is also an algebraic number; we also have that the set of algebraic integers $\mathbb{B}$ is a ring:

Proposition 1.8. *The set of algebraic integers is a subring of the field of algebraic numbers* [see Stewart and Tall [7] p.43].

Further, we find that the restriction of the coefficients to $\mathbb{Z}$ in the definition of algebraic integers is stronger than necessary:

Theorem 1.9. *If $\theta \in \mathbb{C}$ satisfies a monic polynomial $f(t)$ whose coefficients are algebraic integers, then θ is an algebraic integer* [see Stewart and Tall [7] p.43].

This theorem and the proposition above allow us to generate new algebraic integers out of old ones: for example, if α and θ are algebraic integers, so are $\alpha + \theta$ and $3 \cdot \alpha\theta^2$, as well as the solutions of the polynomial $t^3 - (2\alpha^2)t^2 - (5\sqrt{-7})t$.

Building off theorem 1.9, we can establish the following criterion for θ to be an algebraic integer:

Proposition 1.10. *An algebraic number α is an algebraic integer if and only if its minimum polynomial over $\mathbb{Q}$ has coefficients in $\mathbb{Z}$.*

Proof. Let p be the minimum polynomial of α over $\mathbb{Q}$, and recall that this is monic and irreducible in $\mathbb{Q}[t]$. If $p \in \mathbb{Z}[t]$, then α is an algebraic integer by definition. Conversely, if α is an algebraic integer, then $q(\alpha) = 0$ for some monic polynomial $q \in \mathbb{Z}[t]$, and we know that $p|q$. By Gauss' Lemma [see Stewart and Tall [7] p.18], there exists some $\lambda \in \mathbb{Q}$ such that λp is in $\mathbb{Z}[t]$ and divides q. Since p and q are monic, we must have $\lambda = 1$, and hence $p \in \mathbb{Z}[t]$. ☆

Notice that the term "integer" has been used quite often in this section, many times not referring to the elements of $\mathbb{Z}$. To avoid confusion, from now on we will say *rational integer*

for an element of $\mathbb{Z}$, and simply *integer* to mean an element of $\mathbb{B}$. This usage is well-defined by the following:

Proposition 1.11. *An algebraic integer is rational if and only if it's a rational integer; equivalently,* $\mathbb{B} \cap \mathbb{Q} = \mathbb{Z}$.

Proof. Clearly $\mathbb{Z} \subseteq \mathbb{B} \cap \mathbb{Q}$. For the converse, let $\alpha \in \mathbb{B} \cap \mathbb{Q}$. Since $\alpha \in \mathbb{Q}$, its minimum polynomial over $\mathbb{Q}$ is $t - \alpha$. By Proposition 1.10, the coefficients of this are in $\mathbb{Z}$, hence $-\alpha \in \mathbb{Z}$, hence $\alpha \in \mathbb{Z}$, as desired. ☆

1.1.2 Norm and Trace of an Element

We will now begin to describe the fields with which and in which we will be working:

Definition 1.12. A subfield K of $\mathbb{C}$ is a *number field* if the degree of the extension K over $\mathbb{Q}$ is finite.

This implies that every element of a number field is an algebraic number. Further, since $[K : \mathbb{Q}]$ is finite, we can write $K = \mathbb{Q}(\alpha_1, \ldots, \alpha_n)$ for some finite list of algebraic numbers α_i (for example, the elements of the basis of K as a vector space over $\mathbb{Q}$) [see Stewart [6] p.48]. Actually, a much stronger conclusion can be obtained:

Theorem 1.13. *If K number field, then $K = \mathbb{Q}[\theta]$ for some $\theta \in \mathbb{B}$* [see Stewart and Tall [7] p.44 for details].

We will explore these fields in more detail in the next section. But first, let us quickly look at one property:

Proposition 1.14. *If $K = \mathbb{Q}(\theta)$ is a number field of degree n over $\mathbb{Q}$, then there exist exactly n distinct monomorphisms $\sigma_i : K \to \mathbb{C}$. Moreover, the elements $\sigma_i(\theta) = \theta_i$ are the distinct zeros in $\mathbb{C}$ of the minimum polynomial of θ over $\mathbb{Q}$* [see Stewart and Tall [7] p.38 for details].

These n embeddings of K in $\mathbb{C}$ play a fundamental role in our analysis. An important example is given in the following definition:

Definition 1.15. Let α be an element of a number field $K = \mathbb{Q}(\theta)$, and let the σ_i be as above. The elements $\alpha_i = \sigma_i(\alpha)$ for $i = 1, \ldots, n$ are called the *K-conjugates of α*.

Note that, even though it will always be the case that the θ_i are all distinct, it is not necessarily the case that all α_i are distinct. More importantly, it is necessary to realize that the conjugates of α may not be members of K: for example, if we consider $K = \mathbb{Q}[\sqrt[3]{5}]$, the conjugates of $\sqrt[3]{5}$ are $\sqrt[3]{5}$, $\omega\sqrt[3]{5}$, and $\omega^2\sqrt[3]{5}$ for $\omega = e^{2\pi i/3}$; clearly these latter two are not real, and hence not in K.

Building off of this definition, we can generate two more values associated with each element of a number field:

Definition 1.16. With notation as above, we define the *norm of* α:

$$N_K(\alpha) = \prod_{i=1}^{n} \sigma_i(\alpha);$$

and the *trace of* α:

$$T_K(\alpha) = \sum_{i=1}^{n} \sigma_i(\alpha);$$

The norm and trace look like the product of the roots and the sum of the roots, respectfully, for some polynomial with roots $\sigma_i(\alpha)$; recall these would be the constant term and the coefficient of the t^{n-1} term of the said polynomial, respectively. This intuition proves to be useful, given the following definition and proposition:

Definition 1.17. For each $\alpha \in K$, we define the *field polynomial of* α *over* K to be:

$$f_\alpha(t) = \prod_{i=1}^{n} (t - \sigma_i(\alpha)).$$

Proposition 1.18. *Let $K = \mathbb{Q}[\theta]$ and σ_i be as above. Then, for $\alpha \in K$, the field polynomial f_α of α is a power of the minimum polynomial p_α of α over $\mathbb{Q}$.*

Proof. It can be shown that $f_\alpha \in \mathbb{Q}[t]$ [see Stewart and Tall [7] p.39], and we see that $f_\alpha(\alpha) = 0$. Thus, since p_α is the minimal (and irreducible) polynomial α satisfies, $p_\alpha \mid f_\alpha$. Hence we see $f_\alpha = p_\alpha \overline{h}$ for some polynomial $\overline{h} \in \mathbb{Q}[t]$. Let us factor all powers of p_α from $\overline{h}$, yielding $f_\alpha = p_\alpha(p_\alpha^{s-1}h) = p_\alpha^s h$ for some monic $h \in \mathbb{Q}[t]$. Suppose, for contradiction, that h is not constant; then, by our definition of f_α, $\sigma_i(\alpha)$ must satisfy h for some i.

We will show below in Example 1.27 that each $x \in K = \mathbb{Q}[\theta]$ can be written as a

polynomial in θ of degree less than $n-1$; let us say $\alpha = r(\theta)$. Then

$$\sigma_i(\alpha) = \sigma_i(r(\theta)) = r(\sigma_i(\theta)) = r(\theta_i).$$

Let us now define the composition $g = h \circ r$, and note that $g(\theta_i) = h(r(\theta_i)) = 0$. We claim $g(\theta_j) = 0$ for all j: if p is the minimum polynomial of θ, it must also be for every θ_j. Then $p \mid g$, hence $g(\theta_j) = 0$.

We now see:

$$h(\alpha) = h(r(\theta)) = g(\theta) = 0.$$

However, this would imply p_α divides h, a contradiction. Thus h is constant. ☆

Thus the K-conjugates of α are the (potentially repeated) zeros of the field polynomial. We can now show that the possible values for the norm and trace of algebraic integers are very limited:

Proposition 1.19. *The norm and trace of algebraic integers are rational integers.*

Proof. For any $\alpha \in K$, if α is also an integer then by Proposition 1.10 the minimum polynomial m of α over $\mathbb{Q}$ has rational integer coefficients. By Proposition 1.18, we know the field polynomial of α, f_α, is a power of the minimum polynomial m; thus, it clearly must also have rational integer coefficients. We see from our definition that, as intuitively expected, the norm is the constant term, and the trace is the coefficient of the t^{n-1} term; thus both are rational integers, as desired. ☆

It is also easy to see, since all the embeddings σ_i are monomorphisms, that the norm acts multiplicatively:

Proposition 1.20. *If α and β are elements of a number field K, then $N(\alpha\beta) = N(\alpha)N(\beta)$.*

Proof. Since all the σ_i are homomorphisms, they preserve multiplication. Thus we have:

$$N(\alpha\beta) = \sigma_1(\alpha\beta)\ldots\sigma_n(\alpha\beta) = \sigma_1(\alpha)\sigma_1(\beta)\ldots\sigma_n(\alpha)\sigma_n(\beta) = N(\alpha)N(\beta).$$

☆

1.2 Sets

We continue our exploration by looking at the various important sets which contain the types of elements we worked with in the previous section.

1.2.1 Number Fields, Number Rings, and Bases

Recall our construction of a number field $K = \mathbb{Q}[\theta]$ above. Note that while every element in K is an algebraic number, not all are algebraic integers. In fact, the set of integers in K forms a subring:

Definition 1.21. For any number field K, the *ring of integers* of K is the set $K \cap \mathbb{B}$, denoted $\mathfrak{O}_K$. We also call $\mathfrak{O}_K$ a *number ring*, associated with its field of fractions (the number field) K. Further, the subscript may be dropped if the field is obvious.

Proposition 1.22. *K is in fact the field of fractions of its associated ring of integers $\mathfrak{O}$*

Proof. Let α be an element of K; we must show $\alpha = xy^{-1}$ for some $x, y \in \mathfrak{O}$. It is sufficient to show that there exists a $y \in \mathfrak{O}$ such that $x = y\alpha \in \mathfrak{O}$. Since K is an algebraic extension, α is an algebraic number, and hence satisfies a monic polynomial f over $\mathbb{Q}$, say $f(\alpha) = \alpha^m + m_{m-1}\alpha^{m-1} + \ldots + m_1\alpha + m_0 = 0$ with $m_i \in \mathbb{Q}$ for all i. We know there exists some $y \in \mathbb{Z} \subseteq \mathfrak{O}$ such that, for all i, $ym_i \in \mathbb{Z}$. Multiply $f(\alpha)$ by y^m, and we see:

$$\begin{aligned} f(k)y^m &= y^m\alpha^m + m_{m-1}y^m\alpha^{m-1} + \ldots + m_1y^m\alpha + m_0y^m \\ &= (y\alpha)^m + m_{m-1}y(y\alpha)^{m-1} + \ldots + m_1y^{m-1}(y\alpha) + m_0y^m = 0 \end{aligned}$$

Thus $y\alpha \in K$ satisfies a monic polynomial with coefficients in $\mathbb{Z}$, hence $y\alpha \in \mathfrak{O}$, as desired. ☆

It is clear that $\mathfrak{O}$ is a ring since K is a field and $\mathbb{B}$ is a domain. It will be useful later to note further that $\mathfrak{O}$ is an integral domain:

Proposition 1.23. *Any number ring $\mathfrak{O}$ is an integral domain.*

Proof. This follows directly since $\mathfrak{O}$ is a subring of a field.

Example 1.24. The easiest example is the trivial number field, $K = \mathbb{Q}$. In this case clearly (and formally by Proposition 1.11) $R = \mathbb{Z}$.

Example 1.25. Slightly more complicated examples are *quadratic fields*, number fields of degree 2 over $\mathbb{Q}$. These can be shown to be of the form $K = \mathbb{Q}[\sqrt{d}]$ where d is a squarefree rational integer, and these make good examples since the ring of integers of such a field is easily found. It can be shown that the ring of integers of $K = \mathbb{Q}[\sqrt{d}]$ for squarefree d is:

(i) $\mathbb{Z}[\sqrt{d}]$ if $d \not\equiv 1 \pmod 4$; and

(ii) $\mathbb{Z}[\frac{1}{2} + \frac{1}{2}\sqrt{d}]$ if $d \equiv 1 \pmod 4$

We also have an easy formulation for the norm and trace of every element in K:

$$N(r + s\sqrt{d}) = r^2 - ds^2; \quad \text{and} \quad T(r + s\sqrt{d}) = 2r.$$

[For further reading on quadratic fields, see Stewart and Tall [7] p.61].

For the remainder of our paper, the focus of our investigations will be number fields K and their ring of integers $\mathfrak{O}$. However, many of our theorems and proofs hold not only in the number ring $\mathfrak{O}$ of a number field K, but in any commutative ring with identity R with field of fractions K. Often we will restrict our consideration strictly to number fields and number rings, but when we do work with a more general ring R, we will require R to be commutative with identity.

1.2.2 Bases

We stated above that a number field K is a finite extension of $\mathbb{Q}$, and recall that a finite extension of $\mathbb{Q}$ is also a vector space over $\mathbb{Q}$. This allows us to consider the following:

Definition 1.26. Let K be a number field. Then a basis of K as a vector space of $\mathbb{Q}$ is called a $\mathbb{Q}$-*basis of* K.

Example 1.27. Let K be a number field. By Theorem 1.13, we have that $K = \mathbb{Q}(\theta)$ for some algebraic integer θ, and thus the minimum polynomial over θ has degree n, where n is the degree of the extension K over $\mathbb{Q}$. Further, we have that $\{1, \theta, \ldots, \theta^{n-1}\}$ is an example

of a $\mathbb{Q}$-basis for K. [See STEWART [6] p.38 and STEWART AND TALL [7] p.46]

We now define an important property of a $\mathbb{Q}$-basis:

Definition 1.28. Let $K = \mathbb{Q}(\theta)$ be a number field of degree n, and let $\{\alpha_1, \ldots, \alpha_n\}$ be a basis of K. We define the *discriminant of* $\{\alpha_1, \ldots, \alpha_n\}$ to be:

$$\Delta[\alpha_1, \ldots, \alpha_n] = \Big(det[\sigma_i(\alpha_j)]\Big)^2;$$

where the σ_i are the n embeddings of K in $\mathbb{C}$.

It can be shown that there exists limits on the values the discriminant can take:

Proposition 1.29. *The discriminant of any basis is a non-zero rational number* [see STEWART [7] p.40 for details].

It will also be helpful to calculate how a modification of the basis will affect the discriminant. This idea motivates the following results:

Proposition 1.30. *Let* $\{\alpha_1, \ldots, \alpha_n\}$ *and* $\{\beta_1, \ldots, \beta_n\}$ *be two* $\mathbb{Q}$*-bases for* K*. Then* $\Delta[\beta_1, \ldots, \beta_n] = [det(c_{ij})]^2 \Delta[\alpha_1, \ldots, \alpha_n]$*, where* $\beta_j = \sum_{i=1}^{n} c_{ij}\alpha_i$*.* [see STEWART AND TALL [7], p.41]

This result allows us to compare the determinants of two entirely different bases for K. If we instead disturb just one element of the basis, we find the following to be true:

Proposition 1.31. *Let* $\{\alpha_1, \ldots, \alpha_n\}$ *be a* $\mathbb{Q}$*-basis for a number field. Then:*

(i) $\Delta(r\alpha_1, \alpha_2, ..., \alpha_n) = r^2 \Delta(\alpha_1, ...\alpha_n)$ *for all* $r \in \mathbb{Q}$*.*

(ii) Let β *be a linear combination of* $\alpha_2, ..., \alpha_n$ *with coefficients in* $\mathbb{Q}$*. Then* $\Delta\{\alpha_1 + \beta, \alpha_2, ..., \alpha_n\} = \Delta\{\alpha_1, ..., \alpha_n\}$.

Proof. (i) The result of incorporating the r into our calculation of the discriminant will change the first row of the matrix from $[\sigma_1(\alpha_1) \quad \ldots \quad \sigma_1(\alpha_n)]$ to $[\sigma_1(r\alpha_1) \quad \ldots \quad \sigma_1(r\alpha_n)] = [r\sigma_1(\alpha_1) \quad \ldots \quad r\sigma_1(\alpha_n)]$ since $\sigma(r) = r$ for all $r \in \mathbb{Q}$. We know that multiplying a row by a constant changes the determinant of that matrix by a factor of the same constant; since we are then squaring our discriminant value, the result follows.

(*ii*) This follows since the change from α to $\alpha + \beta$ would change the matrix in our calculation only by elementary row operations, and we know such operations do not change the determinant. Hence the discriminant would remain constant. ☆

Proposition 1.32. *Let α be an algebraic integer with minimum polynomial m over $\mathbb{Q}$ of degree n, and let f be a monic polynomial with coefficients (not necessarily irreducible) in $\mathbb{Z}$ such that $f(\alpha) = 0$. Then $\Delta = \Delta\{1, \alpha, \ldots, \alpha^{n-1}\}$ divides $N^{\mathbb{Q}[\alpha]}\big(f'(\alpha)\big)$, where f' is the usual derivative of the polynomial f.*

Proof. Let $\alpha_1, \ldots, \alpha_n$ be the conjugates of α. Then $\Delta = [\det(\alpha_i^j)]^2$ is the square of a Vandermonde determinant, and it can be shown [see Han [1] p.277] that

$$\Delta = \prod_{1 \leq i \lneq j \leq n} (\alpha_i - \alpha_j)^2.$$

Further, we can change our indicies to see that $\Delta = \prod_{i \lneq j} (\alpha_i - \alpha_j)^2 = \pm \prod_{i \neq j} (\alpha_i - \alpha_j)$. Then, since m has rational coefficients, its derivative m' has rational coefficients, and thus:

$$N^{\mathbb{Q}[\alpha]}(m'(\alpha)) = \prod_{i=1}^{n} \sigma_i(m'(\alpha)) = \prod_{i=1}^{n} m'(\sigma_i(\alpha)) = \prod_{i=1}^{n} m'(\alpha_i).$$

Since the α_i are the roots of m, we know $m(x) = \prod_{r=1}^{n} (x - \alpha_r)$. Thus:

$$m'(x) = \sum_{r=1}^{n} \left[\prod_{s \neq r} (x - \alpha_s) \right].$$

Note that when calculating $m'(\alpha_i)$, all the products will become zero except for one:

$$m'(\alpha_i) = \prod_{j=1; j \neq i}^{n} (\alpha_i - \alpha_j).$$

Therefore, we have:

$$\begin{aligned} N^{\mathbb{Q}[\alpha]}(m'(\alpha)) &= \prod_{i=1}^{n} m'(\alpha_i) \\ &= \prod_{i \neq j} (\alpha_i - \alpha_j) = \pm \prod_{i \lneq j} (\alpha_i - \alpha_j)^2 = \pm\Delta; \end{aligned}$$

where the index in $i \neq j$ (or $i \lneq j$) goes over all possible combinations of i and j such that $i \neq j$ ($i \lneq j$).

Now, if f is a monic polynomial that α satisfies, we have $f = mh$ and $f' = m'h + mh'$ for some monic h over $\mathbb{Q}$. Hence $f'(\alpha) = m'(\alpha)h(\alpha) + m(\alpha)h'(\alpha) = m'(\alpha)h(\alpha)$ since α satisfies m. Then note that:

$$\begin{aligned} N^{\mathbb{Q}[\alpha]}(f'(\alpha)) &= N(m'(\alpha)h(\alpha)) \\ &= \left[\prod_{i=1}^{n} m'(\alpha_i)\right] \left[\prod_{i=1}^{n} h(\alpha_i)\right] = \pm\Delta \left[\prod_{i=1}^{n} h(\alpha_i)\right]. \end{aligned}$$

Hence Δ divides $N^{\mathbb{Q}[\alpha]}(f'(\alpha))$, as desired. ☆

1.2.3 Free Abelian Groups

We will now study the additive group of a number ring. We will show it is a special type of group with important properties. For this section, when we are discussing the general case, we will be using additive notation for an abelian group G, with powers of group elements g denoted ng (for $n \in \mathbb{Z}$).

We must first define some terms in preparation for our desired property:

Definition 1.33. G is a *finitely generated abelian group* if there exist $g_1, \ldots, g_n \in G$ such that for all $g \in G$, $g = m_1 g_1 + \ldots + m_n g_n$ for some $m_i \in \mathbb{Z}$.

We will add structure to this concept until we have something resembling the basis of a vector space. To that end, we say:

Definition 1.34. Elements $g_1, \ldots, g_n \in G$ are *linearly independent over* $\mathbb{Z}$ if the only solution to the equation $x_1 g_1 + \ldots + x_n g_n = 0$ with $x_1, \ldots, x_n \in \mathbb{Z}$ is $x_1 = \ldots = x_n = 0$.

Definition 1.35. If G is a finitely-generated abelian group such that its generators $g_1, \ldots, g_n$ are linearly independent, then G is a *free abelian group of rank n*, and the set of generators is called a $\mathbb{Z}$*-basis of* G.

The properties we expect from a basis remain true in this setting: if G has a basis of n elements, all bases for G have n elements, and all elements $g \in G$ can be uniquely represented as a linear combination of the basis elements.

Another important property of these groups is that all subgroups are also free abelian, of lesser-or-equal rank:

Theorem 1.36. *Every subgroup H of a free abelian group G of rank n is also free abelian of rank $s \leq n$. Further, there exists a basis $\{u_1, \ldots, u_n\}$ for G and positive integers $\alpha_1, \ldots, \alpha_s$ such that $\{\alpha_1 u_1, \ldots, \alpha_s u_s\}$ is a basis for H.* [see Stewart and Tall [7] p.28]

We will now connect this idea to our number fields and number rings. We know that all number fields have a $\mathbb{Q}$-basis (a basis as a vector space over $\mathbb{Q}$); we would like to be able to show that the ring of integers of any number field has a $\mathbb{Z}$-basis, telling us that number rings are free abelian groups. Such a basis would need to consist entirely of integers. However, even if we have a basis of K consisting entirely of integers, this does not mean we have a $\mathbb{Z}$-basis for the number ring: for example, in $K = \mathbb{Q}[\sqrt{5}]$, the set $\{1, \sqrt{5}\}$ is clearly a $\mathbb{Q}$-basis for K consisting of integers. However, the elements $\frac{1}{2} + \frac{1}{2}\sqrt{5}$ satisfies $t^2 - t + 1$ and is thus an integer, but is not in the span of $\{1, \sqrt{5}\}$.

Therefore, we must establish that such a $\mathbb{Z}$-basis exists for every ring of integers. We start with a lemma:

Lemma 1.37. *If $\{\alpha_1, \ldots, \alpha_n\}$ is a $\mathbb{Q}$-basis of K consisting of integers, then the discriminant of this basis is a rational integer not equal to zero.*

Proof. We already know that $\Delta = \Delta[\alpha_1, \ldots, \alpha_n]$ is rational by Proposition 1.29, and is an integer since all the α_i are. Thus by Proposition 1.11 it must be a rational integer, and again by Proposition 1.29 $\Delta \neq 0$. ☆

Using this lemma, we can prove our desired result:

Theorem 1.38. *The ring of integers $\mathfrak{O}$ of any number field K has a $\mathbb{Z}$-basis, and thus all rings of integers $\mathfrak{O}$ are free abelian groups.*

Proof. Since K is a number field, we have $K = \mathbb{Q}(\theta)$ for some integer θ. Thus we know there exists at least one basis for K consisting integers, namely $\{1, \theta, \ldots, \theta^{n-1}\}$ where n is the degree of K over $\mathbb{Q}$. However, as noted above, this isn't necessarily a $\mathbb{Z}$-basis for $\mathfrak{O}$. By the above lemma the discriminant of a basis of integers must be a rational integer; let us choose our particular basis consisting of integers $\{\omega_1, \ldots, \omega_n\}$ such that $\left|\Delta[\omega_1, \ldots, \omega_n]\right|$ is least.

We claim this is in fact a $\mathbb{Z}$-basis for $\mathfrak{O}$. Suppose, for contradiction, it is not a $\mathbb{Z}$-basis. Then there exists some integer ω of K such that $\omega = a_1\omega_1 + \ldots + a_n\omega_n$ for $a_i \in \mathbb{Q}$ where not all the a_i are in $\mathbb{Z}$; renumber such that $a_1 \notin \mathbb{Z}$. Then we know $a_1 = a + r$ where $a \in \mathbb{Z}$ and $0 \leq r \lneq 1$.

We now define a new basis $\{\lambda_1, \ldots, \lambda_n\}$, where $\lambda_1 = \omega - a\omega_1 = r\omega_1 + a_2\omega_2 + \ldots + a_n\omega_n$ and $\lambda_i = \omega_i$ for $i = 2, \ldots, n$; clearly the λ_i are linearly independent over $\mathbb{Z}$ since the ω_i are, and they span the integers since the following holds for all $b \in \mathfrak{O}$:

$$b = m_1\omega_1 + \ldots + m_n\omega_n = (m_1r^{-1})\lambda_1 + (m_2 - m_1r^{-1}a_2)\lambda_2 + \ldots + (m_n - m_1r^{-1}a_n)\lambda_n.$$

The determinant of the change of basis matrix from $\{\omega_1, \ldots, \omega_n\}$ to $\{\lambda_1, \ldots, \lambda_n\}$ is:

$$\begin{vmatrix} a_1 - a & a_2 & \ldots & a_n \\ 0 & 1 & \ldots & 0 \\ \ldots & \ldots & \ldots & \ldots \\ 0 & 0 & 0 & 1 \end{vmatrix} = a_1 - a = r;$$

thus, by Proposition 1.30, $\Delta[\lambda_1, \ldots, \lambda_n] = r^2\Delta[\omega_1, \ldots, \omega_n]$. Since $0 \leq r \lneq 1$, this contradicts our choice of $\{\omega_1, \ldots, \omega_n\}$ with minimal discriminant. Therefore $\{\omega_1, \ldots, \omega_n\}$ is a $\mathbb{Z}$-basis for $\mathfrak{O}$, and so $(\mathfrak{O}, +)$ is a free abelian group of rank n. ☆

Definition 1.39. The $\mathbb{Z}$-basis of a number ring $\mathfrak{O}$ in a number field K is called an *integral basis of* K (or of $\mathfrak{O}$).

