Algebraic Number Theory Notes

JJ Hoo

Fall 2022

Contents

1 Algebraic Numbers and Algebraic Integers

1.1 Introduction

Definition 1.1.1. *A number $\alpha \in \mathbb{C}$ is called algebraic number if there exists $0 \neq f(x) \in \mathbb{Q}[x]$ such that $f(\alpha) = 0$. In other words, α is algebraic over $\mathbb{Q}$.*

Note that if α is an algebraic number, then there exists $0 \neq g(x) \in \mathbb{Z}[x]$ such that $g(\alpha) = 0$[1].

Definition 1.1.2. *α is an algebraic integer if there exists $0 \neq f(x) \in \mathbb{Z}[x]$ where f is monic, such that $f(\alpha) = 0$.*

Proposition 1.1.1. *Every algebraic integer is an algebraic number. On the other hand, the converse is false.*

Example 1.1.1. *Let $\alpha = \frac{\sqrt{2}}{3}$. This is an algebraic number, but NOT an algebraic integer.*

Consider $f(x) = 9x^2 - 2 \in \mathbb{Z}[x] \subseteq \mathbb{Q}[x]$. Then, $f(\alpha) = 0$, so α is an algebraic number.

Now, let $g(x) \in \mathbb{Z}[x]$ be a monic polynomial such that $g(\alpha) = 0$. Then, $g(x) = x^n + a_{n-1}x^{n-2} + \cdots + a_1 x + a_0$, where $a_1, \cdots, a_{n-1} \in \mathbb{Z}$.

$$
\begin{aligned}
g(\alpha) = 0 &\implies \left(\frac{\sqrt{2}}{3}\right)^n + a_{n-1}\left(\frac{\sqrt{2}}{3}\right)^{n-1} + \cdots + a_1\left(\frac{\sqrt{2}}{3}\right) + a_0 = 0 \\
&\implies (\sqrt{2})^n + a_{n-1}(\sqrt{2})^{n-1} \cdot 3 + \cdot + a_1(\sqrt{2}) \cdot 3^{n-1} + a_0 3^n = 0 \\
&\implies \sum_{t=0}^{n} (\sqrt{2})^t a_t 3^{n-t} = 0 \\
&\implies \underbrace{\sum_{t \text{ even}} (\sqrt{2})^t a_t 3^{n-t}}_{\in \mathbb{Z}} + \underbrace{\sum_{t \text{ odd}} (\sqrt{2})^t a_t 3^{n-t} = 0}_{\in \sqrt{2}\mathbb{Z} \neq \mathbb{Z}} \\
&\implies \overbrace{\sum_{t \text{ even}} (\sqrt{2})^t a_t 3^{n-t} = 0}^{\textit{Case 1}} \wedge \overbrace{\sqrt{2} \underbrace{\sum_{t \text{ odd}} (\sqrt{2})^{t-1} a_t 3^{n-t} = 0}_{\in \mathbb{Z}}}^{\textit{Case 2}}
\end{aligned}
$$

If n is even, we use Case 1 to get an extra term of $2^{\frac{n}{2}}$ and 3 divides the remaining terms, so we reach a contradiction. If n is odd, we repeat this for Case 2. Thus, no such monic g exists, and so α is not an algebraic integer.

Every $\alpha \in \mathbb{Q}$ is an algebraic number[2]. Now, we consider $\mathbb{Q} \cap \{\text{algebraic integers}\}$.

Let $\alpha = \frac{r}{s} \in \mathbb{Q}$ be an algebraic integer, where $gcd(r, s) = 1$ and $s \neq 0$. There exists, then, a monic non-zero $f(x) \in \mathbb{Z}[x]$ such that $f(\alpha) = 0$.

Let $f(x) = x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0$. Using the same trick as before, we multiply to get:

$$r^n = -(a_{n-1}r^{n-1}s + \cdots + a_1 r s^{n-1})$$

[1] This is done by multiplying $f(x)$ through by the LCM

[2] Take $f(x) = x - \alpha \in \mathbb{Q}[x]$

However, this implies $s|r^n$. If p is a prime dividing s, then $p|r^n \implies p|r \implies gcd(r,s) \geq p \implies s = 1 \implies \alpha = r \in \mathbb{Z}$.

In conclusion, $\mathbb{Z}$ is the set of algebraic integers in $\mathbb{Q}$.