In Proposition 1.30, we see that the determinant of the change-of-basis matrix determines how the discriminant changes between two different bases. Note the following proposition with that in mind:

Proposition 1.40. *The change of basis matrix between two $\mathbb{Z}$-bases is* unimodular (equals ± 1). [see Stewart and Tall [7] p.28]

From this, we can prove the following about the discriminants of integral bases:

Proposition 1.41. *All integral bases of the same number field K have the same discriminant.*

Proof. $\Delta[\alpha_1, \ldots, \alpha_n] = (\pm 1)^2 \Delta[\beta_1, \ldots, \beta_n] = \Delta[\beta_1, \ldots, \beta_n]$ ☆

Definition 1.42. By the above proposition, the discriminant of an integral basis is independent of which particular integral basis of K we pick, and will always be the smallest possible Δ such that $\Delta = \Delta[\alpha_1, \ldots, \alpha_n]$ for some $\mathbb{Z}$-basis $\{\alpha_1, \ldots, \alpha_n\}$. This common value is called the *discriminant of K*.

Example 1.43. Recall our quadratic fields $K = \mathbb{Q}[\sqrt{d}]$ from Example 1.25. It is clear from the definitions of our rings of integers that:

(i) If $d \not\equiv 1 \pmod 4$, then $\{1, \sqrt{d}\}$ is an integral basis with discriminant:

$$\Delta = \left| \begin{smallmatrix} 1 & \sqrt{d} \\ 1 & -\sqrt{d} \end{smallmatrix} \right|^2 = (-2\sqrt{d})^2 = 4d$$

(ii) If $d \equiv 1 \pmod 4$, then $\{1, \frac{1}{2} + \frac{1}{2}\sqrt{d}\}$ is an integral basis with discriminant:

$$\Delta = \left| \begin{smallmatrix} 1 & \frac{1}{2}+\frac{1}{2}\sqrt{d} \\ 1 & -\frac{1}{2}+\frac{1}{2}\sqrt{d} \end{smallmatrix} \right|^2 = (-\sqrt{d})^2 = d$$

Since isomorphic fields have the same discriminant, distinct squarefree integers define anisomorphic fields.

We also have the following result relating properties of the basis with properties of its discriminant:

Corollary 1.44. *Let $\{\alpha_1, \ldots, \alpha_n\}$ be a $\mathbb{Q}$-basis for K consisting of integers. If $\Delta[\alpha_1, \ldots, \alpha_n]$ is squarefree then $\{\alpha_1, \ldots, \alpha_n\}$ is an integral basis.*

Proof. Take some integral basis $\{\beta_1, \ldots, \beta_n\}$. Then there exist $c_{ij} \in \mathbb{Z}$ such that $\alpha_i = \sum c_{ij}\beta_j$, and by Proposition 1.30 $\Delta[\alpha_1, \ldots, \alpha_n] = [det(c_{ij})]^2 \Delta[\beta_1, \ldots, \beta_n]$. Since the left side

is squarefree, it must be the case that $det(c_{ij}) = \pm 1$; thus, by Proposition 1.40, $\{\alpha_1, \ldots, \alpha_n\}$ is a $\mathbb{Z}$-basis for $\mathfrak{O}$. ☆

The fact that $\mathfrak{O}$ is a free abelian group has a number of consequences. Here is one example:

Corollary 1.45. *Let $\mathfrak{O}$ be the ring of integers in some number field K. Then, for any $p \in \mathbb{Z}$, $|\mathfrak{O}/p\mathfrak{O}| = p^n$, where n is the degree of K over $\mathbb{Q}$.*

Proof. Since $\mathfrak{O}$ is a number ring, we know that it is also a free abelian group over $\mathbb{Z}$ of order n by Theorem 1.36, with some integral basis $\{\alpha_1, ...\alpha_n\}$. Thus, for all $\beta \in \mathfrak{O}$, we have $\beta = m_1\alpha_1 + \ldots + m_n\alpha_n$, with $m_i \in \mathbb{Z}$. By the Division Algorithm, we have $m_i = px_i + y_i$ for some $x_i, y_i \in \mathbb{Z}$ with $0 \leq y_i \leq p-1$. Thus we see:

$$\begin{aligned}\beta &= m_1\alpha_1 + \ldots + m_n\alpha_n \\ &= (y_1 + px_1)\alpha_1 + \ldots + (y_n + px_n)\alpha_n \\ &= y_1\alpha_1 + \ldots + y_n\alpha_n + p(x_1\alpha_1 + \ldots + x_n\alpha_n)\end{aligned}$$

Since the last term $p(x_1\alpha_1 + \ldots + x_n\alpha_n)$ is in $p\mathfrak{O}$, and all the y_i are reduced modulo p, we have that $\beta + p\mathfrak{O} = \{y_1\alpha_1 + \ldots + y_n\alpha_n + p\mathfrak{O} \mid 0 \leq y_i \leq p-1\}$. There are p choices for each y_i, and n such i; thus $|\mathfrak{O}/p\mathfrak{O}| = p^n$, as desired. ☆

Results dealing with these types of quotient fields will become very important in our later analysis.

1.2.4 Ideals

In Chapter 3, we will be manipulating the ideals of a number ring, and thus it is important to establish some useful definitions and properties about these special subrings.

Definition 1.46. Let $\mathfrak{a}$ be an ideal in a (commutative with identity) ring R. We define two special types of ideals:

(i) We say $\mathfrak{a}$ is *maximal* if $\mathfrak{a}$ is a proper ideal of $\mathfrak{O}$ and there are no ideals of $\mathfrak{O}$ strictly between $\mathfrak{a}$ and $\mathfrak{O}$.

(ii) We say $\mathfrak{a}$ is *prime* if either of the following hold:

- For all ideals $\mathfrak{b}$ and $\mathfrak{c}$ of $\mathfrak{O}$ such that $\mathfrak{bc} \subseteq \mathfrak{a}$, it must be the case that either $\mathfrak{b} \subseteq \mathfrak{a}$ or $\mathfrak{c} \subseteq \mathfrak{a}$; or
- If $bc \in \mathfrak{a}$, then $b \in \mathfrak{a}$ or $c \in \mathfrak{a}$.

Proposition 1.47. *The two definitions of a prime ideal are equivalent.*

Proof. Suppose $\mathfrak{bc} \subseteq \mathfrak{a}$ implies $\mathfrak{b} \subseteq \mathfrak{a}$ or $\mathfrak{c} \subseteq \mathfrak{a}$, and assume $bc \in \mathfrak{a}$. Then $\langle b\rangle\langle c\rangle \subseteq \mathfrak{a}$. Hence $\langle b\rangle \subseteq \mathfrak{a}$ or $\langle c\rangle \subseteq \mathfrak{a}$, and thus $b \in \mathfrak{a}$ or $c \in \mathfrak{a}$. Conversely, suppose $bc \in \mathfrak{a}$ implies $b \in \mathfrak{a}$ or $c \in \mathfrak{a}$, and assume for contradiction that $\mathfrak{bc} \subseteq \mathfrak{a}$ but $\mathfrak{b} \not\subseteq \mathfrak{a}$ and $\mathfrak{c} \not\subseteq \mathfrak{a}$. Then there exists $b \in \mathfrak{b}$ and $c \in \mathfrak{c}$ such that $b \notin \mathfrak{a}$ and $c \notin \mathfrak{a}$. However, we know $bc \in \mathfrak{a}$, and our supposition yields a contradiction. ☆

Example 1.48. The definition of prime ideal translates exactly to that of a prime element if our ring is a Principle Ideal Domain: if $\mathfrak{a} = \langle a\rangle, \mathfrak{b} = \langle b\rangle$, and $\mathfrak{c} = \langle c\rangle$, then $\mathfrak{bc} \subseteq \mathfrak{a}$ implying $\mathfrak{b} \subseteq \mathfrak{a}$ or $\mathfrak{c} \subseteq \mathfrak{a}$ is equivalent to $a|bc$ implying $a|b$ or $a|c$. From this, we conclude that $x|y$ if and only if $\langle x\rangle \supseteq \langle y\rangle$; further, $\langle p\rangle$ is prime if and only if p is zero or prime.

We can now expand our definitions of "divides" to apply to ideals, as well as elements:

Definition 1.49. Let $\mathfrak{a}$ and $\mathfrak{b}$ be ideals in $\mathfrak{O}$. We say $\mathfrak{a}$ *divides* $\mathfrak{b}$, written $\mathfrak{a}|\mathfrak{b}$, if there exists some ideal $\mathfrak{c}$ such that $\mathfrak{b} = \mathfrak{ac}$.

We also include a definition of relatively prime for ideals in this context:

Definition 1.50. We say two proper ideals $\mathfrak{a}$ and $\mathfrak{b}$ of R are *relatively prime* if $\mathfrak{a} + \mathfrak{b} = R$.

We have the following result concerning relatively prime ideals our ring R, and their associated quotient fields:

Theorem 1.51 (Chinese Remainder Theorem)**.** *Let $\mathfrak{p}_1, \ldots, \mathfrak{p}_n$ be pairwise relatively prime ideals in a ring R. Then the obvious mapping $R/\bigcap_{i=1}^{n} \mathfrak{p}_i \to R/\mathfrak{p}_1$ x ... x $R/\mathfrak{p}_n$ is an isomorphism.*

Proof. We will first prove this for the specific case $n = 2$. The kernel of this natural mapping is clearly trivial, and hence the mapping is 1-1. To show it is onto, take any r_1 and r_2 in R, and consider the element $(r_1 + \mathfrak{p}_1) \times (r_2 + \mathfrak{p}_2)$. Since $\mathfrak{p}_1$ and $\mathfrak{p}_2$ are relatively prime and

$1 \in R$, there exist $a_1 \in \mathfrak{p}_1$ and $a_2 \in \mathfrak{p}_2$ such that $a_1 + a_2 = 1$, and define $r = a_1 r_2 + a_2 r_1$. Then:

$$r = a_i r_j + a_j r_i = a_i r_j + (1 - a_i) r_i = a_i (r_j - r_i) + r_i \equiv r_i \pmod{\mathfrak{p}_i}$$

since a_i, and hence $a_i(r_j - r_i)$, is in $\mathfrak{p}_i$. Thus r maps to $(r_1 + \mathfrak{p}_1) \times (r_2 + \mathfrak{p}_2)$, and hence the mapping is onto; therefore the mapping is a bijection, as desired.

The general result follows since all $\mathfrak{p}_i$ and $\mathfrak{p}_j$ are relatively prime, and thus we can always find appropriate elements $a_{ij} \in \mathfrak{p}_i$ and $a_{ji} \in \mathfrak{p}_j$ such that $a_{ij} + a_{ji} = 1$. ☆

Continuing our work with quotient rings, we have:

Theorem 1.52 (Third Isomorphism Theorem)**.** *Let $\mathfrak{a}$ and $\mathfrak{b}$ be ideals of a ring R, with $\mathfrak{b} \subseteq \mathfrak{a} \subseteq R$. Then the set $\mathfrak{a}/\mathfrak{b}$ is an ideal of the quotient $R/\mathfrak{b}$, and the quotient ring $(R/\mathfrak{b})/(\mathfrak{a}/\mathfrak{b})$ is isomorphic to $R/\mathfrak{a}$.*

Proof. To show $\mathfrak{a}/\mathfrak{b}$ is an ideal, note that $\mathfrak{a}/\mathfrak{b} = \{a + \mathfrak{b} | a \in \mathfrak{a}\}$, while $R/\mathfrak{b} = \{r + \mathfrak{b} | r \in R\}$. Clearly $\mathfrak{a}/\mathfrak{b} \subseteq R/\mathfrak{b}$. Now let $a_1 + \mathfrak{b}, a_2 + \mathfrak{b}$ be arbitrary. Then $(a_1 - a_2) + \mathfrak{b} \in \mathfrak{a}/\mathfrak{b}$ and $ra + \mathfrak{b} \in \mathfrak{a}/\mathfrak{b}$ for all $r \in R$ since $\mathfrak{a}$ is an ideal.

We will now construct an isomorphism ϕ. We start with the two induced mappings from our ring into the two quotient rings, $\pi_a : R \to R/\mathfrak{a}$ and $\pi_b : R \to R/\mathfrak{a}$. Now, since $ker(\pi_a) = \mathfrak{a}$ and $\mathfrak{b} \subseteq \mathfrak{a}$, by the First Homomorphism Theorem there exists a mapping $\overline{\phi} : R/\mathfrak{b} \to R/\mathfrak{a}$ such that $\overline{\phi} \circ \pi_b = \pi_a$, with $\overline{\phi}(\alpha + \mathfrak{b}) = \alpha + \mathfrak{b}$ for all $\alpha \in R$. Since π_a is onto, $\overline{\phi}$ must be as well, and further we note that the kernel of ϕ is $\mathfrak{a}/\mathfrak{b}$. Thus, again by the First Isomorphism Theorem, we have an isomorphism ϕ between $(R/\mathfrak{b})/(\mathfrak{a}/\mathfrak{b})$ and $R/\mathfrak{a}$. ☆

Moreover, there is a strong connection between these quotient rings and the classification of the associated ideal as maximal or prime. We begin with a lemma:

Lemma 1.53. *Let R be a ring, and $\mathfrak{a}$ an ideal of R. Then the ideals of $R/\mathfrak{a}$ are in 1-1 correspondence with the ideals of R containing $\mathfrak{a}$.*

Proof. Take I to be the set of ideals of $R/\mathfrak{a}$ and J to be the set of ideals of R that contain $\mathfrak{a}$. We define the mapping $h : J \to I$ by $h(\mathfrak{b}) = \mathfrak{b}/\mathfrak{a}$. We know $\mathfrak{b}/\mathfrak{a}$ is an ideal of $R/\mathfrak{a}$ by the Third Isomorphism Theorem. We will show (i) h is an injection; and (ii) h is a surjection.

For (i), suppose $h(\mathfrak{b}) = h(\mathfrak{c})$ for $\mathfrak{b}, \mathfrak{c} \in J$, and take $b \in \mathfrak{b}$. Since $\mathfrak{b}/\mathfrak{a} = \mathfrak{c}/\mathfrak{a}$, there exists $c \in \mathfrak{c}/\mathfrak{a}$ such that $b + \mathfrak{a} = c + \mathfrak{a}$, so $b - c \in \mathfrak{a} \subseteq \mathfrak{c}$. Then $b - c = c_2$, so $b = c_2 + c \in \mathfrak{c}$. By a symmetric argument, any arbitrary $c \in \mathfrak{c}$ is in $\mathfrak{b}$. Thus $\mathfrak{b} = \mathfrak{c}$, as desired.

For (ii), let $\mathfrak{b}$ be an ideal of $R/\mathfrak{a}$, and take $\overline{\mathfrak{b}} = \pi^{-1}(\mathfrak{b})$, where $\pi\colon R \to R/\mathfrak{a}$ is the natural epimorphism. We claim $\overline{\mathfrak{b}}$ is an ideal of R containing $\mathfrak{a}$. We see $\overline{\mathfrak{b}}$ is an ideal since π is a homomorphism and $\mathfrak{b}$ is an ideal of $R/\mathfrak{a}$. Further, since $\mathfrak{b}$ is an ideal, it must contain the identity $0 + \mathfrak{a}$, so $\mathfrak{a} \subseteq \pi^{-1}(\mathfrak{b}) = \overline{\mathfrak{b}}$, and hence $\overline{\mathfrak{b}} \in J$. Thus $h(\overline{\mathfrak{b}})$ is well defined and clearly equals $\mathfrak{b}$.

Therefore h is a well-defined bijection between I and J, so the ideals of $R/\mathfrak{a}$ are in 1-1 correspondence with the ideals of R containing $\mathfrak{a}$, as desired. ☆

We can now directly compare the properties of $\mathfrak{a}$ with the properties of the quotient ring $R/\mathfrak{a}$:

Theorem 1.54. *Let R be a ring, $\mathfrak{a}$ an ideal of R. Then:*

(i) $\mathfrak{a}$ is maximal if and only if $R/\mathfrak{a}$ is a field;

(ii) $\mathfrak{a}$ is prime if and only if $R/\mathfrak{a}$ is a domain.

Proof. (i) By the lemma, the ideals of $R/\mathfrak{a}$ are in bijective correspondence with the ideals of R lying between $\mathfrak{a}$ and R. Hence $\mathfrak{a}$ is maximal if and only if $R/\mathfrak{a}$ has no proper ideals, which is true if and only if $R/\mathfrak{a}$ is a field.
(ii) Suppose $\mathfrak{a}$ is prime. If $x, y \in R$ such that $(x + \mathfrak{a})(y + \mathfrak{a}) = 0$, then $xy \in \mathfrak{a}$. Hence $x \in \mathfrak{a}$ or $y \in \mathfrak{a}$, and therefore one of $(x + \mathfrak{a})$ and $(y + \mathfrak{a})$ is zero in $R/\mathfrak{a}$. Thus there are no zero-divisors, so $R/\mathfrak{a}$ is a domain. Conversely, assume $R/\mathfrak{a}$ is a domain. Then $|R/\mathfrak{a}| \neq 1$ so $\mathfrak{a} \neq R$. Then suppose, for contradiction, that $\mathfrak{bc} \subseteq \mathfrak{a}$ but $\mathfrak{b} \not\subseteq \mathfrak{a}$ and $\mathfrak{c} \not\subseteq \mathfrak{a}$ for some ideals $\mathfrak{b}$ and $\mathfrak{c}$ of R. Then we must have elements $b \in \mathfrak{b}$, $c \in \mathfrak{c}$ such that $bc \in \mathfrak{a}$ yet neither b nor c are in $\mathfrak{a}$. Therefore $(b + \mathfrak{a})$ and $(c + \mathfrak{a})$ are zero-divisors, contradicting that $R/\mathfrak{a}$ is a domain. ☆

Corollary 1.55. *All maximal ideals are prime.*

Proof. This follows directly from Theorem 1.54. ☆

This theorem and corollary will be very useful, as we often need to shift our considerations between the ideals $\mathfrak{a}$ of R and the associated quotient fields $R/\mathfrak{a}$, and this allows us to transform the associated structure.

1.2.5 Modules

A module can be considered a generalization of a vector space: informally, consider a module as a vector space where the scalars can be from a ring as well as a field. Formally:

Definition 1.56. For a ring R, an *R-module* is an abelian group M together with a function $\alpha : R \times M \to M$, written $\alpha(r, m) = rm$ with $r \in R$ and $m \in M$, which satisfies:

(i) $(r + s)m = rm + sm$;

(ii) $r(m + n) = rm + rn$;

(iii) $r(sm) = (rs)m$;

(iv) $1m = 1$

for all $r, s \in R$ and $m, n \in M$. The function α is called an *R-action on M*.
Note that, if R is a field, this is exactly the definition of a vector space over R. We will now define a subset of a module which is conceptually very similar to an ideal:

Definition 1.57. An *R-submodule of M* is a subgroup N of M such that for all $n \in N$ and $r \in R$, $rn \in N$.

Example 1.58. A $\mathbb{Z}$-module is just an abelian group M with a naturally defined action: $0m = 0$, $1m = m$, $(n + 1)m = nm + m$, and $(-n)m = -nm$ for $n \in \mathbb{Z}$ and $m \in M$.

Example 1.59. For an arbitrary ring R, there are some natural associated modules:

(i) For any subring S of R, we have that R is an S-module with action $\alpha(s, r) = sr$ defined by the product of elements in R.

(ii) Suppose $\mathfrak{a}$ is an ideal of R. Then $\mathfrak{a}$ is an R-module with $\alpha(r, i) = ri$, where the product is that of elements in R.

1.2.6 Noetherian Rings and Dedekind Domains

In this final introductory section, we will further explore the interesting properties of number rings, recalling that we have already shown that they are free abelian groups as well as integral domains. We will later show that the properties defined below have very powerful consequences when considering different types of factorization.

Definition 1.60. A domain D is *noetherian* if every ideal in D is finitely generated.

Definition 1.61. A domain D satisfies the *ascending chain condition* if given any ascending chain of ideals $\mathfrak{a}_0 \subseteq \mathfrak{a}_1 \subseteq \ldots \subseteq \mathfrak{a}_n \subseteq \ldots$ in $\mathfrak{O}$, there exists some $N \in \mathbb{Z}$ such that $\mathfrak{a}_n = \mathfrak{a}_N$ for all $n \geq N$; thus every ascending chain of ideals stops.

Definition 1.62. A domain D satisfies the *maximal condition* if every non-empty set I of proper ideals has a maximal element (one not contained within any other ideal in I).

Proposition 1.63. *The three definitions above are equivalent for a domain D*

Proof. Assume D is noetherian, and consider an ascending chain $\mathfrak{a}_0 \subseteq \mathfrak{a}_1 \subseteq \ldots$ of ideals. Take $\mathfrak{a} = \bigcup_{n=1}^{\infty} \mathfrak{a}_n$. Then $\mathfrak{a}$ is an ideal, and since D is noetherian it is finitely generated; assume $\mathfrak{a} = \langle x_1, \ldots, x_m \rangle$. Each of the x_i belongs to some ideal $\mathfrak{a}_j$, and let N be the maximum "j" of these m indices. Then $\mathfrak{a} = \mathfrak{a}_N$ and $\mathfrak{a}_n = \mathfrak{a}_N$ for all $n \geq N$.

Now assume D satisfies the ascending chain condition, and let S be a non-empty set of ideals. Suppose, for contradiction, S has no maximal element. Pick an arbitrary $\mathfrak{a}_0 \in S$. Then since S has no maximal element, $\mathfrak{a}_0$ cannot be maximal, so there exists some $\mathfrak{a}_1$ such that $\mathfrak{a}_0 \subsetneq \mathfrak{a}_1$. Inductively, for each $\mathfrak{a}_n$ we can find some $\mathfrak{a}_{n+1}$ with $\mathfrak{a}_n \subsetneq \mathfrak{a}_{n+1}$. However, these form an ascending chain that does not stop, a contradiction.

Finally, assume D satisfies the maximal condition. Let $\mathfrak{a}$ be an arbitrary ideal, and let S be the set of all finitely generated ideals contained in $\mathfrak{a}$. Note that $\{0\}$ is finitely generated and contained in $\mathfrak{a}$, so S is non-empty; thus S has some maximal element $\mathfrak{b}$. If $\mathfrak{b} \neq \mathfrak{a}$, pick some $x \in \mathfrak{a} - \mathfrak{b}$. Then $\langle \mathfrak{b}, x \rangle$ is finitely generated and strictly larger than $\mathfrak{b}$, a contradiction to the maximality of $\mathfrak{b}$. Thus $\mathfrak{b} = \mathfrak{a}$, and therefore $\mathfrak{a}$ is finitely generated. ☆

Theorem 1.64. *Let $\mathfrak{O}$ be the ring of integers of some number field K. Then $\mathfrak{O}$ is noetherian.*

Proof. We will show $\mathfrak{O}$ is noetherian directly, without calling on Proposition 1.63. Let $\mathfrak{a}$ be an ideal of $\mathfrak{O}$. By Theorem 1.38, the additive group of $\mathfrak{O}$ is free abelian of rank $n = [K : \mathbb{Q}]$, and hence by Theorem 1.36 the additive group of $\mathfrak{a}$ is also free abelian of rank $s \leq n$. If $\{x_1, \ldots, x_s\}$ is a $\mathbb{Z}$-basis for $\mathfrak{a}$, then clearly $\langle x_1, \ldots x_s\rangle \subseteq \mathfrak{a}$ since all $x_i \in \mathfrak{a}$ and $\mathfrak{a} \subseteq \langle x_1, \ldots x_s\rangle$ since $\langle x_1, \ldots x_s\rangle$ spans $\mathfrak{a}$. Therefore $\mathfrak{a} = \langle x_1 \ldots x_s\rangle$ is finitely generated, and hence $\mathfrak{O}$ is noetherian, as desired. ☆

Noetherian rings in general have some powerful properties, and some of these will be exploited in the following chapters.

Definition 1.65. Let D be a domain. We say D is *integrally closed* in its field of fractions K if, whenever $\alpha \in K$ is a root of some monic polynomial over D, we have $\alpha \in D$.

We can now define our stronger condition:

Definition 1.66. A domain D is a *Dedekind domain* if it satisfies the following conditions:

(i) D is noetherian;

(ii) D is integrally closed in its field of fractions K;

(iii) Every non-zero prime ideal is maximal.

We will show all number rings are in fact Dedekind Domains; we begin with a lemma:

Lemma 1.67. *Let $\mathfrak{p}$ be a non-zero prime ideal in the ring of integers $\mathfrak{O}$ of a number field K. Then $\mathfrak{O}/\mathfrak{p}$ is a finite field.*

Proof. We have that $\mathfrak{O}/\mathfrak{p}$ is a domain by Theorem 1.54. It is sufficient to show it is finite, since all finite domains are fields [see STEWART AND TALL [7] p. 12]. Let $\alpha \in \mathfrak{p}$ be non-zero, and let $m = N^K(\alpha)$. We know that $m \in \mathbb{Z}$ by Proposition 1.19. Recall that $\mathfrak{O}$ is a free abelian group of degree n. Then, we see $m = \alpha_1 \ldots \alpha_n$ where the α_i are the conjugates of α, and since $\alpha_i \neq 0$ for all i, $m \neq 0$. Further, $\alpha_i = \alpha$ for some i since some embedding σ_i of K must be the identity; renumbering if necessary, let $\alpha = \alpha_1$, and define $\beta = \alpha_2 \ldots \alpha_n$, so $m = \alpha\beta$. Since m and $\alpha^{-1} \in K$, we have $\beta = m\alpha^{-1} \in K$; further, all $\alpha_i \in \mathbb{B}$, so $\beta = \alpha_2 \ldots \alpha_n \in \mathbb{B}$. Thus $\beta \in K \cap \mathbb{B} = \mathfrak{O}$, so $m = \beta\alpha \in \mathfrak{p}$. Therefore $\mathfrak{p}$ contains some non-zero integer m. By Corollary 1.45, $|\mathfrak{O}/m\mathfrak{O}| = m^n$, and since $m\mathfrak{O}$ is a subring of $\mathfrak{p}$, $|\mathfrak{O}/\mathfrak{p}|$ divides m^n. Therefore $\mathfrak{O}/\mathfrak{p}$ is finite. ☆

Theorem 1.68. *Every number ring $\mathfrak{O}$ is a Dedekind domain.*

Proof. We know $\mathfrak{O}$ is noetherian by Theorem 1.64, and $\mathfrak{O}$ is integrally closed by Theorem 1.9. To show that every non-zero prime ideal $\mathfrak{a}$ is maximal, note by Corollary 1.67 that $\mathfrak{O}/\mathfrak{a}$ is a finite field, and thus by Theorem 1.54 $\mathfrak{O}$ is maximal. ☆

1.3 Prime Factorization of Elements

We will now briefly look, often without proof, at some startling results dealing with the factorization of elements of a number ring into irreducibles. For this section, as before let K be a number field with ring of integers $\mathfrak{O}$, noting that $\mathfrak{O}$ is also a domain by Proposition 1.23, and recall the distinction between an irreducible element and a prime element; irreducible means there is no proper factorization, while prime means $\alpha|\beta\gamma$ implies $\alpha|\beta$ or $\alpha|\gamma$.

For discussion, let us consider some non-unit α in a domain D. If α is not irreducible (i.e. is reducible), we can write $\alpha = a_1 a_2$ for some $a_i \in D$. Now consider the a_i; if they are reducible, we can write them as the product of two factors. We can continue in this manor, and go through this process for any $\alpha \in D$. With this in mind, we say:

Definition 1.69. *Factorization into irreducibles is possible* in D if every non-zero, non-unit $\alpha \in D$ is the product of a finite number of irreducible elements; that is, for every α, the process described above stops, and we see $\alpha = p_1 \dots p_r$ for some irreducibles $p_i \in D$.

Example 1.70. Let us consider the ring $\mathbb{B}$ of all algebraic integers, and note that there are no irreducible elements: for all $\alpha \in \mathbb{B}$, we also have that $\sqrt{\alpha} \in \mathbb{B}$; thus every element has a non-trivial factorization $\alpha = (\sqrt{\alpha})^2$. Thus, since there are no irreducible elements, no element can be written as a finite product of such (non-existent) elements, and thus factorization is not possible in $\mathbb{B}$.

This example demonstrates that in an arbitrary extension of the integers, not only is factorization not necessarily unique, but factorization into irreducibles itself isn't even necessarily possible (we are cheating slightly in this example since $[\mathbb{B} : \mathbb{Z}]$ is infinite, and number rings are finite extensions).

However, a condition we have introduced earlier is sufficient to guarantee factorization into irreducibles is possible:

Theorem 1.71. *Factorization into irreducibles is possible in a ring if it is noetherian; thus by Theorem 1.64 factorization is possible in every number ring* $\mathfrak{O}$. [For details see Stewart and Tall [7] p.81]

Further, we can characterize whether or not factorization in such a noetherian domain is unique by examining its irreducible elements; if there is a distinction between prime and

irreducible elements, unique factorization will fail:

Theorem 1.72. *Factorization into irreducibles is unique in $\mathfrak{O}$ if and only if every irreducible in $\mathfrak{O}$ is also prime* [see Stewart and Tall [7] p.87].

Definition 1.73. If factorization into irreducibles is possible and unique in a domain D, then D is called a *unique factorization domain.*

There are many other ways to conclude that a domain D is a unique factorization domain. For example, all Euclidean domains and Principle Ideal domains are also unique factorization domains [see Howie [4] p.32].

However, not all number rings are unique factorization domains; in fact, many are not. A good demonstration of this fact comes from considering complex quadratic fields:

Proposition 1.74. *The ring of integers of $K = \mathbb{Q}[\sqrt{d}]$ for negative, squarefree d has unique factorization into irreducibles if and only if d is one of the following values: -1, -2, -3, -7, -11, -19, -43, -67, and -163* [see Stewart and Tall [7] p.86].

We will now consider an exemplary case of number ring with non-unique factorization, and show that a particular element has multiple factorizations into irreducibles:

Example 1.75. Let $K = \mathbb{Q}[\sqrt{-5}]$, and note it is a quadratic field. Since $-5 \not\equiv 1 \pmod 4$, by our remark in Example 1.25 we know it has ring of integers $\mathfrak{O} = \mathbb{Z}[\sqrt{-5}]$. Consider the element $6 \in K$, and we can easily see that $6 = 2 \cdot 3 = (1 + \sqrt{-5})(1 - \sqrt{-5})$. We claim that the four elements 2, 3, $(1 + \sqrt{-5})$, and $(1 - \sqrt{-5})$ are all irreducible in $\mathfrak{O}$.

We will make use of the norm to help us prove this result. Elements in $\mathfrak{O}$ are of the form $a + b\sqrt{-5}$ for $a, b \in \mathbb{Z}$, and thus the norm $N(a+b\sqrt{-5}) = (a+b\sqrt{-5})(a-b\sqrt{-5}) = a^2+5b^2$; hence, we have $N(2) = 4$, $N(3) = 9$, $N(1 + \sqrt{-5}) = N(1 - \sqrt{-5}) = 6$. Let us consider the element 2 specifically. If 2 factors in $\mathfrak{O}$, say $2 = xy$ for $x, y \in \mathbb{Z}[\sqrt{-5}]$, then, by Proposition 1.20 we have $4 = N(x)N(y)$, and since the norm of an element is an integer by Proposition 1.19, for this factorization to be proper it must be the case that $N(x) = \pm 2 = N(y)$. Similarly, non-trivial factors of 3 must have a norm of ± 3, and non-trivial factors of $1 \pm \sqrt{-5}$ must have norm ± 2 or ± 3. Thus, any proper factor of any of these four elements must have a norm of ± 2 or ± 3.

Take $\alpha \in \mathfrak{O}$ to be a non-trivial factor of 2, 3, $(1+\sqrt{-5})$, or $(1-\sqrt{-5})$. Then $N(\alpha) = N(a+b\sqrt{-5}) = a^2+5b^2 = \pm 2, \pm 3$. Note that if $b \geq 1$, then $|a^2+5b^2| \geq 5$, so we must have $b = 0$. Thus we must have $a^2 = \pm 2, \pm 3$. Clearly this is not possible if a is an integer; thus no possible non-trivial factors exist of 2, 3, $(1+\sqrt{-5})$, or $(1-\sqrt{-5})$. Hence they are all irreducible, and thus 6 has two factorizations into irreducibles in $\mathfrak{O}$. Therefore all elements of the number ring $\mathfrak{O} = \mathbb{Z}[\sqrt{-5}]$ do *not* factor uniquely.

Chapter 2

Prime Factorization of Ideals

As we saw at the end of the previous chapter, factorization of elements in number rings need not be unique. In this chapter, we will show that it is much nicer to consider the ideals of a number ring; we can expand our definitions of "prime" and "factors" to concern ideals, and we find that, in any number ring, all ideals factor uniquely into prime ideals. In this chapter, we will again be working in a number field K with ring of integers $\mathfrak{O}$, and the term "prime" will refer to a non-zero prime ideal of $\mathfrak{O}$.

We will consider two ways to prove the unique factorization of ideals, presented by Stewart and Tall and Marcus: the first involves a concept called "fractional ideals", the second deals with "ideal classes". While these ideas are related, they each give a different perspective on the problem. It is important to note that most of these proofs work for any Dedekind domain $\mathfrak{O}$ with field of fractions K; however, again, we will most often be restricting our view to the more specific case of a number field and its ring of integers.

We begin by showing that every ideal in a number ring contains a product of primes.

Lemma 2.1. *For every ideal $\mathfrak{a}$ in a number ring $\mathfrak{O}$, there exist primes $\mathfrak{p}_1, \ldots, \mathfrak{p}_r$ such that $\mathfrak{p}_1 \ldots \mathfrak{p}_r \subseteq \mathfrak{a}$.*

Proof. Consider the set of all ideals that do not contain a product of primes, and suppose, for contradiction, it is non-empty. Since $\mathfrak{O}$ is noetherian, it satisfies the maximal condition, and thus we have a maximal element $\mathfrak{a}$ of this set. Clearly $\mathfrak{a}$ is not prime (otherwise it trivially contains a product of primes), so there exist ideals $\mathfrak{b}$ and $\mathfrak{c}$ of $\mathfrak{O}$ such that $\mathfrak{bc} \subseteq \mathfrak{a}$

with $\mathfrak{b} \not\subseteq \mathfrak{a}$ and $\mathfrak{c} \not\subseteq \mathfrak{a}$. Take $\mathfrak{a}_1 = \mathfrak{a} + \mathfrak{b}$ and $\mathfrak{a}_2 = \mathfrak{a} + \mathfrak{c}$. Now note that $\mathfrak{a}_1\mathfrak{a}_2 \subseteq \mathfrak{a}$ (since elements of $\mathfrak{a}_1\mathfrak{a}_2$ are sums of elements of the form $a_ia_j + a_ic_j + a_jb_i + b_ic_j$), and both $\mathfrak{a} \subsetneq \mathfrak{a}_1$, $\mathfrak{a} \subsetneq \mathfrak{a}_2$. By the maximality of $\mathfrak{a}$, we know there exist $\mathfrak{p}_1, \ldots, \mathfrak{p}_s, \mathfrak{p}_{s+1}, \ldots, \mathfrak{p}_r$ such that $\mathfrak{p}_1 \ldots \mathfrak{p}_s \subseteq \mathfrak{a}_1$ and $\mathfrak{p}_{s+1} \ldots \mathfrak{p}_r \subseteq \mathfrak{a}_2$. But therefore $\mathfrak{p}_1 \ldots \mathfrak{p}_r \subseteq \mathfrak{a}_1\mathfrak{a}_2 \subseteq \mathfrak{a}$, a contradiction. ☆

We can also construct show there exists an element outside our number ring $\mathfrak{O}$ with an interesting property:

Lemma 2.2. *Let $\mathfrak{a}$ be a proper ideal. Then there exists an element $\gamma \in K \backslash \mathfrak{O}$ such that $\gamma\mathfrak{a} \subseteq \mathfrak{O}$.*

Proof. Since $\mathfrak{a}$ is a proper ideal, it is contained in some maximal (hence prime by Lemma 1.55) ideal $\mathfrak{p}$. Take $a \in \mathfrak{a} \subseteq \mathfrak{p}$. By Lemma 2.1 we know the ideal $\langle a \rangle$ contains a product of primes; say $\mathfrak{p}_1 \ldots \mathfrak{p}_r \subseteq \langle a \rangle$, and we may choose this product such that r is minimal. Since $\langle a \rangle \subseteq \mathfrak{a} \subseteq \mathfrak{p}$, by the definition of prime ideal $\mathfrak{p} \supseteq \mathfrak{p}_i$ for some i; renumbering if necessary let $\mathfrak{p} \supseteq \mathfrak{p}_1$. Since both ideals are maximal, we have $\mathfrak{p}_1 = \mathfrak{p}$. Further, by the minimality of r, we have $\mathfrak{p}_2 \ldots \mathfrak{p}_r \not\subseteq \langle a \rangle$, hence there exists some $b \in \mathfrak{p}_2 \ldots \mathfrak{p}_r \backslash \langle a \rangle$.

But then we have $b \notin \langle a \rangle = a\mathfrak{O}$, so $ba^{-1} \notin \mathfrak{O}$; take $\gamma = ba^{-1} \in K \backslash \mathfrak{O}$. Note that $b\mathfrak{p} \subseteq \langle a \rangle$, and thus $ba^{-1}\mathfrak{p} \subseteq \mathfrak{O}$. Therefore $\gamma\mathfrak{a} = ba^{-1}\mathfrak{a} \subseteq \ ba^{-1}\mathfrak{p} \subseteq \mathfrak{O}$, as desired. ☆

From here, the two proof methods diverge.

2.1 Proof Via Fractional Ideals

We begin with two equivalent definitions of a fractional ideal:

Definition 2.3. We call an $\mathfrak{O}$-submodule $\mathfrak{f}$ of K a *fractional ideal* if there exists some non-zero $c \in \mathfrak{O}$ such that $c\mathfrak{f} \subseteq \mathfrak{O}$.

Definition 2.4. A subset $\mathfrak{f}$ of K is a *fractional ideal* if it is of the form $\mathfrak{f} = c^{-1}\mathfrak{a}$ for some ideal $\mathfrak{a} \subseteq \mathfrak{O}$ and $0 \neq c \in \mathfrak{O}$.

These definitions are equivalent since $c\mathfrak{f}$ is an ideal of $\mathfrak{O}$: $cf_1 - cf_2 = c(f_1 - f_2) = cf_3 \in c\mathfrak{f}$, and $\alpha(cf_1) = c(\alpha f_1) = cf_2 \in c\mathfrak{f}$, for $f_i \in \mathfrak{f}$ and $\alpha \in \mathfrak{O}$. [see Stewart and Tall [7] p.107

for more details]. Note that clearly all ideals of $\mathfrak{O}$ are fractional ideals (take $c = 1$), and further:

Proposition 2.5. *A fractional ideal* $\mathfrak{f}$ *is a true ideal if and only if* $\mathfrak{f} \subseteq \mathfrak{O}$.

Proof. Both directions are trivial. ☆

Example 2.6. In the rational integers, the fractional ideals are the sets $r\mathbb{Z}$ for some $r \in \mathbb{Q}$.

Example 2.7. If $\mathfrak{O}$ is a principle ideal domain, the fractional ideals are the sets $c^{-1}\langle a \rangle = c^{-1}a\mathfrak{O} = \alpha\mathfrak{O}$ for some $\alpha \in K$.

Consider the set $\mathfrak{F}$ of all fractional ideals of a number ring $\mathfrak{O}$. We would like to show $\mathfrak{F}$ is a group. We begin with a lemma:

Lemma 2.8. *If* $\mathfrak{a}$ *is a non-zero ideal of* $\mathfrak{O}$ *and* $\mathfrak{a}S \subseteq \mathfrak{a}$ *for some subset* $S \subseteq K$*, then* $S \subseteq \mathfrak{O}$.

Proof. Let $s \in S$ be arbitrary, and by our supposition $\mathfrak{a}s \subseteq \mathfrak{a}$. Because $\mathfrak{O}$ is noetherian, $\mathfrak{a}$ is finitely generated; say $\mathfrak{a} = \langle a_1, \ldots, a_m \rangle$ for some $a_i \in \mathfrak{O}$, not all zero. Then, since $\mathfrak{a}s \subseteq \mathfrak{a}$, we know $a_i s \in \mathfrak{a}$ for all i. Thus, for all i, we have $a_i s = b_{i1}a_1 + \ldots + b_{im}a_m$ for some $b_{ij} \in \mathfrak{O}$. Consider the following associated system of equations in m unknowns:

$$\begin{aligned} x_1 s &= b_{11}x_1 + \ldots + b_{m1}x_m \\ &\vdots \\ x_m s &= b_{m1}x_1 + \ldots + b_{mm}x_m \end{aligned}$$

We can rearrange these equations into a system of m homogeneous equations in over x_i with coefficient matrix as follows;

$$\begin{bmatrix} b_{11} - s & b_{12} & \ldots & b_{1m} \\ b_{21} & b_{22} - s & \ldots & b_{2m} \\ \ldots & \ldots & \ldots & \ldots \\ b_{m1} & b_{m2} & \ldots & b_{mm} - s \end{bmatrix}$$

Note that we have a non-zero solution, namely $x_i = a_i$, and hence the determinant of this matrix is zero. This gives us a monic polynomial equation with coefficients in $\mathfrak{O}$ that s satisfies, and thus $s \in \mathfrak{O}$ by Theorem 1.9. ☆

Theorem 2.9. *The set of fractional ideals $\mathfrak{F}$ forms a group under multiplication.*

Proof. Let $\mathfrak{f}_i = c_i^{-1}\mathfrak{a}_i$ be fractional ideals (so $c_i \in K$ and $\mathfrak{a}_i$ an ideal of $\mathfrak{O}$) for $i = 1, 2$. Closure, associativity, and the existence of an identity follow easily:

Closure We have $\mathfrak{f}_1\mathfrak{f}_2 = (c_1^{-1}\mathfrak{a}_1)(c_2^{-1}\mathfrak{a}_2) = (c_1c_2)^{-1}\mathfrak{a}_1\mathfrak{a}_2 \in \mathfrak{F}$.

Associativity This follows trivially since ideal and integer multiplication is commutative and associative.

Identity The entire number ring $\mathfrak{O}$ is the identity: $\mathfrak{f}\mathfrak{O} = (c^{-1}\mathfrak{a})\mathfrak{O} = c^{-1}(\mathfrak{a}\mathfrak{O}) = c^{-1}\mathfrak{a} = \mathfrak{f}$.

The proof of the existence of an inverse is non-trivial:

Inverse We will first define $\mathfrak{a}^{-1}$ for a true ideal $\mathfrak{a}$ of $\mathfrak{O}$, and show $\mathfrak{a}$ and $\mathfrak{a}^{-1}$ are inverses: we will demonstrate, first for maximal and then for all ideals, that $\mathfrak{a}\mathfrak{a}^{-1} = \mathfrak{O}$. We will then show that this inverse can be used to find the inverse of a fractional ideal.

For any ideal $\mathfrak{a}$ of $\mathfrak{O}$, define $\mathfrak{a}^{-1} = \{x \in K \mid x\mathfrak{a} \subseteq \mathfrak{O}\}$. It is easy to see that $\mathfrak{a}^{-1}$ is a $\mathfrak{O}$-submodule of K. Note further that, if $\mathfrak{a} \neq 0$, then for all $x \in \mathfrak{a}^{-1}$ and any non-zero $a \in \mathfrak{a}$, we have $ax \in \mathfrak{O}$ and hence $a\mathfrak{a}^{-1} \subseteq \mathfrak{O}$; thus $\mathfrak{a}^{-1}$ is a fractional ideal. Then, since $\mathfrak{a}$ is an ideal of $\mathfrak{O}$, $\mathfrak{O}\mathfrak{a} \subseteq \mathfrak{a}$, so $\mathfrak{O} \subseteq \mathfrak{a}^{-1}$, and hence $\mathfrak{a} = \mathfrak{a}\mathfrak{O} \subseteq \mathfrak{a}\mathfrak{a}^{-1}$. From the definition we have $\mathfrak{a}\mathfrak{a}^{-1} = \mathfrak{a}^{-1}\mathfrak{a} \subseteq \mathfrak{O}$, and thus $\mathfrak{a}\mathfrak{a}^{-1}$ is a true ideal of $\mathfrak{O}$. We would like to show that $\mathfrak{a}\mathfrak{a}^{-1} = \mathfrak{O}$.

Note that, if $\mathfrak{a} \subseteq \mathfrak{b}$, then $\mathfrak{b}^{-1} \subseteq \mathfrak{a}^{-1}$ since, for all $x \in \mathfrak{b}^{-1}$, $x\mathfrak{a} \subseteq x\mathfrak{b} \subseteq \mathfrak{O}$. Take our arbitrary ideal $\mathfrak{a}$. Then, by Lemma 2.2 we know there exists some $\gamma \in K\backslash\mathfrak{O}$ such that $\gamma\mathfrak{a} \in \mathfrak{O}$. Hence by our definition of $\mathfrak{a}^{-1}$ above, we have $\gamma \in \mathfrak{a}^{-1}$; since $\mathfrak{a}$ contains $\mathfrak{O}$, $\mathfrak{O} \subsetneq \mathfrak{a}^{-1}$.

We showed above that $\mathfrak{a}\mathfrak{a}^{-1}$ is an ideal of $\mathfrak{O}$ for all ideals $\mathfrak{a}$; consider the case where $\mathfrak{a} = \mathfrak{p}$ is prime. Then we have $\mathfrak{p} \subseteq \mathfrak{p}\mathfrak{p}^{-1} \subseteq \mathfrak{O}$, so $\mathfrak{p}\mathfrak{p}^{-1}$ must equal either $\mathfrak{p}$ or $\mathfrak{O}$ since $\mathfrak{p}$ is maximal. However, if $\mathfrak{p}\mathfrak{p}^{-1} = \mathfrak{p}$, by Lemma 2.8 $\mathfrak{p}^{-1} \subseteq \mathfrak{O}$, contradicting our above result. Thus $\mathfrak{p}\mathfrak{p}^{-1} = \mathfrak{O}$. Let us build on this and show that $\mathfrak{a}\mathfrak{a}^{-1} = \mathfrak{O}$ for any ideal $\mathfrak{a}$. Suppose not for contradiction, and then choose $\mathfrak{a}$ maximal subject to $\mathfrak{a}\mathfrak{a}^{-1} \neq \mathfrak{O}$. Again, we have $\mathfrak{a} \subseteq \mathfrak{p}$ for some maximal ideal $\mathfrak{p}$. Since $\mathfrak{O} \subsetneq \mathfrak{p}^{-1} \subseteq \mathfrak{a}^{-1}$, we have:

$$\mathfrak{a} \subsetneq \mathfrak{a}\mathfrak{p}^{-1} \subseteq \mathfrak{a}\mathfrak{a}^{-1} \subseteq \mathfrak{O}.$$

Thus, since $\mathfrak{a}\mathfrak{p}^{-1} \subseteq \mathfrak{O}$, $\mathfrak{a}\mathfrak{p}^{-1}$ must be a true ideal. Further, since $\mathfrak{a} \subsetneq \mathfrak{a}\mathfrak{p}^{-1}$, by the maximal condition on $\mathfrak{a}$ we have that $\mathfrak{a}\mathfrak{p}^{-1}(\mathfrak{a}\mathfrak{p}^{-1})^{-1} = \mathfrak{O}$, and thus $\mathfrak{p}^{-1}(\mathfrak{a}\mathfrak{p}^{-1})^{-1} \subseteq \mathfrak{a}^{-1}$ by our definition of $\mathfrak{a}^{-1}$. Therefore:

$$\mathfrak{O} = \mathfrak{a}\mathfrak{p}^{-1}(\mathfrak{a}\mathfrak{p}^{-1})^{-1} \subseteq \mathfrak{a}\mathfrak{a}^{-1} \subseteq \mathfrak{O};$$

and hence $\mathfrak{a}\mathfrak{a}^{-1} = \mathfrak{O}$ for all ideals $\mathfrak{a}$. Finally, for our fractional ideal $\mathfrak{f} = c^{-1}\mathfrak{a}$, we define the inverse $\mathfrak{f}^{-1} = c\mathfrak{a}^{-1}$, and see $\mathfrak{f}\mathfrak{f}^{-1} = (cc^{-1})\mathfrak{a}\mathfrak{a}^{-1} = 1\mathfrak{O} = \mathfrak{O}$, as desired.

Therefore the set of fractional ideals $\mathfrak{F}$ is a group. ☆

Proposition 2.10. *For ideals $\mathfrak{a}$ and $\mathfrak{b}$ of $\mathfrak{O}$, $\mathfrak{a}|\mathfrak{b}$ if and only if $\mathfrak{a} \supseteq \mathfrak{b}$.*

Proof. Suppose $\mathfrak{a}|\mathfrak{b}$. Then $\mathfrak{b} = \mathfrak{c}\mathfrak{a}$ for some ideal $\mathfrak{c}$. The result follows since the product of two ideals is a subset of both factors.

Conversely, if $\mathfrak{a} \supseteq \mathfrak{b}$, define the set $\mathfrak{c} = \mathfrak{a}^{-1}\mathfrak{b}$, and then clearly $\mathfrak{b} = \mathfrak{a}\mathfrak{c}$. Since both $\mathfrak{a}^{-1}$ and $\mathfrak{b}$ are (at least) fractional ideals, and the fractional ideals form a group, $\mathfrak{c}$ is a fractional ideal with $\mathfrak{c} = \mathfrak{a}^{-1}\mathfrak{b} \subseteq \mathfrak{a}^{-1}\mathfrak{a} \subseteq \mathfrak{O}$. Thus $\mathfrak{c}$ is a true ideal, and therefore $\mathfrak{a}|\mathfrak{b}$. ☆

This augments our definition of a prime ideal, making it analogous to the definition of a prime element: if $\mathfrak{p}$ is prime, then whenever $\mathfrak{p}|\mathfrak{a}\mathfrak{b}$, $\mathfrak{p}|\mathfrak{a}$ or $\mathfrak{p}|\mathfrak{b}$.