1.2 Minimal Polynomials

Theorem 1.2.1. *Let α be an algebraic number. Then, there exists a unique polynomial $p(x) \in \mathbb{Q}[x]$ which is monic, irreducible and of lowest degree such that $p(\alpha) = 0$. By definition, $p(x)$ is the minimal polynomial of α over $\mathbb{Q}$. Furthermore, if $f(x) \in \mathbb{Q}[x]$ and $f(\alpha) = 0$, then $p(x)|f(x)$.*

Proof. Since α is an algebraic number, there exist a set of polynomials of the form $f(x) \in \mathbb{Q}[x]$ such that $f(\alpha) = 0$. We choose $p(x)$ from this set to be of lowest degree. We must show that $p(x)$ is irreducible.

Let $p(x) = a(x)b(x)$, where $a(x), b(x) \in \mathbb{Q}[x]$, $deg(a(x)) < deg(p(x))$, and $deg(b(x)) < deg(p(x))$. In other words, assume that $p(x)$ is reducible.

$$0 = p(\alpha) = a(\alpha)b(\alpha)$$

Note that since $\mathbb{C}$ is an integral domain, we get that either $a(\alpha) = 0$ or $b(\alpha) = 0$. This immediately gives a contradiction, as $a(x)$ and $b(x)$ now belong to our original set of possible $f(x)'s$, and are both of lower degree than $p(x)$. Thus, $p(x)$ is irreducible. We can force this to be monic by multiplication of the inverse of the leading coefficient, since $\mathbb{Q}$ is a field. We have thus constructed a $p'(x) \in \mathbb{Q}[x]$ which is monic, irreducible, and of lowest degree.

It remains to be shown that our monic, irreducible polynomial $p(x)$ of lowest degree is unique. Suppose $g(x)$ is another such polynomial. Since $\mathbb{Q}[x]$ is a Euclidean Domain, we enjoy the Division Algorithm, and so $f(x) = q(x)g(x) + r(x)$, where $q(x), r(x) \in \mathbb{Q}[x]$, and either $deg(r(x)) < deg(g(x))$ or $r(x) = 0$. So

$$0 = p(\alpha) = q(\alpha)\underbrace{g(\alpha)}_{=0} + r(\alpha) \implies r(\alpha) = 0$$

Since $g(x)$ is of minimal degree, we must then have $r(x) = 0$. Thus, $p(x) = q(x)g(x)$. Since $p(x)$ and $g(x)$ are of minimal degree, they must have the same degree, which means in turn that $q(x) = c$ for some $c \in \mathbb{Q}$. Given now that $p(x) = cg(x)$ and that p and g are monic, we must have $c = 1$, and so we have our result that $p(x) = g(x)$.

Now, let $f(x) \in \mathbb{Q}[x]$ such that $f(\alpha) = 0$. Then, $f(x) = q(x)p(x) + r(x)$ with $deg(r(x)) < deg(p(x))$ or $r(x) = 0$. By a similar argument as above, $p(\alpha) = 0 \implies r(x) = 0$ by minimality of $p(x)$, so $p(x)|f(x)$. □

Definition 1.2.1. *We denote the degree of α over $\mathbb{Q}$ as $deg_{\mathbb{Q}}(\alpha) = deg(p(x))$, where $p(x)$ is the minimal polynomial of α.*

Example 1.2.1. *Find the minimal polynomial of $\alpha = \sqrt{1+\sqrt{7}}$.*

Let $x = \sqrt{1+\sqrt{7}}$.

$$x^2 = 1 + \sqrt{7}$$
$$x^2 - 1 = \sqrt{7}$$
$$(x^2 - 1)^2 = 7$$
$$x^4 - 2x^2 - 6 = 0$$

Now, let $p(x) = x^4 - 2x^2 - 6$. Then, $p(\alpha) = 0$. p is already monic, so we use Eisenstein's Creiterion with $p = 2$. Since $2^2 \not| 6$, $p(x)$ is indeed irreducible

As a reminder, Eisenstein's Criterion states that if $f(x) = \sum_{i=0}^{n} a_i x^i$, where $a_i \in \mathbb{Z}$, if there is a prime p such that $p \not| a_n$,, $p|a_i$ otherwise, and $p^2 \not| a_0$, then $f(x)$ is irreducible over $\mathbb{Q}$. Another method to keep in mind here would be the Rational Roots Theorem.