We can now prove unique factorization of ideals:

Theorem 2.11. *Every non-zero ideal $\mathfrak{a}$ of $\mathfrak{O}$ can be written as a product of prime ideals, uniquely up to order.*

Proof. By Lemma 2.1, we know every $\mathfrak{a}$ *contains* a product of primes; we will now show it is equal to such a product. Suppose not, with $\mathfrak{a}$ maximal with respect to not being a product of prime ideals. Then $\mathfrak{a}$ cannot be prime, but is contained in some maximal (with respect to the whole ring $\mathfrak{O}$) ideal $\mathfrak{p}$. Then, as in the above proof of Theorem 2.9, we have $\mathfrak{O} \subsetneq \mathfrak{p}^{-1} \subseteq \mathfrak{a}^{-1}$ and thus $\mathfrak{a} \subsetneq \mathfrak{a}\mathfrak{p}^{-1} \subseteq \mathfrak{O}$. By the maximality of $\mathfrak{a}$, the ideal $\mathfrak{a}\mathfrak{p}^{-1}$ must equal a product of primes: $\mathfrak{a}\mathfrak{p}^{-1} = \mathfrak{p}_2 \dots \mathfrak{p}_r$. Thus $\mathfrak{a} = \mathfrak{p}\mathfrak{p}_2 \dots \mathfrak{p}_r$, and hence is equal to a product of primes, a contradiction.

For uniqueness, suppose our ideal $\mathfrak{a}$ has two factorizations into primes: $\mathfrak{a} = \mathfrak{p}_1 \dots \mathfrak{p}_r = \mathfrak{q}_1 \dots \mathfrak{q}_s$. Then $\mathfrak{p}_1$ must divide some $\mathfrak{q}_i$, and from maximality $\mathfrak{p}_1 = \mathfrak{q}_i$. Multiply through by

$\mathfrak{p}_1^{-1}$; continuing this process inductively, we obtain uniqueness of prime factorization up to order of the factors, as desired. ☆

2.2 Proof Via Ideal Classes

We now move to another method of proving ideals factor uniquely in number rings. We begin by defining an equivalence relation:

Definition 2.12. Let $\mathfrak{a}$ and $\mathfrak{b}$ be ideals in a number ring $\mathfrak{O}$. Then we say $\mathfrak{a} \sim \mathfrak{b}$ if and only if $\alpha\mathfrak{a} = \beta\mathfrak{b}$ for some non-zero $\alpha, \beta \in \mathfrak{O}$.

Proposition 2.13. *The relation $\sim$ defined above is an equivalence relation on the ideals of $\mathfrak{O}$* [the proof is trivial].

Definition 2.14. We call each equivalence class an *ideal class.*

The study of the set of ideal classes is on its own a very fruitful subject. For our current endeavors we will show the set is a group [see Marcus [5] p.32 and Stewart and Tall [7] p.157 for other interesting results, including that the set is finite]. We begin with a theorem:

Theorem 2.15. *Let $\mathfrak{a}$ be an ideal in a number ring $\mathfrak{O}$. Then there exists an ideal $\mathfrak{b}$ such that $\mathfrak{ab}$ is principle.*

Proof. Let $a \in \mathfrak{a}$ be non-zero. We take $\mathfrak{b} = \{b \in \mathfrak{O} \mid b\mathfrak{a} \subseteq \langle a \rangle\}$; it follows directly from the definition and the fact that $\langle a \rangle$ is an ideal that $\mathfrak{b}$ is itself an ideal. We note that $\mathfrak{ab} \subseteq \langle a \rangle$. Now consider the set $\mathfrak{c} = a^{-1}\mathfrak{ab}$; we will show $\mathfrak{ab} = \langle a \rangle$ by demonstrating that $\mathfrak{c} = \mathfrak{O}$.

Note that $\mathfrak{c} = a^{-1}\mathfrak{ab} \subseteq a^{-1}\langle a \rangle = \mathfrak{O}$, and further that $\mathfrak{c}$ is an ideal (since $\mathfrak{ab}$ is). Suppose, for contradiction that $\mathfrak{c}$ is a proper ideal of $\mathfrak{O}$. By Lemma 2.2 there exists a $\gamma \notin K \backslash \mathfrak{O}$ such that $\gamma\mathfrak{c} \subseteq \mathfrak{O}$. Since $a \in \mathfrak{a}$ we have that $\mathfrak{b} \subseteq \mathfrak{c}$, and thus $\gamma\mathfrak{b} \subseteq \gamma\mathfrak{c} \subseteq \mathfrak{O}$. Now take $\gamma b \in \gamma\mathfrak{b}$ and $x \in \mathfrak{a}$; then $\gamma bx = \gamma a^{-1}bxa = \gamma(a^{-1}xb)a$, but $a^{-1}xb \in a^{-1}\mathfrak{ab} = \mathfrak{c}$, so $\gamma bx = \gamma(c)a = (\gamma c)a \in \langle a \rangle$ since $\gamma\mathfrak{b} \subseteq \mathfrak{O}$. Thus $\gamma\mathfrak{b} \subseteq \mathfrak{b}$.

Since $\mathfrak{O}$ is noetherian, $\mathfrak{b}$ is finitely generated; take $\mathfrak{b} = \langle \alpha_1, \ldots, \alpha_m \rangle$. As in our proof above in Lemma 2.8, we consider the system of equations generated by expressing each $\gamma\alpha_i$

as a linear combination of our generators, representable as the following matrix equation:

$$\gamma \begin{bmatrix} \alpha_1 \\ \vdots \\ \alpha_m \end{bmatrix} = \mathbf{C} \begin{bmatrix} \alpha_1 \\ \vdots \\ \alpha_m \end{bmatrix}$$

where $\mathbf{C}$ is our coefficient matrix. This can be easily transformed into a system of homogeneous equations, and using the determinant, we produce a monic polynomial with coefficients in $\mathfrak{O}$ that γ satisfies. Thus $\gamma \in \mathfrak{O}$, contradicting $\gamma \in K \backslash \mathfrak{O}$.

Thus $\mathfrak{c}$ is not a proper ideal, and therefore $\mathfrak{ab} = \langle a \rangle$, as desired. ☆

Corollary 2.16. *The ideal classes in $\mathfrak{O}$ form a group*

Proof. We define multiplication in the natural way: if $[\mathfrak{a}]$ and $[\mathfrak{b}]$ are ideal classes, then $[\mathfrak{a}] \cdot [\mathfrak{b}] = [\mathfrak{ab}]$. This is well defined: suppose $\mathfrak{a}_1 \sim \mathfrak{a}_2$ and $\mathfrak{b}_1 \sim \mathfrak{b}_2$; then $\mathfrak{a}_2 = \alpha_1 \alpha_2^{-1} \mathfrak{a}_1$ and $\mathfrak{b}_2 = \beta_1 \beta_2^{-1} \mathfrak{b}_1$ for $\alpha_1, \alpha_2, \beta_1, \beta_2 \in \mathfrak{O}$. Therefore $\mathfrak{a}_1 \mathfrak{b}_1 = \alpha_1^{-1} \alpha_2 \beta_1^{-1} \beta_2 \mathfrak{a}_2 \mathfrak{b}_2$, or $\alpha_1 \beta_1 \mathfrak{a}_1 \mathfrak{b}_1 = \alpha_2 \beta_2 \mathfrak{a}_2 \mathfrak{b}_2$, so $[\mathfrak{a}_1 \mathfrak{b}_1] = [\mathfrak{a}_2 \mathfrak{b}_2]$.

Since multiplication of ideals is closed and associative, so is the multiplication of ideal classes. The identity element is the ideal class of the whole number ring $[\mathfrak{O}]$, since $[\mathfrak{a}][\mathfrak{O}] = [\mathfrak{aO}] = [\mathfrak{a}]$. Finally, we find that the inverse of the class $[\mathfrak{a}]$ is the class of the ideal we found above in Theorem 2.15: for our $\mathfrak{a}$, consider the class of the ideal $\mathfrak{b}$ such that $\mathfrak{ab}$ is principle, say $\mathfrak{ab} = \langle a \rangle$. Then $[\mathfrak{a}][\mathfrak{b}] = [\mathfrak{ab}] = [\langle a \rangle] = [\mathfrak{O}]$ since $1\langle a \rangle = \langle a \rangle = a\mathfrak{O}$. ☆

We continue by looking at some of the implications of this result:

Corollary 2.17. *If $\mathfrak{a}$, $\mathfrak{b}$, and $\mathfrak{c}$ are ideals in a number ring, then $\mathfrak{ab} = \mathfrak{ac}$ implies $\mathfrak{b} = \mathfrak{c}$.*

Proof. We know there exists an ideal $\overline{\mathfrak{a}}$ such that $\mathfrak{a}\overline{\mathfrak{a}}$ is principle, say $\mathfrak{a}\overline{\mathfrak{a}} = \langle a \rangle$. Multiply the equation $\mathfrak{ab} = \mathfrak{ac}$ by $\overline{\mathfrak{a}}$, and we have $a\mathfrak{b} = a\mathfrak{c}$, and thus $\mathfrak{b} = \mathfrak{c}$. ☆

The following corollary is the exact same result as Proposition 2.10, but is proved in a slightly different way:

Corollary 2.18. *For ideals $\mathfrak{a}$ and $\mathfrak{b}$ of $\mathfrak{O}$, $\mathfrak{a}|\mathfrak{b}$ if and only if $\mathfrak{a} \supseteq \mathfrak{b}$.*

Proof. If $\mathfrak{a}|\mathfrak{b}$, then $\mathfrak{b} = \mathfrak{ac}$ for some ideal $\mathfrak{c}$, and then clearly $\mathfrak{a} \supseteq \mathfrak{b}$. Note that this direction is in fact the argument used in Proposition 2.10.

The converse is not proved the same way. Assume $\mathfrak{a} \supseteq \mathfrak{b}$, and take $\overline{\mathfrak{a}}$ such that $\mathfrak{a}\overline{\mathfrak{a}}$ is principle, say $\mathfrak{a}\overline{\mathfrak{a}} = \langle a \rangle$. We now define $\mathfrak{c} = a^{-1}\overline{\mathfrak{a}}\mathfrak{b}$, and note $\mathfrak{c} = a^{-1}\overline{\mathfrak{a}}\mathfrak{b} \subseteq a^{-1}\overline{\mathfrak{a}}\mathfrak{a} = a^{-1}\langle a \rangle = \mathfrak{O}$. We can then say $\mathfrak{c}$ is an ideal since both $\overline{\mathfrak{a}}$ and $\mathfrak{b}$ are, and further, that $\mathfrak{a}\mathfrak{c} = a^{-1}\overline{\mathfrak{a}}\mathfrak{a}\mathfrak{b} = a^{-1}\langle a \rangle \mathfrak{b} = \mathfrak{O}\mathfrak{b} = \mathfrak{b}$, as desired. ☆

We can now prove unique factorization using this method:

Theorem 2.19. *Every non-zero ideal $\mathfrak{a}$ of $\mathfrak{O}$ can be written as a product of prime ideals, uniquely up to order*

Proof. Suppose not, and consider the set of ideals not representable in this fashion. Since $\mathfrak{O}$ is noetherian, this set has some maximal element $\mathfrak{a}$. We know $\mathfrak{a}$ is contained in some prime (and therefore maximal) ideal $\mathfrak{p}$ so $\mathfrak{a} \subseteq \mathfrak{p}$. By our new definition, this means $\mathfrak{p}|\mathfrak{a}$, so $\mathfrak{a} = \mathfrak{b}\mathfrak{p}$ for some ideal $\mathfrak{b}$ by Corollary 2.18. We have that $\mathfrak{b} \supsetneq \mathfrak{a}$, since if $\mathfrak{b} = \mathfrak{a}$, we would have $\mathfrak{a}\mathfrak{p} = \mathfrak{b}\mathfrak{p} = \mathfrak{a} = \mathfrak{a}\mathfrak{O}$, hence $\mathfrak{O} = \mathfrak{p}$ by Corollary 2.17, a contradiction. Thus $\mathfrak{b}$ is larger than $\mathfrak{a}$, and hence, by the maximality of $\mathfrak{a}$, $\mathfrak{b}$ is a product of primes. But then, by the above equality, so is $\mathfrak{a}$.

For uniqueness, suppose we have two equal factorizations into primes: $\mathfrak{a} = \mathfrak{p}_1 \dots \mathfrak{p}_r = \mathfrak{q}_1 \dots \mathfrak{q}_s$. Then $p_1 \supseteq \mathfrak{q}_1 \dots \mathfrak{q}_s$ and hence $\mathfrak{p}_1 \supseteq \mathfrak{q}_i$. Renumbering if necessary let $\mathfrak{p}_1 \supseteq \mathfrak{q}_1$. But since both are prime (and therefore maximal), we have $\mathfrak{p}_1 = \mathfrak{q}_1$. Applying cancellation, and continuing inductively in this manor we have $\mathfrak{p}_i = \mathfrak{q}_i$ for all i. ☆

2.3 Comparison

As noted in some of the proofs, there is great similarity between these methods. They both use their constructions to devise a method to remove an ideal from one side of an equation; using fractional ideals we explicitly define the inverse of an ideal, while using ideal classes we reduce any ideal to a principle ideal and then can indirectly remove it. This is very noticeable in the final proof of unique factorization: if we look at the second proof above, the exact same operation performed by Corollary 2.17 could have been completed by multiplying the equation by $\mathfrak{a}^{-1}$, yielding an identical proof. The formal relationship between these concepts is demonstrated in the following proposition:

Proposition 2.20. *Let $\mathfrak{a}$ be an ideal, and $\overline{\mathfrak{a}}$ the ideal such that $\mathfrak{a}\overline{\mathfrak{a}} = \langle a \rangle$ for some $a \in \mathfrak{O}$. Then $\mathfrak{a}^{-1} = a^{-1}\overline{\mathfrak{a}}$.*

Proof. We know that $\mathfrak{O} = \mathfrak{a}\mathfrak{a}^{-1}$ and $\mathfrak{O} = \langle a \rangle a^{-1} = \mathfrak{a}\overline{\mathfrak{a}}a^{-1}$. Since inverses in a group are unique, we see $\mathfrak{a}^{-1} = a^{-1}\overline{\mathfrak{a}}$.

This slight variation between the methods accounts for the differences in the proof of Proposition 2.10 and Corollary 2.18. The other difference occurs in the proof that an ideal is equal to a product of primes. This is due to the different processes used to force a maximal $\mathfrak{a}$ (maximal with respect to not equaling a product of primes) to actually equal a product of primes.

Both these methods discussed above are equivalent once we have the following relation:

Proposition 2.21. *Two ideals $\mathfrak{a}$ and $\mathfrak{b}$ are in the same ideal class if and only if there exists a fractional ideal $\mathfrak{f}$ that has representations $\mathfrak{f} = c_1^{-1}\mathfrak{a}$ and $\mathfrak{f} = c_2^{-1}\mathfrak{b}$.*

Proof. If $\mathfrak{a} \sim \mathfrak{b}$ then $\alpha\mathfrak{a} = \beta\mathfrak{b}$, so $\beta^{-1}\mathfrak{a} = \alpha^{-1}\mathfrak{b} = \mathfrak{f}$, and $\mathfrak{f}$ is a single fractional ideal with two representations using our ideals. Conversely, if we have a fractional ideal $\mathfrak{f} = \beta^{-1}\mathfrak{a} = \alpha^{-1}\mathfrak{b}$ then $\alpha\mathfrak{a} = \beta\mathfrak{b}$, as desired. ☆

2.4 Examples and Consequences

Each ideal of every number ring $\mathfrak{O}$ has a unique factorization into prime ideals. Let us calculate such a factorization for some specific examples:

Example 2.22. Consider Example 1.75 at the end of Chapter 1: we defined $K = \mathbb{Q}[\sqrt{-5}]$, $\mathfrak{O} = \mathbb{Z}[\sqrt{-5}]$, and showed that $6 = 2 \cdot 3 = (1 + \sqrt{-5})(1 - \sqrt{-5})$ is an example of non-unique factorization, since all elements to the right of 6 are irreducible. However, if we now consider the ideals of $\mathfrak{O}$ associated with these elements, we see that these four elements are in fact

not prime ideals, but instead are reducible:

$$\begin{aligned}
\langle 2\rangle &= \langle 2, 1+\sqrt{-5}\rangle^2 \\
\langle 3\rangle &= \langle 3, 1+\sqrt{-5}\rangle\langle 3, 1-\sqrt{-5}\rangle \\
\langle 1+\sqrt{-5}\rangle &= \langle 2, 1+\sqrt{-5}\rangle\langle 3, 1+\sqrt{-5}\rangle \\
\langle 1-\sqrt{-5}\rangle &= \langle 2, 1+\sqrt{-5}\rangle\langle 3, 1-\sqrt{-5}\rangle
\end{aligned}$$

Let us check the first of these cases (the arguments for the others are similar). Multiplication of generators yields:

$$\langle 2, 1+\sqrt{-5}\rangle^2 = \langle 4, 2+2\sqrt{-5}, -4+2\sqrt{-5}\rangle;$$

and so $\langle 2, 1+\sqrt{-5}\rangle^2 \subseteq \langle 2\rangle$ since:

$$\begin{aligned}
&(a+b\sqrt{-5})[4] + (c+d\sqrt{-5})[2+2\sqrt{-5}] + (e+f\sqrt{-5})[-4+2\sqrt{-5}] \\
&\qquad = \Big[(2a+c-5d-2e-5f) + (2b+c+d+e-2f)\sqrt{-5}\Big][2] \in \langle 2\rangle.
\end{aligned}$$

Note then that $(2+2\sqrt{-5}) - (-4+2\sqrt{-5}) - (4) = 2$, so $2 \in \langle 2, 1+\sqrt{-5}\rangle^2$. Hence $\langle 2\rangle \subseteq \langle 2, 1+\sqrt{-5}\rangle^2$ since $\langle 2\rangle$ is the smallest ideal containing 2.

Further, the ideals on the right are prime. Note that $\mathfrak{O}/\langle 2\rangle = \{2(a+b\sqrt{-5} \mid a, b \in \mathbb{Z}\}$, and then we have $|\mathfrak{O}/\langle 2\rangle| = 4$ since $2+2\sqrt{-5}$, 2, and $2\sqrt{-5}$ are in $\langle 2\rangle$, which forces the options of a and b in our explicit formulation of $\mathfrak{O}/\langle 2\rangle$ to strictly 0 and 1. Thus $|\mathfrak{O}/\langle 2, 1+\sqrt{-5}\rangle|$ must divide 4, and since $\langle 2, 1+\sqrt{-5}\rangle$ properly contains $\langle 2\rangle$ and is properly contained in $\mathfrak{O}$, it must have order 2. Thus $\langle 2, 1+\sqrt{-5}\rangle$ is maximal, and hence prime. The cases for the other factors are similar.

Thus, we see that when these elements (via their principle ideals) are factored into prime (but not principle) ideals, the two factorizations of 6 are actually the same; these four factors are actual multiples of the three "true" factors (in the ideal sense) of 6.

Example 2.23. Let us now take $K = \mathbb{Q}[i]$, and then by our comment on quadratic fields in Example 1.25, we see $\mathfrak{O} = \mathbb{Z}[i]$. This number ring is very important in number theory,

and called the *Gaussian Integers*. We then have the factorizations:

$$\langle 2\rangle = \langle 1-i\rangle^2$$
$$\langle 5\rangle = \langle 2+i\rangle\langle 2-i\rangle$$

A similar argument to that in Example 2.22 will show that all the ideals on the right are prime, demonstrating how, even in a PID, primes can split.

Example 2.24. Finally, let $K = \mathbb{Q}[\sqrt{-17}]$, again by Example 1.25 we know $\mathfrak{O} = \mathbb{Z}[\sqrt{-17}]$. We consider the factorization of the element 18 and its associated principle ideal $\langle 18\rangle$. As above, we can show the factors on the right are prime and are indeed divisors of the objects on the left [see Stewart and Tall [7] p.111 for details]:

$$18 = 2\cdot 3\cdot 3 = (1+\sqrt{-17})(1-\sqrt{-17})$$
$$\langle 18\rangle = \langle 2, 1+\sqrt{-17}\rangle^2\langle 3, 1+\sqrt{-17}\rangle^2\langle 3, 1-\sqrt{-17}\rangle^2$$
$$\langle 2\rangle = \langle 2, 1+\sqrt{-17}\rangle^2$$
$$\langle 3\rangle = \langle 3, 1+\sqrt{-17}\rangle\langle 3, 1-\sqrt{-17}\rangle$$

This last example is similar to Example 2.22 above, in that the non-unique factorization of the element 18 parallels the fact that the prime factors of $\langle 18\rangle$ are not principle ideals, and thus they cannot be properly represented, if you will, as elements of $\mathfrak{O}$. This idea actually holds true in all number rings, and demonstrates a very powerful relationship between the *ideals* of $\mathfrak{O}$ and the factorization of *elements* of $\mathfrak{O}$: we will show that the factorization of elements of $\mathfrak{O}$ into irreducibles is unique if and only if every ideal of $\mathfrak{O}$ is principle.

In order to prove this result, we must explore other consequences of unique factorization of ideals. We will continue to naturally extend the definitions typically given for the integers, and applying them to the ideals in a number ring $\mathfrak{O}$.

Definition 2.25. An ideal $\mathfrak{g}$ is the *greatest common divisor of the ideals* $\mathfrak{a}$ *and* $\mathfrak{b}$, written $gcd(\mathfrak{a}, \mathfrak{b})$, if:

(i) $\mathfrak{g}|\mathfrak{a}$ and $\mathfrak{g}|\mathfrak{b}$; and

(ii) If $\mathfrak{g}'$ is an ideal such that $\mathfrak{g}'|\mathfrak{a}$ and $\mathfrak{g}'|\mathfrak{b}$, then $\mathfrak{g}'|\mathfrak{g}$.

Definition 2.26. An ideal $\mathfrak{l}$ is the *least common multiple of* $\mathfrak{a}$ *and* $\mathfrak{b}$, written $lcm(\mathfrak{a}, \mathfrak{b})$, if:

(i) $\mathfrak{a}|\mathfrak{l}$ and $\mathfrak{b}|\mathfrak{l}$; and

(ii) If $\mathfrak{l}'$ is an ideal such that $\mathfrak{a}|\mathfrak{l}'$ and $\mathfrak{b}|\mathfrak{l}'$, then $\mathfrak{l}|\mathfrak{l}'$.

Clearly, as in the integers, if $\mathfrak{a} = \mathfrak{p}_1^{e_1} \dots \mathfrak{p}_r^{e_r}$ and $\mathfrak{b} = \mathfrak{p}_1^{s_1} \dots \mathfrak{p}_r^{s_r}$ for some primes $\mathfrak{p}_i$ and integers e_i and s_i (which need not be all non-zero):

$$\mathfrak{g} = \prod \mathfrak{p}_i^{\min\{e_i, s_i\}} \quad \text{and} \quad \mathfrak{l} = \prod \mathfrak{p}_i^{\max\{e_i, s_i\}}.$$

Proposition 2.27. *Let* $\mathfrak{a}$, $\mathfrak{b}$ *be ideals. Then:*

(i) $gcd(\mathfrak{a}, \mathfrak{b}) = \mathfrak{a} + \mathfrak{b}$;

(ii) $lcm(\mathfrak{a}, \mathfrak{b}) = \mathfrak{a} \cap \mathfrak{b}$;

Proof. We know that $\mathfrak{c}|\mathfrak{a}$ if and only if $\mathfrak{c} \supseteq \mathfrak{a}$ by Proposition 2.10. Hence $\mathfrak{g}$ must be the smallest ideal containing $\mathfrak{a}$ and $\mathfrak{b}$, and $\mathfrak{l}$ the largest ideal contained within $\mathfrak{a}$ and $\mathfrak{b}$. The rest follows easily. ☆

This exemplifies the seemingly reversed nature of factorization of ideals, where divisors of an ideal contain the original ideal, and multiples of an ideal are contained in the original factor: the greatest common divisor is the smallest ideal that is larger than both our original ideals, and the least common multiple is the largest ideal contained within them.

Some of our earlier examples exploited the simplicity of principle ideal domains. While we will consider other types of domains, we can now show that all ideals in any number ring can be generated by at most two elements:

Theorem 2.28. *Let* $\mathfrak{a}$ *be an ideal in a our number ring* $\mathfrak{O}$*, and let* α *be a non-zero element of* $\mathfrak{a}$*. Then there exists an element* $\beta \in \mathfrak{a}$ *such that* $\mathfrak{a} = \langle \alpha, \beta \rangle = \langle \alpha \rangle + \langle \beta \rangle$.

Proof. Since all ideals have unique factorization, let $\mathfrak{a} = \mathfrak{p}_1^{e_1} \dots \mathfrak{p}_r^{e_r}$ for some primes $\mathfrak{p}_i$. Then, since $\langle \alpha \rangle \subseteq \mathfrak{a}$, $\langle \alpha \rangle = \mathfrak{a}h = \mathfrak{p}_1^{e_1} \dots \mathfrak{p}_r^{e_r} h$ for some ideal h; thus each $\mathfrak{p}_i$ divides $\langle \alpha \rangle$. Note that $\langle \alpha \rangle$ also has a unique factorization, and with the above conclusion in mind we

see $\langle\alpha\rangle = \mathfrak{p}_1^{e_1} \dots \mathfrak{p}_r^{e_r} \mathfrak{q}_1 \dots \mathfrak{q}_s \overline{\mathfrak{p}}_1 \dots \overline{\mathfrak{p}}_t$, where the $\overline{\mathfrak{p}}_k$ are powers of primes not distinct from the $\mathfrak{p}_i$, and the $\mathfrak{q}_j$ are powers of primes distinct from the $\mathfrak{p}_i$.

By our proposition above, we must find a β such that $gcd(\langle\alpha\rangle, \langle\beta\rangle) = \mathfrak{a}$. Further, by our remark after the definition of *gcd*, this means we must find a β such that none of these $\mathfrak{q}_j$ also divide $\langle\beta\rangle$; such a $\mathfrak{q}_j$ would then divide $\mathfrak{a}$, contradicting the unique factorization of $\mathfrak{a}$. Note that this restriction must disallow both higher and lower powers of the $\mathfrak{p}_i$ as well as any powers of new primes found among the $\mathfrak{q}_j$. Thus, formally, we must find a β such that:

$$\beta \in \left(\bigcap_{i=1}^{r} (\mathfrak{p}_i^{e_i} \backslash \mathfrak{p}_i^{e_i+1}) \right) \bigcap \left(\bigcap_{j=1}^{s} (\mathfrak{O} - \mathfrak{q}_j) \right);$$

where the first set restricts to the exact powers of the $\mathfrak{p}_i$ found in $\mathfrak{a}$, and the second requires β to not be in any $\mathfrak{q}_j$.