1.3 Number Fields

Definition 1.3.1. *Let E, F be fields, where $F \subseteq E$. We call E an extension of F (or a field extension), and F is denoted as the base field. For instance, $\mathbb{C}$ is an extension of $\mathbb{Q}$. We further note that E is a vector space over F.*

Recall that if F is a field, and E is an extension of F such that $\alpha \in E$:

$$F[\alpha] = \{f(\alpha) : \ f(x) \in F[x]\} \subseteq E$$

$$F(\alpha) = \{\frac{f(\alpha)}{g(\alpha)} : \ f(x), g(x) \in F[x], g(\alpha) \neq 0\} \subseteq E$$

$F[\alpha]$ is the smallest subring of E containing α, and $F(\alpha)$ is the smallest subfield of E containing α. We note that $F[\alpha] = F(\alpha)$ iff α is algebraic over F.

Definition 1.3.2. *Let α be an algebraic number. Define : $\mathbb{Q}[\alpha] := \{f(\alpha) : \ f(x) \in \mathbb{Q}[x]\}$*

Proposition 1.3.1. *Let α be an algebraic number. $\mathbb{Q}[\alpha]$ is a field, which we will then denote $\mathbb{Q}(\alpha)$.*

Proof. Let $p(x)$ be the minimal polynomial of α Consider $\phi_\alpha : \mathbb{Q}[x] \to \mathbb{Q}[\alpha]$, where $\phi_\alpha(f(x)) = f(\alpha)$. ϕ_α is a ring homomorphism. We note that

$$ker(\phi) = \{f \in \mathbb{Q}[x] : \ \phi(f) = 0\} = \langle p(x) \rangle$$

By the First Isomorphism Theorem, we then have that:

$$\mathbb{Q}[x]/\langle p(x) \rangle = \mathbb{Q}[\alpha]$$

Since $p(x)$ is irreducible, we have that $\langle p(x) \rangle$ is a maximal ideal, so $\mathbb{Q}[x]/\langle p(x) \rangle$ is a field since it is the quotient of an integral domain by a maximal ideal. Thus, $\mathbb{Q}[\alpha]$ is a field. □

Definition 1.3.3. *A field $\mathbb{Q} \subseteq K \subseteq \mathbb{C}$ is an algebraic number field if its dimension as a vector space over $\mathbb{Q}$ is finite.*

Suppose $F \subseteq E$ is a finite extension. We write $[E : F] = \dim_F(E)$. Furthermore, every finite extension is an algebraic extension.

Definition 1.3.4. *E is an algebraic extension of F if every element $\alpha \in E$ is algebraic over F. In other words, $\exists f(x) \in F[x]$ such that $f(\alpha) = 0$.*

We note that $deg_F(\alpha) \leq [E : F]$ if E is a finite extension of F.

So, if K is an algebraic number field, then $K = \mathbb{Q}(\alpha_1, \alpha_2, \cdots, \alpha_n)$ for some $n \in \mathcal{N}$. We note here that $\mathbb{Q}(\alpha, \beta) = \mathbb{Q}(\alpha)$. The dimension of K over $\mathbb{Q}$ is denoted $[K : \mathbb{Q}]$.

If α is an algebraic number, and $deg(\alpha) = n$, then $\mathbb{Q}(\alpha)$ is an algebraic number field, and $[\mathbb{Q}(\alpha) : \mathbb{Q}] = n$, with basis $\{\alpha^i\}_{i=0}^{n-1}$.

Lemma 1.3.1. *Let $F \subseteq \mathbb{C}$ be a subfield of $\mathbb{C}$. Let $f(x) \in F[x]$ of degree n be irreducible. Then $f(x)$ has n distinct roots.*

Proof. Let $f(x) = \sum_{i=0}^{n} a_i x^i$. Recall the formal derivative $f'(x) = \sum_{i=1}^{n} a_i(n-i)x^{n-1}$. Assume, for the sake of contradiction, that $f(x)$ has a repeated root $\alpha \in \mathbb{C}$. In other words, $(x-\alpha)^2 | f(x)$. Let:

$$f(x) = (x-\alpha)^2 g(x) \implies p'(x) = (x-\alpha)^2 g'(x) + 2g(x)(x-\alpha)$$

Thus, $f'(\alpha) = 0$. Let $h(x) = gcd(f(x), f'(x)) \in F[x]$. Note $f'(x) \in F[x]$, and there exist $u(x), v(x) \in F[x]$ such that:

$$h(x) = u(x)f(x) + v(x)f'(x) \implies h(\alpha) = 0$$

Thus, $h|f$, but f is irreducible over F, so $h(x) = c$ or $h(x) = cf(x)$, where $c \in F\backslash\{0\}$. $h(\alpha) = 0$, so we must have that $h(x) = cf(x)$. Then, $f|f'$ because $h|f'$. Thus, there are no repeated roots, so $f(x)$ has n distinct roots in $\mathbb{C}$ □

Theorem 1.3.1 (Primitive Element Theorem)**.** *If α and β are algebraic numbers, then there exists an algebraic number θ such that $\mathbb{Q}(\alpha, \beta) = \mathbb{Q}(\theta)$*

Proof. Let $p(x) = \prod_{i=1}^{n} x - \alpha_i$ and $q(x) = \prod_{i=1}^{m} x - \beta_i$ be the minimal polynomials of $|alpha$ and β respectively, where $\alpha_1 = \alpha$ and $\beta_1 = \beta$. By the previous lemma, all these coefficients are distinct in $\mathbb{C}$.

Consider for any $1 \leq i \leq n$, $2 \leq j \leq m$:

$$\alpha_i + \lambda\beta_j = \alpha + \lambda\beta \tag{1}$$

This implies that $\lambda_{ij} = \frac{\alpha_i - \alpha}{\beta_j - \beta}$. Thus, Equation (1) holds for exactly one value of $\lambda \in \mathbb{C}$ (for a fixed i, j) and at most one $\lambda \in \mathbb{Q}$.

Now, choose $0 \neq c \in \mathbb{Q}$ such that $\alpha_i + c\beta_j \neq \alpha + c\beta$, for every $1 \leq i \leq n$, and every $2 \leq j \leq m$. Such a c always exists because there are only finitely many extensions. This choice is equivalent to choosing $0 \neq c \in \lambda$ such that $c \neq \lambda_{ij}$ for all i, j.

Now, let $\theta = \alpha + C\beta$. We will now show that $\mathbb{Q}(\alpha, \beta) = \mathbb{Q}(\theta)$. Note that $\theta = \alpha + c\beta \implies \theta\mathbb{Q}(\alpha, \beta) \implies \mathbb{Q}(\theta) \subseteq \mathbb{Q}(\alpha, \beta)$. It remains to show that backwards inclusion.

If $\beta \in \mathbb{Q}(\theta)$, then $\alpha = \theta - c\beta \in \mathbb{Q}(\theta)$, so it suffices to show that $\beta \in \mathbb{Q}(\theta)$. Let $r(x) + p(\theta - cx) \in \mathbb{Q}(\theta)[x]$, and $r(\beta) = p(\theta - c\beta) = p(\alpha) = 0$. So β is a common root of $r(x)$ and $q(x)$. Let t be another common root of $r(x)$ and $q(x)$. Then, $t \in \{\beta_j\}_{j=2}^{m}$. Now, for $2 \leq j \leq m$, $r(\beta_j) = p(\theta - c\beta_k)$

So, if $0 = r(\beta_j)$, then $0 = p(\theta - c\beta_k) \implies \theta - c\beta_j \in \{\alpha\}_{i=1}^{n}$. Thus, β is the only common root of $r(x)$ and $p(x)$.

Let $h(x)$ be the minimum polynomial of β over $\mathbb{Q}(\theta)$. This implies that $h(x)|r(x)$ and $h(x)|q(x)$, so β is the only root of $h(x)$ in $\mathbb{C}$, so $deg(h(x)) = 1$, and in particular, $h(x) = x - \beta \in \mathbb{Q}(\theta)[x]$. This means we must have that $\beta \in \mathbb{Q}(\theta)$, and so we are done! □

By induction, $\mathbb{Q}(\alpha_1, \cdots, \alpha_n\} = \mathbb{Q}(\theta)$. Thus, all algebraic number fields can be represented as $\mathbb{Q}(\theta)$ for some algebraic number θ.