We can construct this β using the Theorem 1.51, the Chinese Remainder Theorem. In each set $(\mathfrak{p}_i^{e_i} \backslash \mathfrak{p}_i^{e_i+1})$, take some element β_l (these sets are non-empty since factorization into prime ideals is unique). Then note that, for all i and j, $\mathfrak{p}_i^{e_i+1} + \mathfrak{q}_j = \mathfrak{O}$ since the sum is equal to the greatest common divisor, which clearly must be the entire number ring. Now let β satisfy the following system of congruences via the Chinese Remainder Theorem:

$$\begin{aligned} \beta &\equiv \beta_i \pmod{\mathfrak{p}_i^{e_i+1}} && \text{for } i = 1, \dots, r \\ \beta &\equiv 1 \pmod{\mathfrak{q}_j} && \text{for } j = 1, \dots, s \end{aligned}$$

This β works, as desired. ☆

We also now have a correlation between prime elements and prime principle ideals:

Proposition 2.29. *Let $\alpha \in \mathfrak{O}$. Then α is a prime element if and only if $\langle\alpha\rangle$ is a prime ideal.*

Proof. Suppose $\langle\alpha\rangle$ is prime, and assume, for contraction, α has a unique factorization $\alpha = p_1 \dots p_r$. Then $\langle\alpha\rangle = \langle p_1\rangle \dots \langle p_r\rangle$, but since $\langle\alpha\rangle$ is prime it has no proper factorization, so all but one of the factors $\langle p_j\rangle = \mathfrak{O}$. Thus all but one p_i are units, and hence α has no proper factorization itself, and is thus irreducible. By Theorem 1.72, since $\mathfrak{O}$ is a unique factorization domain, α is prime.

Conversely, Suppose α is prime, and let $ab \in \langle\alpha\rangle$. Then $\langle a\rangle\langle b\rangle \subseteq \langle\alpha\rangle$, so $ab = r\alpha$ for some $r \in \mathfrak{O}$. Thus $\alpha|ab$, hence $\alpha|a$ or $\alpha|b$ since α is prime. Therefore $a \in \langle\alpha\rangle$ or $b \in \langle\alpha\rangle$, so $\langle\alpha\rangle$ is prime. ☆

We can now prove our desired result:

Theorem 2.30. *Factorization of elements of $\mathfrak{O}$ into irreducibles is unique if and only if every ideal of $\mathfrak{O}$ is principle.*

Proof. The "only if" is straightforward as a result from ring theory (see HOWIE [4] p.32). For the converse, let $\mathfrak{O}$ be a unique factorization domain. We will show every prime ideal is principle; the general result will follow since any ideal $\mathfrak{a}$ would be a unique product of principle ideals, and would hence itself be principle.

Let $\alpha \in \mathfrak{p}$. Then by the argument in Lemma 1.67, we know $m = N(\alpha) \in \mathbb{Z} \cap \mathfrak{p}$, and hence $\langle m\rangle \subseteq \mathfrak{p}$ and $\mathfrak{p}|\langle m\rangle$. Let us factor m in $\mathfrak{O}$, say $m = \lambda_1 \dots \lambda_s$. Then, since $\mathfrak{p}$ is prime, $\mathfrak{p}|\langle\lambda_i\rangle$ for some i. Further, by Proposition 2.29, each $\langle\lambda_i\rangle$ is prime. Thus, by uniqueness of factorization, $\mathfrak{p} = \langle\lambda_i\rangle$ for some i, and hence is principle. ☆

As a demonstration, suppose $\alpha \in \mathfrak{O}$ is irreducible but not prime for some number ring $\mathfrak{O}$. Then the principle ideal $\langle\alpha\rangle$ is not prime, so has a factorization into prime ideals $\langle\alpha\rangle = \mathfrak{p}_1 \dots \mathfrak{p}_r$. Now *none* of the $\mathfrak{p}_i$ can be principle, for if $\mathfrak{p}_i = \langle p\rangle$, then we'd have $\langle p\rangle|\langle\alpha\rangle$, implying $p|\alpha$. But since α is irreducible, this would require p to either be a unit (which would contradict $\langle p\rangle$ being prime), or an associate of α and hence making $\langle\alpha\rangle = \mathfrak{p}_i$ (which would contradict our assumption that $\langle\alpha\rangle$ is not prime).

In summary, we see that a number ring $\mathfrak{O}$ always has unique factorization of ideals. Further, it has unique factorization of elements into irreducibles if and only if all irreducibles are primes. In this case, the factorization of elements exactly corresponds to factorization of principle ideals. However, if $\mathfrak{O}$ does not have unique factorization of elements, the principle ideal of any non-prime element factors into a product of prime ideals, each with exactly two generators.

Chapter 3

Primes in Extensions

In this chapter, we will further explore the behavior of prime ideals. Using the main result of the last chapter, that the ideals of a number ring factor uniquely into prime ideals, we will build on this, but in a slightly different setting. Whereas before we only considered some number field K over $\mathbb{Q}$, here we will look at a towers of fields L over K, both containing $\mathbb{Q}$. We find that almost all definitions in which K is an extension of $\mathbb{Q}$ can be extended to the case where L is an extension of K: we retain the definition of algebraic numbers and algebraic integers (since both our fields L and K are also important as number fields over $\mathbb{Q}$), leading us to define two rings of integers, $\mathfrak{O}_K$ and $\mathfrak{O}_L$, one for each number field. We will also now consider polynomials with coefficients in K, and we can define norms and traces of elements in L, both over K as well as over $\mathbb{Q}$;

Definition 3.1. Let K and L be number fields with $K \subseteq L$, and n the degree of L over K. Denote with $\sigma_1, \ldots, \sigma_n$ the n embeddings of L in $\mathbb{C}$ which fix K pointwise. We then define the norm and trace of an element α in L over K (as opposed to over Q), N_K^L and T_K^L, respectively, to be defined:

$$N_K^L(\alpha) = \prod_{i=1}^{n} \sigma_i(\alpha); \quad \text{and} \quad T_K^L(\alpha) = \sum_{i=1}^{n} \sigma_i(\alpha).$$

With this notation, we have $N^K = N_{\mathbb{Q}}^K$ and $T^K = T_{\mathbb{Q}}^K$. Further, we define the field polynomial of α over K to be $f(x) = \prod(x - \sigma_i(\alpha))$. These extended definitions allows us to state and prove a new version Proposition 1.19:

Proposition 3.2. *Let K and L be number fields with $K \subseteq L$, $\mathfrak{O}_K$ and $\mathfrak{O}_L$ the associated rings of integers. Then for all $\alpha \in \mathfrak{O}_L$, $N_K^L(\alpha) \in \mathfrak{O}_K$.*

Proof. Since α is an integer, let $p(t) = t^n + m_{n-1}t^{n-1} + \ldots + m_1 t + m_0$ be the minimum, monic, irreducible polynomial of α over K; then we have $m_i \in \mathfrak{O}_K$. Let $\sigma_1, \ldots, \sigma_n$ denote the embeddings of L in $\mathbb{C}$ which fix K pointwise. Then consider field polynomial f of α over K, and note that it is a power of p by the argument of Proposition 1.18. Further notice that the norm of α is a power of the constant term in f. Therefore the norm must be a power of an element in $\mathfrak{O}_K$, and thus must be in $\mathfrak{O}_K$, as desired. ☆

3.1 Splitting of Primes in Extensions

We will find that ideals which are prime in K need not remain prime when considered as ideals of L; we will explore exactly how these primes split into a prime factorization in L. We begin by formalizing the notation discussed above to denote the rings and fields with which we will be working. Let K and L be number fields with $K \subseteq L$, and let $\mathfrak{O}_K = \mathbb{B} \cap K$, $\mathfrak{O}_L = \mathbb{B} \cap L$; i.e. let $\mathfrak{O}_K$ and $\mathfrak{O}_L$ be the respective rings of integers in these number fields. We will use $\mathfrak{p}$ as a prime (ideal) in $\mathfrak{O}_K$, and $\mathfrak{q}$ as a prime (ideal) in $\mathfrak{O}_L$. When we stated above, informally, that primes of K need not also be primes of L, what we are really considering is the prime factorization of the ideal generated by some prime $\mathfrak{p}$ of $\mathfrak{O}_K$ in the larger number ring $\mathfrak{O}_L$, which is the ideal $\mathfrak{p}\mathfrak{O}_L$. This ideal, $\mathfrak{p}\mathfrak{O}_L$, need not be prime in $\mathfrak{O}_L$ even if $\mathfrak{p}$ is prime in $\mathfrak{O}_K$.

This phenomenon is called "splitting":

Definition 3.3. Let $\mathfrak{O}_K$ and $\mathfrak{O}_L$ be number rings, $\mathfrak{O}_K \subseteq \mathfrak{O}_L$, and $\mathfrak{p}$ a prime ideal in $\mathfrak{O}_K$. We say $\mathfrak{p}$ *splits* in $\mathfrak{O}_L$ if $\mathfrak{p}\mathfrak{O}_L$ is not a prime ideal in $\mathfrak{O}_L$.

Example 3.4. We saw above that, for $K = \mathbb{Q}$ and $L = \mathbb{Q}[\sqrt{-5}]$, in $\mathfrak{O}_L = \mathbb{Z}[\sqrt{-5}]$ the ideal $3\mathfrak{O}_L = \langle 3, 1 + \sqrt{-5}\rangle\langle 3, 1 - \sqrt{-5}\rangle$, even though $\langle 3\rangle$ is prime in $\mathfrak{O}_K = \mathbb{Z}$.

For the remainder of this chapter, we will be exploring the ways in which primes split in various field extensions. We begin with a proposition which relates primes in various

extensions to each other:

Proposition 3.5. *Let K, L, $\mathfrak{O}_K$, $\mathfrak{O}_L$, $\mathfrak{p}$, and $\mathfrak{q}$ be as above. Then the following conditions are equivalent:*

(i) $\mathfrak{q} \mid \mathfrak{p}\mathfrak{O}_L$

(ii) $\mathfrak{q} \supseteq \mathfrak{p}\mathfrak{O}_L$

(iii) $\mathfrak{q} \supseteq \mathfrak{p}$

(iv) $\mathfrak{q} \cap \mathfrak{O}_K = \mathfrak{p}$

(v) $\mathfrak{q} \cap K = \mathfrak{p}$

Proof. $(i) \leftrightarrow (ii)$: Corollary 2.18;

$(ii) \leftrightarrow (iii)$: Trivial since $\mathfrak{q}$ is an ideal in $\mathfrak{O}_L$;

$(iv) \rightarrow (iii)$: Trivial;

$(iv) \leftrightarrow (v)$: Trivial since $\mathfrak{q} \subseteq \mathbb{B}$ and $K \cap \mathbb{B} = \mathfrak{O}_K$;

$(iii) \rightarrow (iv)$: Note that $\mathfrak{q} \cap \mathfrak{O}_K$ contains $\mathfrak{p}$ and is an ideal in $\mathfrak{O}_K$; since $\mathfrak{p}$ is maximal by Theorem 1.68, we have $\mathfrak{q} \cap \mathfrak{O}_K$ must equal $\mathfrak{p}$ or $\mathfrak{O}_K$. If $\mathfrak{q} \cap \mathfrak{O}_K = \mathfrak{O}_K$, then $1 \in \mathfrak{q}$, implying $\mathfrak{q} = \mathfrak{O}_L$, a contradiction. Thus $\mathfrak{q} \cap \mathfrak{O}_K = \mathfrak{p}$. ☆

Definition 3.6. Let $\mathfrak{p}$ and $\mathfrak{q}$ be as above. When the properties listed above in Proposition 3.5 hold, we say that $\mathfrak{q}$ *lies over* $\mathfrak{p}$, and $\mathfrak{p}$ *lies under* $\mathfrak{q}$.

Example 3.7. In Example 3.4 above, we had a factorization $\langle 3 \rangle = \langle 3, 1+\sqrt{-5} \rangle \langle 3, 1-\sqrt{-5} \rangle$. Thus $\langle 3, 1 \pm \sqrt{-5} \rangle$ are exactly the two primes of L lying over $\langle 3 \rangle$.

This definition allows us to see towers of primes, in towers of number rings, in towers of number fields.

Theorem 3.8. *Let $\mathfrak{O}_K$ and $\mathfrak{O}_L$ be as above. Then:*

(i) Every prime $\mathfrak{q}$ of $\mathfrak{O}_L$ lies over a unique prime $\mathfrak{p}$ of $\mathfrak{O}_K$.

(ii) Every prime $\mathfrak{p}$ of $\mathfrak{O}_K$ lies under at least one prime $\mathfrak{q}$ of $\mathfrak{O}_L$.

Proof. By Proposition 3.5, proving (i) is equivalent to showing $\mathfrak{p} = \mathfrak{q} \cap \mathfrak{O}_K$ is prime in $\mathfrak{O}_K$, since $\mathfrak{q}$ can only lie over one prime in $\mathfrak{O}_K$.

Note first that there is an obvious way in which $\mathfrak{O}_K/\mathfrak{p}$ is contained in $\mathfrak{O}_L/\mathfrak{q}$: we already have $\mathfrak{O}_K \subseteq \mathfrak{O}_L$, and this containment induces a homomorphism $\mathfrak{O}_K \to \mathfrak{O}_L/\mathfrak{q}$, with kernel $\mathfrak{q} \cap \mathfrak{O}_K = \mathfrak{p}$. Therefore, by the First Homomorphism Theorem we have a mapping $\psi : \mathfrak{O}_K/\mathfrak{p} \to \mathfrak{O}_L/\mathfrak{q}$. Note that ψ is an injection: if we have $\psi(r + \mathfrak{p}) = \psi(\overline{r} + \mathfrak{p})$, it must be that $r + \mathfrak{q} = \overline{r} + \mathfrak{q}$, and hence $r - \overline{r} \in \mathfrak{q}$. However, we also know that r and $\overline{r}$ are in $\mathfrak{O}_K$, so $r - \overline{r} \in \mathfrak{q} \cap \mathfrak{O}_K$, or $r + \mathfrak{q} \cap \mathfrak{O}_K = \overline{r} + \mathfrak{q} \cap \mathfrak{O}_K$ also holds, and so $r + \mathfrak{p} = \overline{r} + \mathfrak{p}$. Thus $\mathfrak{O}_K/\mathfrak{p}$ is embedded in $\mathfrak{O}_L/\mathfrak{q}$. Since $\mathfrak{O}_L/\mathfrak{q}$ is a field, $\mathfrak{O}_K/\mathfrak{p}$ must then be a domain; by Theorem 1.54 this implies $\mathfrak{p}$ is a prime ideal. Finally, we know $\mathfrak{p} \neq \mathfrak{O}_K$ since if $\mathfrak{q} \cap \mathfrak{O}_K = \mathfrak{p} = \mathfrak{O}_K$, and hence $1 \in \mathfrak{q}$, contradicting $\mathfrak{q}$ being a proper prime ideal. Thus $\mathfrak{p}$ is a proper prime ideal.

For (ii), we know that the primes lying over $\mathfrak{p}$ are the prime divisors of $\mathfrak{p}\mathfrak{O}_L$. Thus, we must show that $\mathfrak{p}\mathfrak{O}_L \neq \mathfrak{O}_L$, implying that $\mathfrak{p}\mathfrak{O}_L$ has at least one prime divisor. Equivalently, we can show $1 \notin \mathfrak{p}\mathfrak{O}_L$. Note that even though we know $1 \notin \mathfrak{p}$, it is non-trivial to show that there do not exist some $\alpha_i \in \mathfrak{p}$ and $\beta_i \in \mathfrak{O}_L$ such that $1 \neq \alpha_1\beta_1 + ... + \alpha_r\beta_r$.

To show $1 \notin \mathfrak{p}\mathfrak{O}_L$, we use Lemma 2.2 to find a $\gamma \in K \backslash \mathfrak{O}_K$ such that $\gamma\mathfrak{p} \subseteq \mathfrak{O}_K$. Then $\gamma\mathfrak{p}\mathfrak{O}_L \subseteq \mathfrak{O}_K\mathfrak{O}_L = \mathfrak{O}_L$. Suppose $1 \in \mathfrak{p}\mathfrak{O}_L$; then $\gamma \in \mathfrak{O}_L$. But then γ is an algebraic integer by the definition of $\mathfrak{O}_L$, contradicting $\gamma \notin K \backslash \mathfrak{O}_K$. ☆

Let us extract part of the discussion in this proof, as it is vital to our exploration. The above proposition states that the ideal $\mathfrak{q}$ of $\mathfrak{O}_L$ lies over exactly one prime of $\mathfrak{O}_K$, namely $\mathfrak{p} = \mathfrak{q} \cap \mathfrak{O}_K$. Since $\mathfrak{p}$ and $\mathfrak{q}$ are prime in their respective fields, $\mathfrak{O}_K/\mathfrak{p}$ and $\mathfrak{O}_L/\mathfrak{q}$ are finite fields by Theorem 1.68 and Lemma 1.67.

Definition 3.9. The fields $\mathfrak{O}_K/\mathfrak{p}$ and $\mathfrak{O}_L/\mathfrak{q}$ are called the *residue fields associated with* $\mathfrak{p}$ *and* $\mathfrak{q}$.

Further, we have seen that there is a natural mapping between the quotient fields $\mathfrak{O}_K/\mathfrak{p}$ and $\mathfrak{O}_L/\mathfrak{q}$. In fact, this mapping is 1-1 since the kernel is trivial: $\mathfrak{O}_K \cap \mathfrak{q}/\mathfrak{p} = \mathfrak{p}/\mathfrak{p}$. Thus we have an embedding $\mathfrak{O}_K/\mathfrak{p} \to \mathfrak{O}_L/\mathfrak{q}$, and hence another tower of containments, parallel

to the first ($K \subseteq L$). Since the both fields are finite, we know $\mathfrak{O}_L/\mathfrak{q}$ is a finite extension of $\mathfrak{O}_K/\mathfrak{p}$.

Definition 3.10. With $\mathfrak{O}_L$, $\mathfrak{O}_K$, $\mathfrak{q}$, and $\mathfrak{p}$ as above, the degree of the extension $\mathfrak{O}_L/\mathfrak{q}$ over $\mathfrak{O}_K/\mathfrak{p}$ is called the *inertial degree of* $\mathfrak{q}$ *over* $\mathfrak{p}$, *denoted* $f = f(\mathfrak{q}|\mathfrak{p})$.

Example 3.11. Consider Example 2.22, with $\langle 2\rangle$ lying under $\langle 2, 1+\sqrt{-5}\rangle$. We see $\mathfrak{O}_L/2\mathfrak{O}_L$ has order 4, and $2\mathfrak{O}_L \subsetneq \langle 2, 1+\sqrt{-5}\rangle$. Therefore $|\mathfrak{O}_L/\langle 2, 1+\sqrt{-5}\rangle|$ must be a proper divisor of 4, the only possibility being 2. So $|\mathfrak{O}_L/\langle 2, 1+\sqrt{-5}\rangle| = 2$. Then, since $\mathfrak{O}_K/\langle 2\rangle$ is contained in $\mathfrak{O}_L/\langle 2, 1+\sqrt{-5}\rangle$ yet is also a proper ideal, we must also have $|fo_K/\langle 2\rangle| = 2$. Therefore, since they are both fields of order 2, $f(\langle 2, 1+\sqrt{-5}\rangle|\langle 2\rangle) = 1$.

Up until now we have been working with a specific prime $\mathfrak{q}$ over $\mathfrak{p}$. Let us break from this for a moment and consider some properties related to the entire factorization of $\mathfrak{p}$.

Definition 3.12. Let $\mathfrak{O}_K$ and $\mathfrak{O}_L$ be as above, and $\mathfrak{p}$ a prime in $\mathfrak{O}_K$. Let $\mathfrak{p}$ factor in $\mathfrak{O}_L$ as $\mathfrak{p}\mathfrak{O}_L = \mathfrak{q}_1^{e_1}...\mathfrak{q}_r^{e_r}$, with the $\mathfrak{q}_i$ all distinct, and note that the $\mathfrak{q}_i$ are exactly the r primes of $\mathfrak{O}_L$ lying over $\mathfrak{p}$. Each exponent e_i in this unique factorization is called the *ramification index of* $\mathfrak{q}_i$ *over* $\mathfrak{p}$, and is denoted $e_i = e(\mathfrak{q}_i|\mathfrak{p})$.

Example 3.13. With our same example as above, we have $2\mathfrak{O}_L = \langle 2, 1+\sqrt{-5}\rangle^2$, and $3\mathfrak{O}_L = \langle 3, 1+\sqrt{-5}\rangle\langle 3, 1-\sqrt{-5}\rangle$. Thus $e(\langle 2, 1+\sqrt{-5}\rangle \mid \langle 2\rangle) = 2$ and $e(\langle 3, 1\pm\sqrt{-5}\rangle \mid \langle 3\rangle) = 1$.

We find that these values are multiplicative in towers:

Proposition 3.14. *Let* $K \subseteq L \subseteq T$ *be number fields, and* $\mathfrak{p} \subseteq \mathfrak{q} \subseteq \mathfrak{u}$ *be primes in* $\mathfrak{O}_K \subseteq \mathfrak{O}_L \subseteq \mathfrak{O}_T$, *respectively. Then:*

(i) $e(\mathfrak{u}|\mathfrak{p}) = e(\mathfrak{u}|\mathfrak{q}) \cdot e(\mathfrak{q}|\mathfrak{p})$;

(ii) $f(\mathfrak{u}|\mathfrak{p}) = f(\mathfrak{u}|\mathfrak{q}) \cdot f(\mathfrak{q}|\mathfrak{p})$.

Proof. (i) We have two different splittings of $\mathfrak{p}$: In the largest ring $\mathfrak{O}_T$, $\mathfrak{p}\mathfrak{O}_T = \mathfrak{u}^{e(\mathfrak{u}|\mathfrak{p})}\mathfrak{P}_1$, where $\mathfrak{u}$ and $\mathfrak{P}_1$ are relatively prime (so $\mathfrak{u}$ does not divide $\mathfrak{P}_1$) and $\mathfrak{P}_1$ is a product of primes of $\mathfrak{O}_T$; in the middle ring $\mathfrak{O}_L$, $\mathfrak{p}\mathfrak{O}_L = \mathfrak{q}^{e(\mathfrak{q}|\mathfrak{p})}\mathfrak{P}_2$, where $\mathfrak{q}$ and $\mathfrak{P}_2$ are relatively prime and $\mathfrak{P}_2$

is a product of primes of $\mathfrak{O}_L$. Further, we have the splitting of $\mathfrak{q}$ in $\mathfrak{O}_T$: $\mathfrak{q}\mathfrak{O}_T = \mathfrak{u}^{e(\mathfrak{u}|\mathfrak{q})}\mathfrak{P}_3$, where $\mathfrak{u}$ and $\mathfrak{P}_3$ are relatively prime and $\mathfrak{P}_3$ is a product of primes of $\mathfrak{O}_T$. Note that $\mathfrak{u}$ and $\mathfrak{P}_2\mathfrak{O}_T$ must also be relatively prime since $\mathfrak{u}$ lies over a unique prime in $\mathfrak{O}_L$, namely our $\mathfrak{q}$, and thus cannot be a factor of $\mathfrak{P}_2$. Hence we have:

$$\mathfrak{u}^{e(\mathfrak{u}|\mathfrak{p})}\ \mathfrak{P}_1 = \mathfrak{p}\mathfrak{O}_T = \mathfrak{q}^{e(\mathfrak{q}|\mathfrak{p})}\ \mathfrak{P}_2\mathfrak{O}_T = (\mathfrak{u}^{e(\mathfrak{u}|\mathfrak{q})}\ \mathfrak{P}_3)^{e(\mathfrak{q}|\mathfrak{p})}\ \mathfrak{P}_2 = \mathfrak{u}^{e(\mathfrak{u}|\mathfrak{q})\cdot e(\mathfrak{q}|\mathfrak{p})}\ \mathfrak{P}_3^{e(\mathfrak{q}|\mathfrak{p})}\ \mathfrak{P}_2;$$

where $\mathfrak{u}$ does not divide $\mathfrak{P}_i$ for $i = 1, 2, 3$. Thus, by unique factorization, it must be the case that $\mathfrak{P}_3^{e(\mathfrak{q}|\mathfrak{p})}\mathfrak{P}_2 = \mathfrak{P}_1$ and, more importantly $e(\mathfrak{u}|\mathfrak{p}) = e(\mathfrak{u}|\mathfrak{q}) \cdot e(\mathfrak{q}|\mathfrak{p})$.

(*ii*) This says $[\mathfrak{O}_T/\mathfrak{u} : \mathfrak{O}_K/\mathfrak{p}] = [\mathfrak{O}_T/\mathfrak{u} : \mathfrak{O}_L/\mathfrak{q}]\ [\mathfrak{O}_L/\mathfrak{q}{:}\mathfrak{O}_K/\mathfrak{p}]$, which is an easy result from field theory [for more information, see Stewart and Tall [7] p.21]. ☆

Next, we can begin to put some restrictions on the possible values of e and f. To do so, it will be helpful to consider the order of the residue fields. We note that if $\mathfrak{q}$ is any prime in $\mathfrak{O}_L$, then $\mathfrak{q}$ lies over a unique prime $\langle p\rangle \in \mathbb{Z}$ by Theorem 3.8 (*ii*). Then we see that $\mathfrak{O}_L/\mathfrak{q}$ is a finite extension of $\mathbb{Z}/\langle p\rangle$, and thus is a field of order p^f, where $f = f(\mathfrak{q}|\langle p\rangle)$. We know that $\mathfrak{q}$ contains $p\mathfrak{O}_L$, and thus the order of $\mathfrak{O}_L/\mathfrak{q}$ is at most the order of $\mathfrak{O}_L/p\mathfrak{O}_L$. Since $|\mathfrak{O}_L/p\mathfrak{O}_L| = p^n$ for $n = [L : \mathbb{Q}]$ by Corollary 1.45, we have that $f \leq n$ when the base field $K = \mathbb{Q}$.