Theorem 1.3.2. *Every algebraic number θ is of the form $\frac{\alpha}{c}$ where α is an algebraic integer and $c \in \mathbb{Q}$.*

Proof. Let $f(x)$ be the minimum polynomial of θ, $deg(f) = n$. The coefficients of f are rational. Let c be the lowest common multiple of all the denominators of the a_i's. Now, consider:

$$g(x) = x^n + ca_{n-1}x^{n-1} + c^2a_{n-2}x^{n-2} + \cdots c^n a_0$$

Note the general term above is $c^t a_{n-t}x^{n-t}$. Now:

$$g(c\theta) = c^n(\theta^n + a_{n-1}\theta^{n-1}\cdots) = f(\theta) = 0$$

Note that $g(x) \in \mathbb{Z}[x] \implies c\theta$ is an algebraic integer, so let $\alpha = c\theta$. Then, $\theta = \frac{\alpha}{c}$ as desired. □

Corollary 1.3.1. *Every algebraic number field can be represented by $\mathbb{Q}(\alpha)$ for some algebraic integer α*

Proof. We know every algebraic number field can be represented by $\mathbb{Q}(\theta)$, where θ is an algebraic number. But $\theta = \frac{\alpha}{c}$. where $c \in \mathbb{Z}$ and α is an algebraic integer, so $\mathbb{Q}(\theta) = \mathbb{Q}(\frac{\alpha}{c}) = \mathbb{Q}(\alpha)$. □

Example 1.3.1. *Find the value of θ such that:*

$$\mathbb{Q}(\sqrt{2}, \sqrt[3]{6}) = \mathbb{Q}(\theta)$$

The minimum polynomial of $\sqrt{2}$ is $f(x) = x^2 - 2 = (x - \sqrt{2})(x + \sqrt{2})$. The minimum polynomial of $\sqrt[3]{5}$ is $g(x) = x^3 - 5 = (x - \sqrt[3]{5})(x - w\sqrt[3]{5})(x - w^2\sqrt[3]{5})$, where $w = -\frac{1}{2} + \frac{\sqrt{3}}{2}i$. Choose c such that $\alpha_i + c\beta_j \neq \alpha + c\beta$ for any $i = 1, 2$, $j = 2, 3$. Choose $c = 1$, and this works. So take $\theta = \alpha + c\beta = \alpha + \beta = \sqrt{2} + \sqrt[3]{5}$.

The minimum polynomial of $\sqrt{2} + \sqrt[3]{5}$ can be left as an exercise, but turns out to be $f(x) = x^6 - 6x^2 - 10x^3 + 12x^2 - 60x + 16$.

Definition 1.3.5. *Now, let α be an algebraic number with minimum polynomial of degree n. Then*

$$p(x) = \prod_{i=1}^{n} x - \alpha_i \in \mathbb{Q}[x]$$

where by the Lemma, all α_i's are distinct complex numbers. $\alpha = \alpha_1, \alpha_2, \alpha_3, \cdots, \alpha_n$ are called the <u>conjugates</u> of α.

Then, we have n field isomorphisms (embeddings):

$$\sigma_i : \mathbb{Q}(\alpha) \to \mathbb{Q}(\alpha_i)$$

with $\alpha \mapsto \alpha_i$. Note: These conjugate fields are independent of choice of α.

If $K = \mathbb{Q}(\alpha) = \mathbb{Q}(\beta)$, then $\exists\ c_i \in \mathbb{Q}$ such that

$$\beta = c_0 + c_1\alpha + c_2\alpha^2 + \cdots + c_{n-1}\alpha^{n-1}$$

For $t = 1, 2, \cdots, n$, set

$$\beta_t = c_0 + c_1\alpha_1 + c_2\alpha_2^2 + \cdots + c_{n-1}\alpha_t^{n-1} = \sigma_i(\beta)$$

Then the β_i's are the conjugates of β and $\mathbb{Q}(\alpha_t) = \mathbb{Q}(\beta_t)$, for every $t = 1, 2, \cdots, n$.

1.4 Symmetric Polynomials

Definition 1.4.1. *Let S_n denote the symmetric group on n letters. For any $\sigma \in S_n$ and $f \in \mathbb{F}[x_1, x_2, \cdots, x_n]$, where $\mathbb{F}$ is a field, define*

$$f^\sigma(x_1, x_2, \cdots, x_n) = f(x_{\sigma(1)}, \cdots, x_{\sigma(n)})$$

A polynomial f is symmetric if $f^\sigma = f$, for every $\sigma \in S_n$

Example 1.4.1. *$f(x_1, x_2, x_3) = x_1 + x_2 + x_3$ is symmetric.*

Example 1.4.2. *$f(x_1, x_2, x_3) = x_1 + x_2x_3$. Then, if $\sigma = (1\ 2\ 3)$, $f^\sigma = x_2 + x_3x_1$, so f is not symmetric.*