We can generalize this conclusion, and find that $f \leq n$ for all primes $\mathfrak{q}$ over $\mathfrak{p}$ in number fields L over K, respectively. This is a consequence of a much stronger and more important result: we will show that, for a prime factorization $\mathfrak{p}\mathfrak{O}_L = \mathfrak{q}_1^{e_1}...\mathfrak{q}_r^{e_r}$, we have $\sum_{i=1}^{r} e_i f_i = n$.

3.2 Road to Theorem 3.20

Proving this result requires a series of propositions and lemmas, many of which are interesting in their own right. We begin by formally naming a concept with which we have already worked extensively:

Definition 3.15. Let $\mathfrak{p}$ be a prime ideal in a number ring $\mathfrak{O}_K$. The *norm of* $\mathfrak{p}$, denoted

$\|\mathfrak{p}\|$, is defined to be the order of the residue field $\mathfrak{O}_K/\mathfrak{p}$.

We have already seen that an understanding of this value can be useful for describing our number fields and rings. Exploring further, as with e and f, we find that the norm acts well under multiplication:

Proposition 3.16. *Let $\mathfrak{O}_K$, $\mathfrak{O}_L$, K, and L be as before, and $n = [L : K]$. Then for ideals $\mathfrak{a}$ and $\mathfrak{b}$ in $\mathfrak{O}_K$, $\|\mathfrak{ab}\| = \|\mathfrak{a}\|\|\mathfrak{b}\|$.*

Proof. We prove this first for the case in which $\mathfrak{a}$ and $\mathfrak{b}$ are relatively prime. Taking them to be so, by Proposition 2.27 and the definition of the *gcd* and *lcm* we have that $\mathfrak{a} + \mathfrak{b} = \mathfrak{O}_K$ and $\mathfrak{a} \cap \mathfrak{b} = \mathfrak{ab}$. By the Chinese Remainder Theorem, we have an isomorphism $\mathfrak{O}_K/\mathfrak{ab} \cong \mathfrak{O}_K/\mathfrak{a} \times \mathfrak{O}_K/\mathfrak{b}$; thus $\|\mathfrak{ab}\| = \|\mathfrak{a}\|\|\mathfrak{b}\|$.

We claim $\|\mathfrak{p}^m\| = \|\mathfrak{p}\|^m$, where $\mathfrak{p}$ is any prime ideal. We will prove this by first noting that we have a descending chain of ideals $\mathfrak{O}_K \supseteq \mathfrak{p} \supseteq \mathfrak{p}^2 \supseteq \ldots \supseteq \mathfrak{p}^m$. Then we will show that for each k, $|\mathfrak{p}^k/\mathfrak{p}^{k+1}| = \|\mathfrak{p}\|$, where the $\mathfrak{p}^k$ are considered as additive groups of $\mathfrak{O}_K$. By the Third Isomorphism Theorem we have $(\mathfrak{O}/\mathfrak{p}^2)/(\mathfrak{p}/\mathfrak{p}^2) \cong \mathfrak{O}/\mathfrak{p}$, thus $|(\mathfrak{O}/\mathfrak{p}^2)/(\mathfrak{p}/\mathfrak{p}^2)| = |\mathfrak{O}/\mathfrak{p}|$ and hence $|\mathfrak{O}/\mathfrak{p}^2| = |\mathfrak{O}/\mathfrak{p}||\mathfrak{p}/\mathfrak{p}^2|$; inductively we have $|\mathfrak{O}/\mathfrak{p}^{n-1}| = |\mathfrak{O}/\mathfrak{p}||\mathfrak{p}/\mathfrak{p}^2|...|\mathfrak{p}^{n-1}/\mathfrak{p}^n|$ for all n. This will yield the equality $\|\mathfrak{p}^m\| = |\mathfrak{p}/\mathfrak{p}^2||\mathfrak{p}^2/\mathfrak{p}^3|...|\mathfrak{p}^{m-1}/\mathfrak{p}^m| = \|\mathfrak{p}\|...\|\mathfrak{p}\| = \|\mathfrak{p}\|^m$.

In order to prove that $|\mathfrak{p}^k/\mathfrak{p}^{k+1}| = \|\mathfrak{p}\|$ for all k, we will show $\mathfrak{O}_K/\mathfrak{p} \cong \mathfrak{p}^k/\mathfrak{p}^{k+1}$. Start by fixing any $\alpha \in \mathfrak{p}^k \backslash \mathfrak{p}^{k+1}$. The inclusion $\alpha\mathfrak{O}_K \subseteq \mathfrak{p}^k$ induces the homomorphism $\alpha\mathfrak{O}_K \to \mathfrak{p}^k/\mathfrak{p}^{k+1}$, with kernel $(\alpha\mathfrak{O}_K) \cap \mathfrak{p}^{k+1} = lcm(\alpha\mathfrak{O}_K, \mathfrak{p}^{k+1})$ and image $((\alpha\mathfrak{O}_K) + \mathfrak{p}^{k+1})/\mathfrak{p}^{k+1} = gcd(\alpha\mathfrak{O}_K, \mathfrak{p}^{k+1})/\mathfrak{p}^{k+1}$. Note further that $gcd(\alpha\mathfrak{O}_K, \mathfrak{p}^{k+1}) = \mathfrak{p}^k$: since $\alpha \in \mathfrak{p}^k$, $\alpha\mathfrak{O}_K \subseteq \mathfrak{p}^k$ and thus $\mathfrak{p}^k | \alpha\mathfrak{O}_K$; and clearly $\mathfrak{p}^k | \mathfrak{p}^{k+1}$. If $\mathfrak{p}^k$ were not the *gcd*, then it would must be $\mathfrak{p}^{k+1}$, but we know $\alpha\mathfrak{O}_K \not\subseteq \mathfrak{p}^{k+1}$ since $\alpha \notin \mathfrak{p}^{k+1}$. Similarly note that $lcm(\alpha\mathfrak{O}_K, \mathfrak{p}^{k+1}) = \alpha\mathfrak{p}$: clearly $\mathfrak{p}^{k+1}$ divides the *lcm*; from the above we have that $\mathfrak{p}^k$ is the highest power of $\mathfrak{p}$ appearing in $\alpha\mathfrak{O}_K$, and thus we have $\alpha\mathfrak{O}_K = \mathfrak{p}^k\mathfrak{P}$ for some product of primes $\mathfrak{P}$. Thus $\mathfrak{P}$ must also divide the *lcm*, and hence $lcm = \mathfrak{p}^{k+1}\mathfrak{P} = (\mathfrak{p}^k\mathfrak{P})\mathfrak{p} = (\alpha\mathfrak{O}_K)\mathfrak{p} = \alpha\mathfrak{p}$.

Thus the image is equal to $\mathfrak{p}^k/\mathfrak{p}^{k+1}$, and hence this mapping is an epimorphism with kernel $\alpha\mathfrak{p}$. Therefore by the First Isomorphism Theorem we have $\alpha\mathfrak{O}_K/\alpha\mathfrak{p} \cong \mathfrak{p}^k/\mathfrak{p}^{k+1}$.

Finally, we have an obvious isomorphism $\mathfrak{O}_K/\mathfrak{p} \cong \alpha\mathfrak{O}_K/\alpha\mathfrak{p}$, and thus $\mathfrak{O}_K/\mathfrak{p} \cong \mathfrak{p}^k/\mathfrak{p}^{k+}$, as desired.

Therefore we have $\|\mathfrak{p}^m\| = \|\mathfrak{p}\|^m$, which implies that $\|\mathfrak{p}_1^{m_1}...\mathfrak{p}_r^{m_r}\| = \|\mathfrak{p}_1\|^{m_1}...\|\mathfrak{p}_r\|^{m_r}$. Factoring $\mathfrak{a}$ and $\mathfrak{b}$ in primes and applying this formula gives us our result. ☆

We can now prove the desired result in a specific case, when the base field $K = \mathbb{Q}$.

Lemma 3.17. *Let L be a number field with number ring $\mathfrak{O}_L$, and let $n = [L : \mathbb{Q}]$. Fix a prime $\mathfrak{p}$ of $\mathbb{Z}$, and let $\mathfrak{q}_1$,...,$\mathfrak{q}_r$ be the primes of $\mathfrak{O}_L$ lying over $\mathfrak{p}$. Denote by e_1,...,e_r and f_1,...,f_r the corresponding ramification indicies $e(\mathfrak{q}_i|\mathfrak{p})$ and inertial degrees $f(\mathfrak{q}_i|\mathfrak{p})$. Then $\sum_{i=1}^{r} e_i f_i = n$.*

Proof. Since our base field is $\mathbb{Q}$ and $\mathfrak{O}_{\mathbb{Q}} = \mathbb{Z}$, we have $\mathfrak{p} = p\mathbb{Z}$ for some prime $p \in \mathbb{Z}$. We consider the given prime factorization of $\mathfrak{p}$ in $\mathfrak{O}_L$: $p\mathfrak{O}_L = \prod_{i=1}^{r} \mathfrak{q}_i^{e_i}$. Thus $\|p\mathfrak{O}_L\| = \prod_{i=1}^{r} \|\mathfrak{q}_i\|^{e_i} = \prod_{i=1}^{r} (p^{f_i})^{e_i}$. We also know that $\|p\mathfrak{O}_L\| = p^n$ by Proposition 1.45, and thus $p^{\sum f_i e_i} = p^n$. Therefore $n = \sum_{i=1}^{r} f_i e_i$. ☆

Let us now prove a short generalization of Lemma 2.2:

Corollary 3.18. *Let $\mathfrak{a}$, $\mathfrak{b}$ be non-zero ideals in $\mathfrak{O}$ with $\mathfrak{b} \subsetneq \mathfrak{a}$. Then there exists $\gamma \in K$ such that $\gamma\mathfrak{b} \subseteq \mathfrak{O}$ and $\gamma\mathfrak{b} \not\subseteq \mathfrak{a}$.*

Proof. By Theorem 2.15 there exists a non-zero ideal $\mathfrak{c}$ such that $\mathfrak{bc} = \langle a \rangle$ for some $a \in \mathfrak{b}, \mathfrak{c}$. Note that $\mathfrak{bc} = \langle a \rangle = a\mathfrak{O} \supsetneq a\mathfrak{a}$ since $\mathfrak{a}$ is a proper ideal. Then $\mathfrak{bc} \supsetneq a\mathfrak{a}$, so $\mathfrak{bc} \not\subseteq a\mathfrak{a}$. Let $c \in \mathfrak{c}$ be such that $c\mathfrak{b} \not\subseteq a\mathfrak{a}$; such an element exists since we know there exists some $b \in \mathfrak{b}$ and $c \in \mathfrak{c}$ such that $bc \notin a\mathfrak{a}$. Take $\gamma = ca^{-1}$. Then, first, $\gamma\mathfrak{b} = ca^{-1}\mathfrak{b} \subseteq a^{-1}\mathfrak{bc} = a^{-1}\langle a \rangle = \mathfrak{O}$. Second, if $\gamma\mathfrak{b} = a^{-1}c\mathfrak{b} \subseteq \mathfrak{a}$ then $c\mathfrak{b} \subseteq \mathfrak{a}$, a contradiction. Thus γ works as desired. ☆

We can now extend the result of Proposition 3.16 to cover ideals of the form $\mathfrak{a}\mathfrak{O}_L$, where $\mathfrak{a}$ is an ideal of $\mathfrak{O}_K$:

Lemma 3.19. *Let $\mathfrak{a}$ be an ideal of $\mathfrak{O}_K$ and $n = [L : K]$. For the $\mathfrak{O}_L$-ideal $\mathfrak{a}\mathfrak{O}_L$, $\|\mathfrak{a}\mathfrak{O}_L\| = \|\mathfrak{a}\|^n$.*

Proof. With the help of Proposition 3.16, it is sufficient to prove this for the case in which $\mathfrak{a}$ is a prime $\mathfrak{p}$, and the general case will follow by factoring $\mathfrak{a}$ into primes: if $\mathfrak{a} = \mathfrak{p}_1^{e_1} \dots \mathfrak{p}_r^{e_r}$, then, by Proposition 3.16,

$$\|\mathfrak{a}\mathfrak{O}_L\| = \|\mathfrak{p}_1^{e_1}\mathfrak{O}_L\| \dots \|\mathfrak{p}_r^{e_r}\mathfrak{O}_L\| = \|\mathfrak{p}_1^{e_1}\|^n \dots \|\mathfrak{p}_r^{e_r}\|^n = (\|\mathfrak{p}_1\|^{e_1} \dots \|\mathfrak{p}_r\|^{e_r})^n = \|\mathfrak{a}\|^n$$

Notice that $\mathfrak{O}_L/\mathfrak{p}\mathfrak{O}_L$ is a vector space over the field $\mathfrak{O}_K/\mathfrak{p}$; we claim that the dimension of $\mathfrak{O}_L/\mathfrak{p}\mathfrak{O}_L$ over $\mathfrak{O}_K/\mathfrak{p}$ equals n (which would prove our result).

First we will show the dimension is at most n by demonstrating that any $n+1$ elements of $\mathfrak{O}_L/\mathfrak{p}\mathfrak{O}_L$ are linearly dependent over $\mathfrak{O}_K/\mathfrak{p}$. Fix $n+1$ arbitrary elements $\overline{\alpha}_1 ... \overline{\alpha}_{n+1} \in \mathfrak{O}_L/\mathfrak{p}\mathfrak{O}_L$, and let $\alpha_1,...,\alpha_{n+1} \in \mathfrak{O}_L$ be corresponding elements in $\mathfrak{O}_L$, that is, $\alpha_i + \mathfrak{O}_L = \overline{\alpha}_i$. Since we have $n+1$ different α_i, these are clearly linearly dependent over K, and thus over $\mathfrak{O}_K$. Thus we have $\beta_1\alpha_1 + ... + \beta_{n+1}\alpha_{n+1} = 0$ for some $\beta_i \in \mathfrak{O}_K$, not all zero. Our challenge is to show that the β_i need not all be in $\mathfrak{p}$, so that when we reduce modulo $\mathfrak{p}$ they do not all go to zero, and what remains is a valid dependence equation, this time for the $\overline{\alpha_i}$.

If the β_i are not all in $\mathfrak{p}$, then we are done. However, suppose all the β_i are in $\mathfrak{p}$. Then we see that $\langle \beta_1,...\beta_{n+1} \rangle \subseteq \mathfrak{p}$. Use Lemma 3.18 with $\mathfrak{a} = \mathfrak{p}$ and $\mathfrak{b} = \langle \beta_1,...\beta_{n+1} \rangle$ to produce $\gamma \in K$ such that $\gamma\langle \beta_1, \dots, \beta_{n+1} \rangle \subseteq \mathfrak{O}_K$ but $\gamma\langle \beta_1, \dots, \beta_{n+1} \rangle = \langle \gamma\beta_1, \dots, \gamma\beta_{n+1} \rangle \not\subseteq \mathfrak{p}$. Thus it must be the case that $\gamma\beta_i \notin \mathfrak{p}$ for some i. If we multiply our dependency equation by γ, we have a new dependency equation with all coefficients still in $\mathfrak{O}_K$ but (at least) one not in $\mathfrak{p}$. Hence we can reduce modulo $\mathfrak{p}$ and get a dependence in $\mathfrak{O}_K/\mathfrak{p}$, and therefore $\mathfrak{O}_L/\mathfrak{p}\mathfrak{O}_L$ is at most n-dimensional over $\mathfrak{O}_K/\mathfrak{p}$.

To establish equality, let $\mathfrak{p} \cap \mathbb{Z} = p\mathbb{Z}$, and consider all primes $\mathfrak{p}_i$ of $\mathfrak{O}_K$ lying over $\langle p \rangle$. We know $\mathfrak{O}_L/\mathfrak{p}_i\mathfrak{O}_L$ is a vector space over $\mathfrak{O}_K/\mathfrak{p}_i$ of dimension $n_i \leq n$; we will show equality holds for all i, hence in particular when $\mathfrak{p}_i = \mathfrak{p}$.

Set $e_i = e(\mathfrak{p}_i|\langle p \rangle)$ and $f_i = f(\mathfrak{p}_i|\langle p \rangle)$. Then $\sum e_i f_i = m$, where m is the degree of K over $\mathbb{Q}$, via our special case (Lemma 3.17). We have $p\mathfrak{O}_K = \prod \mathfrak{p}_i^{e_i}$, so $p\mathfrak{O}_L = \prod (\mathfrak{p}_i\mathfrak{O}_L)^{e_i}$.

Using Proposition 3.16, we see:

$$\|p\mathfrak{O}_L\| = \|\prod(\mathfrak{p}_i\mathfrak{O}_L)^{e_i}\| = \prod\|\mathfrak{p}_i\mathfrak{O}_L\|^{e_i} = \prod\|\mathfrak{p}_i^{n_i}\|^{e_i} = \prod\|\mathfrak{p}_i\|^{n_ie_i} = \prod(p^{f_i})^{n_ie_i}.$$

Thus $\|p\| = \sum f_in_ie_i = mn$. Now we know $n_i \leq n$ for all i. Suppose there exists an i such that $n_i \lneq n$. Then $\sum f_in_ie_i \lneq \sum f_ine_i = n\sum f_ie_i = nm$, a contradiction. Thus all n_i must equal n. Therefore, $|\mathfrak{O}_L/\mathfrak{p}\mathfrak{O}_L| = |\mathfrak{O}_K/\mathfrak{p}|^n$, as desired. ☆

We now have all the tools at our disposal to prove our result in the general case:

Theorem 3.20. *Let n be the degree of L over K (with L, K, $\mathfrak{O}_K$, $\mathfrak{O}_L$ as above), and let $\mathfrak{q}_1, \ldots, \mathfrak{q}_r$ be primes of $\mathfrak{O}_L$ lying over a prime $\mathfrak{p}$ of $\mathfrak{O}_K$. Denote by $e_1, \ldots, e_r$ and $f_1, \ldots, f_r$ the corresponding ramification indicies and inertial degrees. Then $\sum_{i=1}^{r} e_if_i = n$.*

Proof. We have $\mathfrak{p}\mathfrak{O}_L = \prod\mathfrak{q}_i^{e_i}$, so $\|\mathfrak{p}\mathfrak{O}_L\| = \|\prod\mathfrak{q}_i^{e_i}\| = \prod\|\mathfrak{q}_i^{e_i}\| = \prod\|\mathfrak{q}_i\|^{e_i} = \prod\|\mathfrak{p}\|^{f_ie_i}$ by Proposition 3.16 and the definition of f_i. However, we just showed above in Lemma 3.19 that $\|\mathfrak{p}\mathfrak{O}_L\| = \|\mathfrak{p}\|^n$. Therefore $n = \sum e_if_i$.

☆

The usefulness of this result can be clearly demonstrated by a simple corollary and a couple examples.

Corollary 3.21. *Let $\mathfrak{a}$ be an ideal in a number ring $\mathfrak{O}_K$. If $\|\mathfrak{a}\| = p$ for some prime $p \in \mathbb{Z}$ then $\mathfrak{a}$ is a prime ideal of $\mathfrak{O}_K$.*

Proof. Factoring $\mathfrak{a}$ and taking norms yields $\|\mathfrak{a}\| = \|\mathfrak{p}_1\| \ldots \|\mathfrak{p}_r\| = p$. Thus there exists some i such that $\|\mathfrak{p}_i\| = p$ and for all other factors $\mathfrak{p}_j$, $\|\mathfrak{p}_j\| = 1$. Then $\mathfrak{p}_j = \mathfrak{O}_K$ for all $j \neq i$, and hence $\mathfrak{a}$ is prime. ☆

For each of the following examples, we will be looking at cases where we have some factorization in the upper number ring into relatively prime (but not necessarily prime) ideals. However, we will use the conditions present and Theorem 3.20 to determine that the ideals given must indeed be prime.

Example 3.22. Let $K = \mathbb{Q}$, and $L = \mathbb{Q}[\omega]$, where $\omega = e^{2\pi i/p}$ for some prime $p \in \mathbb{Z}$. It can be shown that the associated number ring is $\mathfrak{O}_L = \mathbb{Z}[\omega]$, and that the minimum polynomial of ω over $\mathbb{Q}$ is $f(t) = t^{p-1}+\ldots+t+1$; thus $n = [\mathbb{Q}[\omega] : \mathbb{Q}] = p-1$ [see STEWART AND TALL [7] p.67]. Further note that since $f(t)\cdot(t-1) = t^p - 1$, the other roots of $f(t)$ must be the other p^{th} roots of unity, and hence we have the factorization $f(t) = (t-\omega)(t-\omega^2)\ldots(t-\omega^{p-1})$.

Let us carefully consider the case where $p = 5$. Then $\omega = e^{2\pi i/5}$, and

$$f(t) = t^4 + t^3 + t^2 + t + 1 = (t-\omega)(t-\omega^2)(t-\omega^3)(t-\omega^4)$$

Since ω is a root, we see $\omega^4 = -1 - \omega - \omega^2 - \omega^3$, and hence:

$$\begin{aligned}(1-\omega)^4 &= 1 - 4\omega + 6\omega^2 - 4\omega^3 + \omega^4 \\ &= 1 - 4\omega + 6\omega^2 - 4\omega^3 - 1 - \omega - \omega^2 - \omega^3 \\ &= -5\omega + 5\omega^2 - 5\omega^3 = 5(-\omega + \omega^2 - \omega^3).\end{aligned}$$

Thus $\langle 1-\omega\rangle^4 \subseteq 5\mathfrak{O}_L$, so the ideal $\langle 1-\omega\rangle$ of $\mathfrak{O}_L$ lies over $\langle 5\rangle$ of $\mathfrak{O}_K = \mathbb{Z}$. Further, we have:

$$\begin{aligned}5 = f(1) &= (1-\omega)(1-\omega^2)(1-\omega^3)(1-\omega^4) \\ &= (1-\omega)[(1-\omega)(1+\omega)][(1-\omega)(1+\omega+\omega^2)][(1-\omega)(1\omega+\omega^2+\omega^3)] \\ &= (1-\omega)^4[(1+\omega)(1+\omega+\omega^2)(1+\omega+\omega^3)].\end{aligned}$$

Thus $5 \in \langle(1-\omega)^4\rangle$ since $(1+\omega)(1+\omega+\omega^2)(1+\omega+\omega^3) \in \mathfrak{O}_L$, and $\langle(1-\omega)^4\rangle = \langle 1-\omega\rangle^4$ by multiplication of generators, so $5\mathfrak{O}_L \subseteq \langle 1-\omega\rangle^4$. Therefore, by mutual containment, $5\mathfrak{O}_L = \langle 1-\omega\rangle^4$.

We can now use Theorem 3.20 and Corollary 3.21 to show that the ideal $\langle 1-\omega\rangle$ is prime in $\mathfrak{O}_L$ in two different ways. First, notice that any further splitting of $\langle 1-\omega\rangle$ would violate Theorem 3.20: we know $n = 4$ and $e_1 \geq 4$ (even if $\langle 1-\omega\rangle$ is not prime, the exponent would transfer to all of its prime factors). Therefore we must have $f = r = 1$, so $\langle 1-\omega\rangle^4 = 5\mathfrak{O}_L$ must be *the* prime factorization of $5\mathfrak{O}_L$, and hence $\langle 1-\omega\rangle^4$ must be prime.

Second, since norms are multiplicative and $\langle 1-\omega\rangle^4 = 5\mathfrak{O}_L$, by Lemma 3.19 we have:

$$\|\langle 1-\omega\rangle\|^4 = \|\langle 1-\omega\rangle^4\| = \|5\mathfrak{O}_L]\| = 5^4;$$

and hence $\|\langle 1-\omega\rangle\| = 5$; by Corollary 3.21 we have that $\langle 1-\omega\rangle$ is prime.

Example 3.23. Now consider the integer α which satisfies the polynomial $x^3 - x - 1$, and let $K = \mathbb{Q}$ and $L = \mathbb{Q}[\alpha]$. It can be shown, in a more general case, that if some θ satisfies $t^3 + at + b$ then $\Delta\{1, \theta, \theta^2\} = -(4a^3 + 27b^2)$ [see MARCUS [5] p.26 and p.46]. Then, for our α, we see $a = b = -1$, and hence $\Delta\{1, \alpha, \alpha^2\} = -(4(-1)^3 + 27(-1)^2) = -23$. Since -23 is squarefree, $\{1, \alpha, \alpha^2\}$ is an integral basis by Corollary 1.44. Thus $\mathfrak{O}_L = \mathbb{Z}[\alpha]$.

Further, let us consider the ideal $\langle 23\rangle$ of $\mathbb{Q}$ in the number ring $\mathfrak{O}_L$. We claim $23\mathfrak{O}_L = \langle 23, \alpha - 10\rangle^2\langle 23, \alpha - 3\rangle$. Clearly $23\mathfrak{O}_L \subseteq \langle 23, \alpha - 10\rangle^2\langle 23, \alpha - 3\rangle$. Conversely, multiplying the generators on the right yields

$$\begin{aligned}\langle 23, \alpha - 10\rangle^2\langle 23,\alpha - 3\rangle = \langle 23^2, 23\alpha - 23 * 10, \alpha^2 - 20\alpha + 100\rangle\langle 23, \alpha - 3\rangle \\ \langle 23^3, 23^2\alpha - 23^2 \cdot 10, 23\alpha^2 - 23 \cdot 20\alpha + 23 \cdot 100, 23^2\alpha - 23^2 \cdot 3, \\ 23\alpha^2 - 23 \cdot 10\alpha - 23 \cdot 3\alpha + 23 \cdot 30, \alpha^3 - 23\alpha^2 + 160\alpha - 300\rangle.\end{aligned}$$

All of these generators are clearly divisible by 23, with the possible exception of the final term. However, since $\alpha^3 = \alpha + 1$, we have

$$\alpha^3 - 23\alpha^2 + 160\alpha - 300 = -23\alpha^2 + 161\alpha - 299 = 23(-\alpha^2 + 7\alpha - 13).$$

Hence $\langle 23, \alpha - 10\rangle^2\langle 23, \alpha - 3\rangle \subseteq 23\mathfrak{O}_L$.

We can also show that these two ideals, $\langle 23, \alpha - 10\rangle$ and $\langle 23, \alpha - 3\rangle$, are relatively prime. We will prove $\mathfrak{O}_L = \langle 23, \alpha - 3, \alpha - 10\rangle$; then we will have $\langle 23, \alpha - 10\rangle + \langle 23, \alpha - 3\rangle = \langle 23, \alpha - 3, \alpha - 10\rangle = \mathfrak{O}_L$, and hence the union would equal $\mathfrak{O}_L$.

We will show this first equality by showing $1 \in \langle 23, \alpha - 3, \alpha - 10\rangle$. Clearly $(\alpha - 3) - (\alpha - 10) = 7 \in \langle 23, \alpha - 3, \alpha - 10\rangle$, so we have $10(7) - 3(23) = 1 \in \langle 23, \alpha - 3, \alpha - 10\rangle$. Since

our ideal contains 1, it must be the whole ring, and our equality holds.

Therefore, we have our desired splitting of $23\mathfrak{O}_L$ into two relatively prime ideals. With the notation as in Theorem 3.20, we have $n = 3$, $e_1 \geq 2$, $e_2 \geq 1$, and $r \geq 2$. Hence it must be the case that these are equalities, with $f_1 = f_2 = 1$, requiring $23\mathfrak{O}_L = \langle 23, \alpha - 10\rangle^2 \langle 23, \alpha - 3\rangle$ to be the unique factorization of $23\mathfrak{O}_L$ into primes.

Example 3.24. Finally, let us consider an example of a cubic field (i.e. $n = 3$). Let $K = \mathbb{Q}$ and take $L = \mathbb{Q}[\sqrt[3]{2}]$. Using techniques similar to those used in the previous examples, we can show that $\mathfrak{O}_L = \mathbb{Z}[\sqrt[3]{2}]$. If we consider the ideal $\langle 2\rangle$ in $\mathbb{Z}$, we see that $2\mathfrak{O}_L = \langle \sqrt[3]{2}\rangle^3$, and hence, since $n = 3$ and $e_1 = 3$, by Theorem 3.20 we must have $r = f = 1$ and thus $\langle \sqrt[3]{2}\rangle$ must be prime with inertial degree of 1 over $\langle 2\rangle$.

In this same scenario, let us observe what happens to $\langle 5\rangle$. It can similarly be shown that $5\mathfrak{O}_L = \langle 5, \sqrt[3]{2} + 2\rangle \langle 5, (\sqrt[3]{2})^2 + 3(\sqrt[3]{2}) - 1\rangle$, where the two ideals on the right are relatively prime. It can also be shown that $\langle 5, (\sqrt[3]{2})^2 + 3(\sqrt[3]{2}) - 1\rangle$ is a prime with inertial degree 2. Then it must be the case that $\langle 5, \sqrt[3]{2} + 2\rangle$ is also a prime, with inertial degree 1 (we know $n = 3$, $f_1 = 2$, and $r \geq 2$; therefore $r = 2$ and $f_2 = 1$). [See MARCUS [5] p.70 for details]

3.3 Ramification of Primes

In some of the examples above, we saw there were cases where primes split into powers of new primes. It is especially interesting to consider those cases where $e \neq 1$ for some prime $\mathfrak{q}$ over $\mathfrak{p}$:

Definition 3.25. We say that a prime $\mathfrak{p}$ of $\mathfrak{O}_K$ is *ramified in* $\mathfrak{O}_L$ (or L) if there exists some prime $\mathfrak{q}$ of $\mathfrak{O}_L$ such that $e(\mathfrak{q}|\mathfrak{p}) \gneq 1$. In other words, $\mathfrak{p}$ is ramified if $\mathfrak{p}\mathfrak{O}_L$ is not squarefree.

Example. In addition to the examples above, going back further to Example 2.23, we see in the Gaussian Integers $\mathbb{Z}[i]$, $2\mathfrak{O}_L = \langle 1 - i\rangle^2$, and thus $\langle 2\rangle$ is ramified in $\mathbb{Z}[i]$.

It is also important to note the following regarding the discriminant Δ of $\mathbb{Z}[i]$:

$$\Delta(\mathbb{Z}[i]) = \begin{vmatrix} \sigma_1(1) & \sigma_1(i) \\ \sigma_2(1) & \sigma_2(i) \end{vmatrix}^2 = \begin{vmatrix} 1 & i \\ 1 & -i \end{vmatrix}^2 = (-2i)^2 = -4$$

and we see that 2 divides -4.

This observation, that $\langle 2 \rangle$ is ramified in $\mathbb{Z}[i]$ and 2 divides $\Delta(\mathbb{Z}[i])$, is true in a more general context.

Theorem 3.26. *A prime $\langle p \rangle \in \mathbb{Z}$ is ramified in the ring of integers $\mathfrak{O}_K$ of some number field K if and only iff $p|\Delta(\mathfrak{O}_K)$.*

We will only prove the forward direction of this "if and only if"; the converse requires tools not presented in this paper [for details, see MARCUS [5] p. 112].

In order to do so, we first need a lemma. It is necessary to note that this lemma deals with normal extensions, the main topic of our next section.

Lemma 3.27. *Let $K \subseteq L$ be number fields with L normal over $\mathbb{Q}$ (and hence over K), $G = Gal(L/K)$ be the associated Galois group, and $\mathfrak{p}$ a prime of the ring of integers $\mathfrak{O}_K$ of K. If $\mathfrak{q}$ is a prime lying over $\mathfrak{p}$, then $\sigma(\mathfrak{q})$ is a prime ideal in $\sigma(\mathfrak{O}_L) = \mathfrak{O}_L$ lying over $\sigma(\mathfrak{p}) = \mathfrak{p}$, for all $\sigma \in G$.*

Proof. Let $\sigma_1, \ldots, \sigma_n$ be the elements of G, and consider their restrictions $\sigma_i|_{\mathfrak{O}_L}$ for $i = 1, \ldots, n$. We claim that $\sigma_i(\mathfrak{O}_L) = \mathfrak{O}_L$. To prove this claim, take $\alpha \in \mathfrak{O}_L$, and $p(x)$ to be the irreducible monic polynomial of α over $\mathbb{Z}$; note that since σ_i is the identity on $K \supseteq \mathbb{Q} \supseteq \mathbb{Z}$ point-wise, we have $\sigma(p(\alpha)) = p(\sigma(\alpha))$, and thus we have a monic polynomial over $\mathbb{Z}$ which $\sigma(\alpha)$ satisfies, and hence $\sigma(\alpha)$ is an integer and thus in $\mathfrak{O}_L$.

Let $\mathfrak{p}$ be a prime ideal of $\mathfrak{O}_K$, and let $\mathfrak{q}$ be any prime ideal of $\mathfrak{O}_L$ lying over $\mathfrak{p}$. Now consider the composition of σ with the induced mapping $\mathfrak{O}_L \to \mathfrak{O}_L/\mathfrak{q}$. Clearly this composition is onto, and the kernel is $\sigma^{-1}(\mathfrak{q})$. Thus, by the First Isomorphism Theorem, $\mathfrak{O}_L/\sigma^{-1}(\mathfrak{q}) \cong \mathfrak{O}_L/\mathfrak{q}$. We know $\mathfrak{O}_L/\mathfrak{q}$ is a domain since $\mathfrak{q}$ is prime by Theorem 1.54, and

thus so must be $\mathfrak{O}_L/\sigma^{-1}(\mathfrak{q})$; again by the same theorem $\sigma^{-1}(\mathfrak{q})$ must be prime. Further, σ^{-1} fixes $\mathfrak{p} \subseteq K$ point-wise, and since $\mathfrak{p}\mathfrak{O}_L \subseteq \mathfrak{q}$, $\mathfrak{p}\mathfrak{O}_L = \sigma^{-1}(\mathfrak{p}\mathfrak{O}_L) = \sigma^{-1}(\mathfrak{q})$, as desired. ☆

We now begin our proof of Theorem 3.26: Let $\mathfrak{p}$ be a prime of $\mathfrak{O}_K$ lying over $\langle p \rangle$ such that $e(\mathfrak{p}|\langle p \rangle) \gneq 1$. Then $p\mathfrak{O}_K = \mathfrak{p}\mathfrak{P}$, with $\mathfrak{P}$ some product of primes of $\mathfrak{O}_K$ that is divisible by all primes of $\mathfrak{O}_K$ lying over $\langle p \rangle$; this is allowed since $e \gneq 1$ and thus some power of $\mathfrak{p}$ divides $\mathfrak{P}$.

By Theorem 1.38 we know there exists an integral basis $\{\alpha_1,...,\alpha_n\}$ for $\mathfrak{O}_K$. We will modify this basis by replacing one of the α_i with a new properly defined element which will allow us to see directly that p divides $\Delta(\mathfrak{O}_K)$. We begin by observing that, since $p\mathfrak{O}_K \subsetneq \mathfrak{P}$, there exists some $\alpha \in \mathfrak{P} \backslash p\mathfrak{O}_K$. Note that α is in every prime of $\mathfrak{O}_K$ lying over $\langle p \rangle$ (since $\alpha \in \mathfrak{P}$, the product of all such primes, and the product of ideals is a subset of all of its factors), but again is not in $p\mathfrak{O}_K$ (even though we may be tempted to think, falsely, that $p\mathfrak{O}_K$ is prime $\mathfrak{O}_K$). If we write $\alpha = m_1\alpha_1 + ... + m_n\alpha_n$ (for $m_i \in \mathbb{Z}$), then the fact that $\alpha \notin p\mathfrak{O}_K$ implies that not all m_i are divisible by p; we can renumber the α_i such that $p \nmid m_1$.

Take $\Delta = \Delta(\mathfrak{O}_K) = \Delta\{\alpha_1, ..., \alpha_n\}$, and let $\beta = m_2\alpha_2 + \ldots + m_n\alpha_n$; we have that $\alpha = \beta + m_1\alpha_1$. Then, by Proposition 1.31 (i), we see that $\Delta\{m_1\alpha_1, \alpha_2, \ldots, \alpha_n\} = m_1^2\Delta\{\alpha_1, ..., \alpha_n\} = m_1^2 d$, and then by (ii) we have $\Delta\{\alpha, \alpha_2, ..., \alpha_n\} = \Delta\{\beta + m_1\alpha_1, \alpha_2, ..., \alpha_n\} = \Delta\{m_1\alpha_1, \alpha_2, \ldots, \alpha_n\} = m_1^2 d$. Since $p \nmid m_1$, it will be sufficient to show that $p|\Delta\{\alpha, \alpha_2, ..., \alpha_n\}$.

Now consider an extension L of K which is normal over $\mathbb{Q}$ (and hence K). It follows that α is in every prime of $\mathfrak{O}_L = \mathbb{B} \cap L$ lying over $\langle p \rangle$, since each such $\mathfrak{q}$ contains $\mathfrak{p}$ for some prime $\mathfrak{p}$ of $\mathfrak{O}_K$ lying over $\langle p \rangle$ and $\alpha \in \mathfrak{p}$ for all such $\mathfrak{p}$. Fix any of these primes $\mathfrak{q}$ of $\mathfrak{O}_L$ lying over $\langle p \rangle$; by the lemma $\sigma^{-1}(\mathfrak{q})$ is a prime of $\mathfrak{O}_L$ lying over $\langle p \rangle$, and hence $\alpha \in \sigma^{-1}(\mathfrak{q})$. Then we see the stronger condition that $\sigma_i(\alpha) \in \mathfrak{q}$ for all $\sigma_i \in G$.

Notice that the calculation of $\Delta\{\alpha, \alpha_2, ..., \alpha_n\}$ only involves ring operations on elements we now know to be in $\mathfrak{q}$ — the $\sigma_i(\alpha)$ — and elements we know to be in $\mathfrak{O}$ — the $\sigma_i(\alpha_j)$. It follows that this discriminant is in $\mathfrak{q}$. Since the discriminant must also be in $\mathbb{Z}$ by Proposition 1.37, we know it is in $\mathfrak{q} \cap \mathbb{Z} = p\mathbb{Z}$. Thus $p \mid \Delta\{\alpha, \alpha_2, ...\alpha_n\}$, and therefore $p \mid \Delta(\mathfrak{O}_K)$,

as desired. ☆

We can build off of this theorem to prove a very interesting result about this aspect of splitting primes: for number rings $\mathfrak{O}_K$ and $\mathfrak{O}_L$ such that $\mathfrak{O}_K \subseteq \mathfrak{O}_L$, only finitely many primes of $\mathfrak{O}_K$ are ramified in $\mathfrak{O}_L$. We will first need a corollary.

Corollary 3.28. *Only finitely many primes of $\mathbb{Z}$ are ramified in a number ring $\mathfrak{O}_K$.*

Proof. Since $\Delta(\mathfrak{O}_K)$ is a finite rational integer, there are only finitely many $p \in \mathbb{Z}$ that divide it; thus, by the theorem, there are only finitely many possibly ramified primes $\langle p \rangle$ in $\mathbb{Z}$. ☆

We are now ready to prove our desired result:

Theorem 3.29. *Let $\mathfrak{O}_K$ and $\mathfrak{O}_L$ be rings of integers of some number fields $K \subseteq L$, respectively. Then only finitely many primes of $\mathfrak{O}_K$ are ramified in $\mathfrak{O}_L$.*

Proof. If $\mathfrak{p}$ is a prime of $\mathfrak{O}_K$ which is ramified in $\mathfrak{O}_L$, then $\mathfrak{p} \cap \mathbb{Z} = p\mathbb{Z}$ is ramified in $\mathfrak{O}_L$ since ramification indices are multiplicative in towers. There are only finitely many possibilities for p, and each one lies under only finitely many primes of $\mathfrak{O}_K$. Hence there are only finitely many possibilities for $\mathfrak{p}$, as desired. ☆

We can also further restrict which primes may ramify in L:

Corollary 3.30. *Let $K = \mathbb{Q}$, $L = \mathbb{Q}[\alpha]$, $\alpha \in \mathfrak{O}_L$, and f be any monic polynomial over $\mathbb{Z}$ such that $f(\alpha) = 0$. If $p \in \mathbb{Z}$ is a prime such that $p \nmid N_K^L\Big(f'(\alpha)\Big)$, then $\langle p \rangle$ is unramified in L.*

Proof. By Proposition 1.32, we know that $\Delta\{1, \alpha, \ldots, \alpha^{n-1}\}$ divides $N^K\Big(f'(\alpha)\Big)$. Thus, since $p \nmid N_K^L\Big(f'(\alpha)\Big)$, we also have that $p \nmid \Delta(1, \alpha, \ldots, \alpha^{n-1})$. Therefore, by Theorem 3.26, $\langle p \rangle$ is not ramified in L. ☆

3.4 Normal Extensions

We will now restrict our considerations to number fields K and L, where L is a normal extension of K.

Definition 3.31. Recall that L is *normal* over K when any of the following (equivalent) conditions holds:

(i) L is the splitting field of a polynomial in $K[x]$;

(ii) All embeddings of L into the algebraic closure of K which fix K point-wise are K-automorphisms on L;

(iii) Every irreducible polynomial in $K[x]$ which has a root in L factors completely into linear factors in $L[x]$.

Refer back to Example 3.23. Note that the primes lying over $\langle 23 \rangle$ do not have the same ramification index, and in the previous examples the primes over $\langle 5 \rangle$ did not have the same inertial degree. We will see shortly that this sort of behavior can only occur if L is *not* normal over K.

We have already seen with Lemma 3.27 the structural benefits of a normal extension; this result can be extended to the stronger conclusion about the relationship between $G = Gal(L/K)$ and the primes of $\mathfrak{O}_K$ and $\mathfrak{O}_L$:

Theorem 3.32. *Let K, L, $\mathfrak{O}_K$, and $\mathfrak{O}_L$ be as above (with L normal over K), and let $\mathfrak{q}$ and $\mathfrak{q}'$ be two primes of $\mathfrak{O}_L$ lying over the same prime $\mathfrak{p}$ of $\mathfrak{O}_K$. Then there exists some $\sigma \in G$ such that $\sigma(\mathfrak{q}) = \mathfrak{q}'$.*

Proof. Suppose not; then $\sigma(\mathfrak{q}) \neq \mathfrak{q}'$ for all $\sigma \in G$. Then, by the Chinese Remainder Theorem there is a solution to the system of congruences:

$x \equiv 0 \pmod{\mathfrak{q}'}$

$x \equiv 1 \pmod{\sigma(\mathfrak{q})}$ for all $\sigma \in G$.

Let $\alpha \in \mathfrak{O}_L$ be such a solution, and note that $\alpha \in \mathfrak{q}'$ since $\alpha \equiv 0 \pmod{\mathfrak{q}'}$. Then we have $N_K^L(\alpha) \in \mathfrak{O}_K \cap \mathfrak{q}' = \mathfrak{p}$ since one of the factors of $N_K^L(\alpha)$ is $\alpha \in \mathfrak{q}'$, and $N_K^L(\alpha)$ is in $\mathfrak{O}_K$

by Proposition 3.2. We also have, by our construction of α, that $\alpha \notin \sigma(\mathfrak{q})$ for all $\sigma \in G$, and hence $\sigma^{-1}(\alpha) \notin \mathfrak{q}$. Notice that we can express $N_K^L(\alpha)$ as the product of all $\sigma^{-1}(\alpha)$ (as opposed to the product of all $\sigma(\alpha)$) since we also have $\sigma^{-1} \in G$ for all $\sigma \in G$. Then $N_K^L(\alpha) \in \mathfrak{q}$ since $\sigma^{-1}(\alpha) \notin \mathfrak{q}$ for all $\sigma \in G$. However, we showed above that $N_K^L(\alpha) \in \mathfrak{p} \subseteq \mathfrak{q}$, a contradiction. Therefore there must exist some $\sigma \in G$ such that $\sigma(\mathfrak{q}) = \mathfrak{q}'$. ☆

Using Theorem 3.32, we see that primes split in a very particular way in normal extensions (unlike our splittings in the examples above):

Corollary 3.33. *If L is normal over K, and $\mathfrak{q}_1$ and $\mathfrak{q}_2$ are two primes of $\mathfrak{O}_L$ lying over a prime $\mathfrak{p}$ in $\mathfrak{O}_K$, then:*

(i) $e(\mathfrak{q}_1|\mathfrak{p}) = e(\mathfrak{q}_2|\mathfrak{p})$;

(ii) $f(\mathfrak{q}_1|\mathfrak{p}) = f(\mathfrak{q}_2|\mathfrak{p})$.

Proof. (i) We factor $\mathfrak{p}\mathfrak{O}_L$ in $\mathfrak{O}_L$, and write $\mathfrak{p}\mathfrak{O}_L = \mathfrak{q}_1^{e_1}\mathfrak{q}_2^{e_2}\mathfrak{P}$ with $\mathfrak{q}_1$, $\mathfrak{q}_2$, and $\mathfrak{P}$ relatively prime, $\mathfrak{P}$ a product of primes. Choose σ such that $\sigma(\mathfrak{q}_1) = \mathfrak{q}_2$ by Theorem 3.32, and note that $\sigma(\mathfrak{p}\mathfrak{O}_L) = \mathfrak{p}\mathfrak{O}_l$ since σ fixes $\mathfrak{p}$ point-wise and is an isomorphism on $\mathfrak{O}_L$. Then:

$$\begin{aligned}\mathfrak{q}_1^{e_1}\mathfrak{q}_2^{e_2}\,\mathfrak{P} &= \mathfrak{p}\mathfrak{O}_L = \sigma(\mathfrak{p}\mathfrak{O}_L)\\ &= \sigma(\mathfrak{q}_1^{e_1}\mathfrak{q}_2^{e_2}\,\mathfrak{P}) = \sigma(\mathfrak{q}_1^{e_1})\,\sigma(\mathfrak{q}_2^{e_2})\,\sigma(\mathfrak{P}) = \ \sigma(\mathfrak{q}_1)^{e_1}\,\sigma(\mathfrak{q}_2)^{e_2}\,\sigma(\mathfrak{P})\\ &= \mathfrak{q}_2^{e_1}\,\sigma(\mathfrak{q}_2)^{e_2}\,\sigma(\mathfrak{P}).\end{aligned}$$

Further, we have $\sigma(\mathfrak{q}_2) \neq \mathfrak{q}_2$ since that would require $\mathfrak{q}_1 = \mathfrak{q}_2$, and $\sigma(\mathfrak{P}) \not\subseteq \mathfrak{q}_2$ since that would imply $\mathfrak{q}_1 \subseteq \mathfrak{P}$ which would contradict the fact that $\mathfrak{P}$ and $\mathfrak{q}_1$ are relatively prime. Thus, by uniqueness of factorization on the above equation, it must be that case that $e_1 = e_2$.

(ii) It is sufficient to show there exists an isomorphism ϕ from $\mathfrak{O}_L/\mathfrak{q}_1$ to $\mathfrak{O}_L/\mathfrak{q}_2$. Consider the composition of $\sigma : \mathfrak{O}_L \to \mathfrak{O}_L$ and the induced mapping $\mathfrak{O}_L \to \mathfrak{O}_L/\mathfrak{q}_2$, and since $\sigma^{-1}(\mathfrak{q}_2) = \mathfrak{q}_1$ we know the kernel of this composition is $\mathfrak{q}_1$. Thus by the First Homomorphism Theorem we know there exists a mappings $\phi : \mathfrak{O}_L/\mathfrak{q}_1 \to \mathfrak{O}_L/\mathfrak{q}_2$ by $\phi(s + \mathfrak{q}_1) = \sigma(s) + \mathfrak{q}_2$,

where $\sigma(\mathfrak{q}_1) = \mathfrak{q}_2$. Further, since the composition is onto, ϕ is an isomorphism by the First Isomorphism Theorem. Thus $\mathfrak{O}_L/\mathfrak{q}_1 \cong \mathfrak{O}_L/\mathfrak{q}_2$, and since each is a finite field, they have the same number of elements, and further they have the same degree over $\mathfrak{O}_K/\mathfrak{p}$ which they both cover. ☆

This corollary shows that when L is normal over K, a prime $\mathfrak{p}$ of $\mathfrak{O}_K$ splits uniformly in $\mathfrak{O}_L$: $\mathfrak{p}\mathfrak{O}_L = (\mathfrak{q}_1 \dots \mathfrak{q}_r)^e$, where $\mathfrak{q}_i$ are distinct primes, and each have the same inertial degree f over $\mathfrak{p}$. Moreover:

Corollary 3.34. *Let L, K, $\mathfrak{O}_L$, and $\mathfrak{O}_K$ be as above, with L normal over K and $n = [L : K]$. Then, for any prime $\mathfrak{p} \in \mathfrak{O}_K$ which factors in $\mathfrak{O}_L$ as $\mathfrak{p}\mathfrak{O}_L = (\mathfrak{q}_1 \dots \mathfrak{q}_r)^e$ with $f = f(\mathfrak{q}_i|\mathfrak{p})$, we have $r \cdot e \cdot f = n$.*

Proof. This follows from a direct application of Theorem 3.20 to this factorization. ☆

3.4.1 Intermediate Fields

We will now look at certain intermediate fields between K and L, and see how primes of $\mathfrak{O}_K$ split in these fields. Recall our setup: we have number fields $K \subseteq L$ with L normal over K, associated rings of integers $\mathfrak{O}_K$ and $\mathfrak{O}_L$, and Galois group $G = Gal(L/K)$ with order $n = [L : K]$. We begin by looking at specific subgroups of G:

Definition 3.35. For a fixed prime $\mathfrak{p}$ of $\mathfrak{O}_K$, and a particular prime $\mathfrak{q}$ of $\mathfrak{O}_L$ lying over $\mathfrak{p}$, we define the *decomposition group* of $\mathfrak{q}$ over $\mathfrak{p}$ as:

$$D = D(\mathfrak{q}|\mathfrak{p}) = \{\sigma \in G \mid \sigma\mathfrak{q} = \mathfrak{q}\}.$$

With notation as above, define the *inertial group* of $\mathfrak{q}$ over $\mathfrak{p}$ as:

$$E = E(\mathfrak{q}|\mathfrak{p}) = \{\sigma \in G \mid \sigma(\alpha) \equiv \alpha \pmod{\mathfrak{q}} \quad \forall \alpha \in \mathfrak{O}_L\}.$$

Proposition 3.36. *Let L, K, $\mathfrak{O}_K$, $\mathfrak{O}_L$, $\mathfrak{p}$, and $\mathfrak{q}$ be as above. Then:*

(i) $D(\mathfrak{q}|\mathfrak{p})$ and $E(\mathfrak{q}|\mathfrak{p})$ are subgroups of $G = Gal(L/K)$;

(ii) $E \subseteq D$.