Definition 1.4.2. *The elementary symmetric polynomials are defined as:*

$$e_0(x_1, \cdots, x_n) = 1$$
$$e_1(x_1, \cdots, x_n) = x_1 + x_2 + \cdots + x_n$$
$$e_2(x_1, \cdots, x_n) = \sum_{1 \le i \le j \le n} x_i x_j$$
$$e_n(x_1, \cdots, x_n) = x_1 x_2 \cdots x_n$$

Theorem 1.4.1 (Fundamental Theorem of Symmetric Polynomials)**.** *Every symmetric polynomial can be written uniquely as a polynomial expression (not necessarily symmetric) in the elementary symmetric polynomials. In other words, if $f(x_1, \cdots, x_n) \in \mathbb{F}[x_1, \cdots, x_n]$, is a symmetric polynomial, then there exists a g such that $f(x_1, \cdots, x_n) = g(e_1(x_1, \cdots, x_n), \cdots, e_n(x_1, \cdots, x_n))$. $\mathbb{F}$ could just be a commutative ring that is not a field.*

Example 1.4.3. *Let $f(x_1, x_2) = x_1^3 + x_2^3 - 7$ be symmetric. Let $g(x_1, x_2) = x_1^3 - 3x_1x_2 - 7$ be not symmetric. But then, we see that:*

$$\begin{aligned} f(x_1, x_2) &= g(e_1(x_1, x_2) + e_2(x_1, x_2)) \\ &= q(x_1, x_2)^3 - 3e_1(x_1, x_2)e_2(x_1x_2) - 7 \end{aligned}$$

Proposition 1.4.1. *Suppose $p(x) \in \mathbb{Q}[x]$ (monic) has roots $\alpha_1, \cdots, \alpha_n$, and any symmetric polynomial $f(x_1, \cdots, x_n)) \in \mathbb{Q}[x_1, \cdots, x_n]$, then $f(\alpha_1, \cdots, \alpha_n) \in \mathbb{Q}$*

Proof. $p(x) = \prod_{i=1}^{n}(x - \alpha_i) \in \mathbb{Q}[x]$, so $e_t(\alpha_1, \cdots, \alpha_n) \in \mathbb{Q}$, for every $1 \le t \le n$. By the Fundamental Theorem of Symmetric Polynomials, there exists $g(x_1, \cdots, x_n) \in \mathbb{Q}[x_1, \cdots, x_n]$ such that $f(x_1, \cdots, x_n) = g(e_1(x_1, \cdots, x_n), \cdots, e_n(x_1, \cdots, x_n))$. So:

$$f(\alpha_1, \cdots, \alpha_n) = g(e_1(x_1, \cdots, x_n), \cdots, e_n(x_1, \cdots, x_n)) \in \mathbb{Q}$$

□

Theorem 1.4.2. *Embeddings are independent of choice of α. In other words, let $K = \mathbb{Q}(\alpha)$ be an algebraic number field, and $p(x) = \prod_{i=1}^{n}(x - \alpha_i) \in \mathbb{Q}$ be a minimum polynomial of α with $\alpha = \alpha_1$. The embeddings are $\alpha \to \alpha_i$. If $K = \mathbb{Q}(\beta)$ also, $\beta = c_0 + c_1\alpha + c_2\alpha^2 + \cdots + c_{n-1}\alpha^{n-1}$ because these powers from a basis for $K = \mathbb{Q}(\alpha)$. Let $\beta_i = \sigma_i(\beta)$ for $1 \leq i \leq n$. Then, $\beta = \beta_1, \beta_2, \cdots, \beta_n$ are the conjugates of β and $\mathbb{Q}(\alpha_i) = \mathbb{Q}(\beta_i)$ for every $1 \leq i \leq n$.*

Proof. Let

$$\begin{aligned} f(x) &= \prod_{i=1}^{n}(x - \beta_i) \\ &= \prod_{i=1}^{n}(x - \sigma_i(\beta)) \\ &= \prod_{i=1}^{n}(x - (c_0 + c_1\alpha_i + c_2\alpha_i^2 + \cdots + c_{n-1}\alpha_i^{n-1})) \\ &\in \underbrace{\mathbb{Q}(\alpha_1, \alpha_2, \cdots, \alpha_n)}_{K_1}[x] \end{aligned}$$