Proof. (i) It will be sufficient to show that D and E are closed under compositions since G is a finite group. First, for $\sigma_1,\ \sigma_2 \in D$, we have $\sigma_1 \circ \sigma_2(\mathfrak{q}) = \sigma_1(\sigma_2(\mathfrak{q})) = \sigma_1(\mathfrak{q}) = \mathfrak{q}$. In addition, for $\sigma_1,\ \sigma_2 \in E$ and an arbitrary $\alpha \in \mathfrak{O}_L$, $\sigma_1 \circ \sigma_2(\alpha) = \sigma_1(\sigma_2(\alpha)) \equiv \sigma_1(\alpha) \equiv \alpha \pmod{\mathfrak{q}}$.

(ii) Let $\sigma \in E$ and $\alpha \in \mathfrak{q}$. Then $\sigma(\alpha) \equiv \alpha \equiv 0 \pmod{\mathfrak{q}}$ (by the condition to be an element of E, and the fact that $\alpha \in \mathfrak{q}$). Thus $\sigma(\alpha) \in \mathfrak{q}$. ☆

Now consider the residue fields $\mathfrak{O}_L/\mathfrak{q}$ and $\mathfrak{O}_K/\mathfrak{p}$. The elements of D induce automorphisms of the field $\mathfrak{O}_L/\mathfrak{q}$ in a natural way: each $\sigma \in G$ restricts to an automorphism of $\mathfrak{O}_L$, and if $\sigma \in D$, the composition of σ with the induced mapping $\mathfrak{O}_L \to \mathfrak{O}_L/\mathfrak{q}$ has kernel $\sigma^{-1}(\mathfrak{q}) = \mathfrak{q}$. Thus, by the First Isomorphism Theorem, each $\sigma \in D$ induces an automorphism $\overline{\sigma}$ of $\mathfrak{O}_L/\mathfrak{q}$ such that the following diagram commutes, where $\overline{\sigma}(\alpha + \mathfrak{q}) = \sigma(\alpha)$:

$$\begin{array}{ccc} \mathfrak{O}_L & \xrightarrow{\sigma} & \mathfrak{O}_L \\ \downarrow & & \downarrow \\ \mathfrak{O}_L/\mathfrak{q} & \xrightarrow{\overline{\sigma}} & \mathfrak{O}_L/\mathfrak{q} \end{array}$$

Moreover it is clear that $\overline{\sigma}$ fixes the subfield $\mathfrak{O}_K/\mathfrak{p}$ point-wise (since σ fixes K, hence $\mathfrak{O}_K$, point-wise). Thus $\overline{\sigma} \in \overline{G}$, where $\overline{G}$ is the Galois group of $\mathfrak{O}_L/\mathfrak{q}$ over $\mathfrak{O}_K/\mathfrak{p}$.

In other words, we have a mapping $\psi : D \to \overline{G}$ that sends σ to $\overline{\sigma}$, which is a group homomorphism since compositions of automorphisms in D correspond to composition in $\overline{G}$; we can add commuting squares to the diagram above with $\sigma_i \in D$ above and $\overline{\sigma_i} \in \overline{G}$ below. Further:

Proposition 3.37. *The kernel of the homomorphism ψ described above is exactly the subgroup E of G.*

Proof. Let $\sigma \in E$ and $\alpha \in \mathfrak{O}_L$ be arbitrary. Then $\sigma(\alpha) \equiv \alpha \pmod{\mathfrak{q}}$, and hence $\sigma(\alpha) - \alpha \in \mathfrak{q}$. Thus $\psi(\sigma(\alpha + \mathfrak{q})) = \overline{\sigma}(\alpha + \mathfrak{q}) = \sigma(\alpha) + \mathfrak{q} = \alpha + \mathfrak{q}$, so clearly $\psi(\sigma)$ is the identity.

Conversely, if $\psi(\sigma)$ is the identity, it must be the case that $\alpha + \mathfrak{q} = \sigma(\alpha) + \mathfrak{q}$, exactly the condition required for σ to be in E. ☆

From this result, we see that E must be a normal subgroup of D, and that D/E is embedded in $\overline{G}$ by the First Homomorphism Theorem.

Now let H be a subgroup of G. We can consider special fields associated with H:

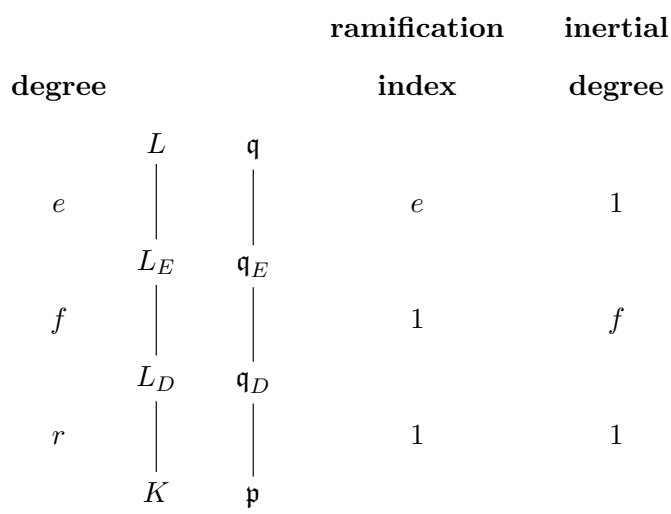
Definition 3.38. Let K, L, $\mathfrak{O}_K$ and $\mathfrak{O}_L$ be as above, $\mathfrak{p}$ a prime of $\mathfrak{O}_K$, and $\mathfrak{q}$ a prime of $\mathfrak{O}_L$ lying over $\mathfrak{p}$. Let H be a subgroup of $G = Gal(L/K)$. The *fixed field of* H is $L_H = \{\alpha \in L | \sigma(\alpha) = \alpha \text{ for all } \sigma \in H\}$.
We call the fixed field of D the *decomposition field* L_D; the fixed field of E is the *inertial field* L_E.

In order to keep things organized, we will adopt some additional notation, introduced by Marcus [5]. With notation as above:

- If H is a subgroup of G, we use the notation above and let L_H denote the fixed field of H; for example, if I is the identity on L then $L_{\{I\}} = L$ and, since L is normal over K, $L_G = K$.
- If X is a subset of L, let $X_H = X \cap L_H$; for example, $(\mathfrak{O}_L)_H = \mathfrak{O}_L \cap L_H = \mathbb{B} \cap L \cap L_H = L_H \cap \mathbb{B}$ is the ring of integers in L_H; and $\mathfrak{q}_H = \mathfrak{q} \cap L_H = \mathfrak{q} \cap \mathfrak{O}_L \cap L_H = \mathfrak{q} \cap (\mathfrak{O}_L)_H$ is the unique prime of $\mathfrak{O}_H$ lying under $\mathfrak{q}$, which clearly lies over $\mathfrak{p}$ (by Theorem 3.8).
  We will break this particular notational convention almost immediately when discussing number rings, and instead write $\mathfrak{O}_H$ when we mean $(\mathfrak{O}_L)_H$.
- Finally, we note that, since $\mathfrak{q}_H$ is a proper prime of $\mathfrak{O}_H$, $\mathfrak{O}_H/\mathfrak{q}_H$ is a field; further, we have a mapping $\mathfrak{O}_K/\mathfrak{p} \to \mathfrak{O}_H/\mathfrak{q}_H \to \mathfrak{O}_L/\mathfrak{q}$ defined by $r + \mathfrak{p} \mapsto r + \mathfrak{q}_H \mapsto r + \mathfrak{q}$ since $\mathfrak{O}_K \subseteq \mathfrak{O}_H \subseteq \mathfrak{O}_L$ and $\mathfrak{p} \subseteq \mathfrak{q}_H \subseteq \mathfrak{q}$. These mappings are injective since they map fields to fields, and hence we will always think of $\mathfrak{O}_H/\mathfrak{q}_H$ as an intermediate field between $\mathfrak{O}_K/\mathfrak{p}$ and $\mathfrak{O}_L/\mathfrak{q}$.

We can now state our main result, which shows the precise way the prime $\mathfrak{p}$ splits in these specific fields between K and L:

Theorem 3.39. *Let K, L, $\mathfrak{O}_K$, $\mathfrak{O}_L$, $\mathfrak{p}$, $\mathfrak{q}$, G, D, E, r, e, f, and n be as above. Then:*



Proof. We begin by establishing the values associated with the extension L_D over K.

We will first show that $[L_D : K] = r$. From Galois theory we know that $[L_D : K]$ is equal to the index (number of cosets) of D in G, $|G/D|$. Each left coset σD of G/D (with $\sigma \in G$) sends $\mathfrak{q}$ to $\sigma(\mathfrak{q})$ since for all $\tau \in D$, $\sigma\tau(\mathfrak{q}) = \sigma(\mathfrak{q})$. Further, we claim that $\sigma D = \tau D$ if and only if $\sigma(\mathfrak{q}) = \tau(\mathfrak{q})$. If $\sigma D = \tau D$, then $\tau^{-1}\sigma \in D$ and so $\tau^{-1}\sigma = \delta$ for some $\delta \in D$. Therefore $\sigma = \tau\delta$, and thus $\sigma(\mathfrak{q}) = \tau\delta(\mathfrak{q}) = \tau(\mathfrak{q})$. Conversely, if $\sigma(\mathfrak{q}) = \tau(\mathfrak{q})$, then we have $\tau^{-1}\sigma(\mathfrak{q}) = \mathfrak{q}$, so $\tau^{-1}\sigma \in D$, and thus $\sigma D = \tau D$.

This establishes a one-to-one correspondence between the left cosets σD and the primes $\sigma\mathfrak{q};$. By Theorem 3.32, the set of primes of the form $\sigma(\mathfrak{q})$ exactly covers all primes of $\mathfrak{O}_L$ lying over p, and hence there are r of them. Thus $[L_D : K] = r$.

Next, we will show that the ramification index and the inertial degrees between $\mathfrak{q}_D$ and $\mathfrak{p}$, $e(\mathfrak{q}_D|\mathfrak{p})$ and $f(\mathfrak{q}_D|\mathfrak{p})$, both equal 1. We can consider the Galois group G_1 of L over L_D (since L is normal over $K \subseteq L_D$, G_1 is well defined), and we know the primes $\mathfrak{q}$ of L lying over $\mathfrak{q}_D$ are permuted transitively by the elements of G_1. However, $G_1 = D$ by our definition of D and Galois theory, and we know $\sigma(\mathfrak{q}) = \mathfrak{q}$ for all $\sigma \in D$. Thus there is only one prime of $\mathfrak{O}_L$ lying over $\mathfrak{q}_D$, namely $\mathfrak{q}$, so in the case of L over L_D, $r = 1$.

Applying Theorem 3.20 to this scenario, we see $[L : L_D] = e(\mathfrak{q}|\mathfrak{q}_D) \cdot f(\mathfrak{q}|\mathfrak{q}_D) \cdot 1$. Further,

we know $[L : L_D] = \frac{[L:K]}{[L_D:K]} = n/r = ref/r = ef$ (again by Theorem 3.20). Moreover, we note that $e(\mathfrak{q}|\mathfrak{q}_D) \leq e$ and $f(\mathfrak{q}|\mathfrak{q}_D) \leq f$ since these values are multiplicative in towers. Hence these inequalities must in fact be equalities, and therefore, since $e \cdot f = e(\mathfrak{q}|\mathfrak{q}_D) \cdot f(\mathfrak{q}|\mathfrak{q}_D)$, we see $e(\mathfrak{q}_D|\mathfrak{p}) = f(\mathfrak{q}_D|\mathfrak{p}) = 1$.

Once these bottom values have been established, we jump to the top of these towers. We will show $f(\mathfrak{q}|\mathfrak{q}_E) = 1$ by demonstrating that the Galois group G_2 of $\mathfrak{O}_L/\mathfrak{q}$ over $\mathfrak{O}_E/\mathfrak{q}_E$ is trivial (i.e. contains only the identity). To that end, let $\lambda \in \mathfrak{O}_L/\mathfrak{q}$, and fix any $\alpha \in \mathfrak{O}_L$ corresponding to λ, so $\lambda = \alpha + \mathfrak{q}$. Now consider the polynomial $g(x) = \prod_{\sigma \in E} (x - \sigma(\alpha))$. Note that the coefficients are in $\mathfrak{O}_E$ by Proposition 3.2. Now, reduce the coefficients modulo $\mathfrak{q}$ to generate a polynomial $\overline{g} \in (\mathfrak{O}_L/\mathfrak{q})[x]$. We find $\overline{g}$ actually has coefficients in $\mathfrak{O}_E/\mathfrak{q}_E$ since g had coefficients in $\mathfrak{O}_E$ and $\mathfrak{O}_E \cap \mathfrak{q} = \mathfrak{q}_E$. However, all $\sigma(\alpha)$ reduce to λ modulo $\mathfrak{q}$ since $\sigma \in E$, and thus $\overline{g}(x) = (x - \lambda)^m \in (\mathfrak{O}_E/\mathfrak{q}_E)[x]$, where $m = |E|$. Note that σ sends roots of $\overline{g}$ to other roots for all $\sigma \in G_2$, since $\overline{g}$ is a polynomial with coefficients in the fixed field of G_2. This means all $\sigma \in G_2$ map λ to λ, and since λ was arbitrary we have that all $\sigma \in G_2$ are the identity. Hence $f(\mathfrak{q}|\mathfrak{q}_E) = 1$.

Since $f(\mathfrak{q}_D|\mathfrak{p}) = f(\mathfrak{q}|\mathfrak{q}_E) = 1$, by Theorem 3.20 we must have $f(\mathfrak{q}_E|\mathfrak{q}_D) = f(\mathfrak{q}|\mathfrak{p}) = f$. Then, retaining our consideration of L_E (normal) over L_D, we can apply Theorem 3.20 again to define the lower bound $[L_E : L_D] \geq f$. But we know E is a normal subgroup of D and D/E is embedded in $\overline{\mathrm{G}}$, which is a group of order f. Then $[L_E : L_D] = |D/E| \leq f$; hence it must be exactly f. Then, by again applying Theorem 3.20 to L_E over L_D, we have $e(\mathfrak{q}_E|\mathfrak{q}_D) = 1$.

Finally, we complete our array and obtain $[L : L_E] = e$ and $e(\mathfrak{q}|\mathfrak{q}_E) = e$ by Theorem 3.20 and the figures already established. Thus all values are as desired. ☆

This result demonstrates some of the beautiful underlying structure of these intermediate fields and the splitting of primes within them. Let us now consider a special case, where we see the terms "inertial" and "decomposition" describe exactly what happens to primes in these special intermediate fields:

Corollary 3.40. *Let K, L, $\mathfrak{O}_K$, $\mathfrak{O}_L$, $\mathfrak{p}$, $\mathfrak{q}$, G, D, E, r, e, f, and n be as above, except suppose D is a normal subgroup of G. Then:*

(i) The prime $\mathfrak{p}$ of K splits into r distinct primes in L_D and L_E, so each factor $\mathfrak{p}'$ of $\mathfrak{p}\mathfrak{O}_D$ lies under a unique factor $\mathfrak{p}''$ of $\mathfrak{p}\mathfrak{O}_E$, and each factor $\mathfrak{p}''$ of $\mathfrak{p}\mathfrak{O}_E$ lies under a unique factor $\mathfrak{p}'''$ of $\mathfrak{p}\mathfrak{O}_L$;

If E is also a normal subgroup of G, then:

(ii) None of the r factors of $\mathfrak{p}\mathfrak{O}_E$ are ramified (neither over $\mathfrak{p}$ nor its unique $\mathfrak{p}'$);

(iii) Each of the r distinct prime factors of $\mathfrak{p}\mathfrak{O}_L$ is raised to the e^{th} power.

Proof. (i) If D is normal in G, then L_D is a normal extension of K by the Fundamental Theorem of Galois Theory. By Corollary 3.33, every prime $\mathfrak{p}'$ of $\mathfrak{O}_D$ lying over $\mathfrak{p}$ has the same ramification index and inertial degree, and by Theorem 3.39 we know both of these are 1. Therefore, by Theorem 3.20, there must be exactly r such primes in $\mathfrak{O}_D$ lying over $\mathfrak{p}$. Building off this result, since $\mathfrak{p}$ splits into r primes in L_D and L, it must also do so in L_E.

(ii) If E is normal in G, then L_E is also a normal extension of K, and hence a normal extension of $L_D \supseteq K$. We must show that none of the $\mathfrak{p}''$ are ramified over $\mathfrak{p}$ and $\mathfrak{p}'$. However, this follows directly when E is normal over K since Theorem 3.39 and Corollary 3.33 state that $e(\mathfrak{p}''|\mathfrak{p}) = e(\mathfrak{q}_E|\mathfrak{p}) = 1$, so $e(\mathfrak{p}''|\mathfrak{p}') = 1$. Thus each factor $\mathfrak{p}'$ of $\mathfrak{p}\mathfrak{O}_D$ is inert between $\mathfrak{O}_D$ and $\mathfrak{O}_E$.

(iii) Since $e(\mathfrak{p}''|\mathfrak{p}) = 1$, we have $e(\mathfrak{p}'''|\mathfrak{p}'') = \frac{e(\mathfrak{p}'''|\mathfrak{p})}{e(\mathfrak{p}''|\mathfrak{p})} = e/1 = e$. Therefore for each factor $\mathfrak{p}''$ of $\mathfrak{p}\mathfrak{O}_E$, $\mathfrak{p}''\mathfrak{O}_L = (\mathfrak{p}''')^e$, and thus each prime factor of $\mathfrak{p}\mathfrak{O}_L$ is raised to the e^{th} power.

Definition 3.41. Let $K \subseteq L$ be number fields with number rings $\mathfrak{O}_K$ and $\mathfrak{O}_L$ respectively. If $\mathfrak{p}$ is a prime in $\mathfrak{O}_K$, we say $\mathfrak{p}$ is *inert in* L if $\mathfrak{p}\mathfrak{O}_L$ is also a prime in $\mathfrak{O}_L$.

Clearly, in the situation above (where D and E are normal subgroups of G), a prime $\mathfrak{p}$ splits into its r components by the time it reaches L_D, and then these primes remain inert up through L_E, after which they ramify.

We will continue with some examples that show the power and usefulness of Theorem 3.39 and its corollaries.

Example 3.42. It can be shown that $\mathfrak{p} = \langle 2 \rangle \subseteq \mathbb{Z}$ splits into two distinct primes in the number ring $\mathbb{Z}[\sqrt{-23}]$ associated with the number field $K = \mathbb{Q}[\sqrt{-23}]$, and further that these two factors remain prime in $L = \mathbb{Q}[\omega]$, where $\omega = e^{2\pi i/23}$ (one can show that $\mathbb{Q}[\sqrt{-23}] \subseteq \mathbb{Q}[\omega]$). Thus, with notation as above, we see $r = 2$, so the decomposition field has degree two over $\mathbb{Q}$. Moreover, since the Galois group of L over $\mathbb{Q}$ is cyclic of order 22, and the factors of the order of a cyclic group are in 1-1 correspondence with its subgroups, there is exactly one subgroup (which must be normal) of order two. Hence there exists exactly one subextension of degree 2, namely $\mathbb{Q}[\sqrt{-23}]$, and therefore it must be the case that $L_D = \mathbb{Q}[\sqrt{-23}]$. Further, since $\langle 2 \rangle$ is not ramified in $\mathbb{Q}[\omega]$, the inertial field is the entire field $L_E = L = \mathbb{Q}[\omega]$. [For more details, see MARCUS [5] p.40, 74–76, 86]

This behavior is true in a more general case:

Proposition 3.43. *Let L be a normal extension of a number field K with cyclic Galois group G, and take $\mathfrak{p}$ to be a prime in K which splits into r primes in L. Then the decomposition field L_D is the unique intermediate field of degree r over K, and $\mathfrak{p}$ splits into r primes in every intermediate field containing the decomposition field.*

Proof. Recall the properties of cyclic groups listed in the above example: all subgroups of a cyclic group are normal, and the factors of the order of the group are in 1-1 correspondence with its subgroups, which are further in 1-1 correspondence with the subextensions L_H of L over K. Note that Theorem 3.20 requires L_D to have degree r, and hence there is exactly one subextension which satisfies this condition. Then, by Corollary 3.40 we see $\mathfrak{p}$ splits into exactly r primes in this subfield L_D. Now, since $\mathfrak{p}$ splits into r primes in L, in any subfield F such that $L_D \subseteq F \subseteq L$, $\mathfrak{p}$ splits into exactly r primes. ☆

Let us look at another example with an abelian Galois group:

Example 3.44. Let $L = \mathbb{Q}[i, \sqrt{2}, \sqrt{5}]$, and $K = \mathbb{Q}$. Then L is a normal extension of degree 8 over K, and the Galois group is the direct sum of three cyclic groups of order 2. Let us observe how the prime $\langle 5 \rangle$ of $\mathbb{Q}$ behaves in each of the obvious subextensions. As we have seen before, it splits into two primes $\langle 2+i \rangle$ and $\langle 2-i \rangle$ in $\mathbb{Q}[i]$, and becomes a square $\langle \sqrt{5} \rangle^2$ in $\mathbb{Q}[\sqrt{5}]$. Further, it is inert in $\mathbb{Q}[\sqrt{2}]$: since $\mathbb{Z}[\sqrt{2}]$ is a unique factorization domain (see HARDY AND WRIGHT [2] p.217) and here the element 5 is clearly irreducible, by Proposition 2.29 $\langle 5 \rangle$ is a prime ideal. Therefore, if $\langle 5 \rangle \mathfrak{O}_L = (\mathfrak{q}_1 \dots \mathfrak{q}_r)^e$, then:

(i) the number of primes $r \geq 2$ (there must exist at least two factors to lie over the split in $\mathbb{Q}[i]$);

(ii) the ramification index $e \geq 2$ (there is a square below, so must be squares above);

(iii) the inertial degree $f \geq 2$ ($f = 2$ in $\mathbb{Q}[\sqrt{2}]$ since $ref = 2$ and $r = e = 1$).

By Theorem 3.20, each must be exactly 2. By Theorem 3.39 the inertial field must be of degree 4 over $\mathbb{Q}$ (since $r = f = 2$) where $\langle 5 \rangle$ is still unramified (since by Corollary 3.40 all ramification occurs between L_E and L). The only choice is $\mathbb{Q}[i, \sqrt{2}]$. Thus $\langle 2 + i \rangle$ and $\langle 2 - i \rangle$ remain prime in $\mathbb{Q}[i, \sqrt{2}]$, and become squares of primes in L.

Finally, let us consider an example where the Galois group is non-abelian:

Example 3.45. Take $K = \mathbb{Q}$ and $L = \mathbb{Q}[\sqrt[3]{19}, \omega]$ where $\omega = e^{2\pi i/3}$. Then we know L is normal over K, and it can be shown that the Galois group $G = Gal(L/K)$ equals S_3, the permutation group over three letters [see MARCUS [5] p.103].

Let us consider how the prime $\langle 3 \rangle$ of $\mathbb{Z}$ splits in L. If we look at the two most obvious subfields of L, we see that in $\mathbb{Q}[\omega] = \mathbb{Q}[\sqrt{-3}]$, $\langle 3 \rangle$ is a square (namely $\langle \sqrt{-3} \rangle^2$), and it can be shown that it has the form $\mathfrak{p}^2\overline{\mathfrak{p}}$ in $\mathbb{Q}[\sqrt[3]{19}]$, where $\mathfrak{p}$ and $\overline{\mathfrak{p}}$ are primes. Thus, in L, there must be at least two primes lying over $\langle 3 \rangle$, and each must have a ramification index divisible by 2 (since each must lie over a square). Therefore it must be the case that $\langle 3 \rangle$ splits into three primes in L, each with $e = 2$ and $f = 1$.

By Theorem 3.20, since $r = 3$, the decomposition field for any of these three primes over $\mathbb{Q}$ has degree 3. There are three such subfields of L: $\mathbb{Q}[\sqrt[3]{19}]$, $\mathbb{Q}[\omega\sqrt[3]{19}]$, and $\mathbb{Q}[\omega^2\sqrt[3]{19}]$. This

gives us three towers of fields over $\langle 3 \rangle$, with one of these subfields acting as the decomposition field in each tower. It its interesting to note that each of these fields can be sent to any other by an automorphism of L since they are all roots of the polynomial $t^3 - 19$. In each of them, $\langle 3 \rangle$ would again decompose as above in the form $\mathfrak{p}^2\overline{\mathfrak{p}}$. Further, since $f = 1$ for both primes, the inertial field is the same as the decomposition field in each of these three towers.

It is important to notice that $\langle 3 \rangle$ does not split into three distinct primes in any of the three possible decomposition fields; in each it is of the form $\mathfrak{p}^2\overline{\mathfrak{p}}$ and hence is ramified in each. This verifies that the normality condition is necessary in Corollary 3.40.

The general conclusion we take from the above theorems and examples is that these two fields, the decomposition field and inertial field, are special and play a vital role in the structure of how primes split between K and L.

Bibliography

[1] D. Han, K. Kornelson, D. Larson, and E. Weber. *Frames for Undergraduates*. American Mathematical Society, USA 2007.)

[2] G.H. Hardy and E.M. Wright. *An Introduction to the Theory of Numbers* (5th ed.), Clarendon Press, Oxford 1979.

[3] I.N. Herstein. *Abstract ALgebra* (3rd ed.), John Wiley & Sons, USA 1999.

[4] J.M. Howie. *Fields and Galois Theory*. Springer, London 2006.

[5] D.A. Marcus. *Number Fields*, Springer, New York 1977.

[6] I. Stewart. *Galois Theory* (2nd ed.), Chapman & Hall/CRC, New York 1983.

[7] I. Stewart and D. Tall. *Algebraic Number Theory and Fermat's Last Theorem* (3rd ed.), A K Peters, Natick 2002.