So $\mathbb{Q} \subseteq K \subseteq K_1 \subseteq \mathbb{C}$. Now:

$$\begin{aligned} p(x) &= \prod_{i=1}^{n}(x - \beta_i) \\ &= x^n - e_1(\beta_1, \cdots, \beta_n)x^{n-1} + \cdots + (-1)^n e_n(\beta_1, \cdots, \beta_n) \end{aligned}$$

Each $e_i(\beta_1, \cdots, \beta_n)$ will be symmetric in the α's. Thus, by the fundamental theorem, there exists $g(x_1, \cdots, x_n) \in \mathbb{Q}[x]$ such that $e_t(\beta_1, \cdots, \beta_n) = g_t(\alpha_1, \cdots, \alpha_n)$. From Proposition 3, we get that $g_t \in \mathbb{Q}$, so each $e_t \in \mathbb{Q}$, so $f(x) \in \mathbb{Q}[x]$.

S0 $f(x) = \prod_{i=1}^{n}(x - \beta_i) \in \mathbb{Q}[x]$. $f(\beta) = 0$, so if $h(x)$ is the minimal polynomial for β, then $h|f$. But $deg(f) = n$ and $[\mathbb{Q}(\beta) : \mathbb{Q}] = [\mathbb{Q}(\alpha) : \mathbb{Q}] = n$, so $deg(h) = n$. Since h and f are monic of the same degree, we must have that $h = f$, so $f(x)$ is the minimum polynomial of β. But the conjugate fields are $\mathbb{Q}(\beta_i) \subseteq \mathbb{Q}(\alpha_i)$, and both are of degree n, so finally we get that $\mathbb{Q}(\beta_i) = \mathbb{Q}(\alpha_i)$. □

1.5 Sets of Algebraic Integers as Rings - $\mathcal{O}_K$

Definition 1.5.1. *Let $\mathcal{O} \subseteq \mathbb{C}$ be the set of all algebraic integers*

Theorem 1.5.1. *The following are equivalent:*

(a) α is an algebraic integer

(b) The minimum polynomial of α is in $\mathbb{Z}[x]$.

(c) $\mathbb{Z}[\alpha]$ is a finitely generated $\mathbb{Z}$-module.

(d) There exists a finitely generated $\mathbb{Z}$-submodule of $\mathbb{C}$, $M \neq \{0\}$ such that $\alpha M \subseteq M$.

Proof. $(a) \implies (b)$:

Since α is an algebraic integer, there exists $f(x) \in \mathbb{Z}[x]$ monic such that $f(\alpha) = 0$. Choose $p(x)$ of minimum degree from such $f(x)$'s. Then, $p(X)$ is irreducible over $\mathbb{Z}$[3]. Thus, $p(x)$ is irredcible over $\mathbb{Q}$ by Gauss' Lemma, and so $p(x)$ is the minimal polynomial of α over $\mathbb{Q}$.

$(b) \implies (c)$:

$$\mathbb{Z}[\alpha] = \{f(x) : \ f(x) \in \mathbb{Z}[x]\}$$

Now, $\mathbb{Z}[\alpha]$ is generated by $\{1, \alpha, \cdots, \alpha^{n-1}\}$, where $deg_{\mathbb{Q}}\alpha = n$. Let $f(x)$ be the polynomial of α. Then:

$$0 = f(\alpha) = \sum_{i=0}^{n} a_i \alpha^i$$
$$\implies \alpha^n \in \text{Span}(\{1, \alpha, \cdots, \alpha^{n-1}\})$$

By induction, $\alpha^N \in \text{Span}(\{1, \alpha, \cdots, \alpha^{n-1}\})$, for every $N \geq n$. So $\mathbb{Z}[\alpha] \subseteq \text{Span}_{\mathbb{Z}})\{1, \alpha, \cdots, \alpha^{n-1}\})$. The reverse inclusion is obviously true, so we get equality, and thus we have as desired that $\mathbb{Z}[\alpha]$ is a finitely generated $\mathbb{Z}$-module.

$(c) \implies (d)$:

Let $M = \mathbb{Z}[\alpha]$. Then, trivially, $\alpha M \subseteq M$.

$(d) \implies (a)$:

Let M be a finitely generated $\mathbb{Z}$-submodule of $\mathbb{C}$ such that $\alpha M \subseteq M$. Let:

$$M = \mathbb{Z}x_1 + \mathbb{Z}x_2 + \cdots + \mathbb{Z}x_n$$

In other words, the $x_1, \cdots x_n$'s are the generators. Each $x_i \in M$, so $\alpha x_i \in M$ by (c). Now, let:

$$\alpha x_i = \sum_{j=1}^{n} c_y x_j$$

for $1 \leq j \leq n$, $C_y \in \mathbb{Z}$. Let $C = (C_y)$ as an $n \times n$ matrix. So:

$$(C - \alpha I) \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix} = 0$$
$$\implies \det(C - \alpha I) = 0$$

[3]If not, there exists a lower degree polynomial of which α is a root, thus providing a contradiction

The above follows because the vector $(x_1, \cdots, x_n)^t op$ is non-zero. Now, let $f(x) = (-1)^n \det(C - \lambda I)$. We then get that $f(\alpha) = 0$. Also, $f(x)$ is monic in $\mathbb{Z}[x]$ because $c_{ij} \in \mathbb{Z}$. Thus, α is an algebraic integer. □

Proposition 1.5.1. *$\mathcal{O}$ is a ring.*

Proof. Let α, β be algebraic integers of degrees n and m. We want to show that $\alpha \pm \beta$ and $\alpha\beta$ are also algebraic integers, essentially amounting to the Subring Test.

So, $1, \alpha, \cdots, \alpha^{n-1}$ generate $\mathbb{Z}[\alpha]$ and $1, \beta, \cdots, \beta^{n-1}$ generate $\mathbb{Z}[\beta]$ as $\mathbb{Z}$-modules. Then, $\alpha^i \beta^j$ span $\mathbb{Z}[\alpha, \beta]$, for $1 \leq i \leq n$, $1 \leq j \leq m$. Thus, $M = \mathbb{Z}[\alpha, \beta]$ is a finitely generated submodule of $\mathbb{C}$, non-zero , and noting that $(\alpha \pm \beta)M \subseteq M$, and $\alpha\beta M \subseteq M$, and thus $\alpha \pm \beta$ and $\alpha\beta$ are algebraic integers. □

Definition 1.5.2. *Let K be an algebraic number field. Then define $\mathcal{O}_K = \mathcal{O} \cap K$ to be the set of all algebraic integers in K.*

Corollary 1.5.1. *$\mathcal{O}_K$ is a ring.*

Proof. This is the intersection of two rings. □

We have seen that $\mathcal{O}_{\mathbb{Q}} = \mathbb{Z}$. Also, $\mathcal{O}_{\mathbb{Q}(i)} = \mathbb{Z}[i]$.

1.6 Discriminants

Definition 1.6.1. *Let K be an algebraic number field of degree n. Let $\omega_1, \omega_2, \cdots, \omega_n \in K$. Let σ_i for $1 \leq i \leq n$ denote the n distinct embeddings of K. For $j = 1, \cdots, n$, let:*

$$\omega_j^{(i)} = \sigma_i(\omega_j)$$

Then, the discriminant of $\omega_1, \cdots, \omega_n$ is denoted $D(\omega_1, \cdots, \omega_n)$ (or sometimes $\Delta(\omega_1, \cdots, \omega_n)$), and is computed as:

$$D(\omega_1, \cdots, \omega_n) = (det(\sigma_i(\omega_j))_{ij})^2$$

Let $\alpha_1, \cdots, \alpha_n$ and $\beta_1, \cdots, \beta_n$ be two bases for K. Let:

$$\beta_j = \sum_{i=1}^{n} c_{ij}\alpha_i$$

for some $c_{ij} \in \mathbb{Q}$. Let $C = (c_{ij})_{ij}$, for $1 \leq i, j \leq n$. Consider:

$$\begin{aligned}(\sigma_i(\beta_j))_{ij} &= (\sigma_i \left(\sum_{k=1}^{n} c_{kj}\alpha_k \right))_{ij} \\ &= \left(\sum_{k=1}^{n} c_{kj}\sigma_i(\alpha_k) \right)_{ij} \\ &= \left(\sum_{k=1}^{n} \sigma_i(\alpha_k)c_{kj} \right)_{ij} \\ &= (\sigma_i(\alpha_j))_{ij}C\end{aligned}$$

$$\begin{aligned}D(\beta_1, \cdots, \beta_n) &= (\det(\sigma_i(\beta_j)_{ij}))^2 \\ &= (\det(\sigma_i(\alpha_j)_{ij}))^2(\det C)^2 \\ &= D(\alpha_1, \cdots, \alpha_n)(\det C)^2\end{aligned}$$

We define, for $\alpha \in K$:

$$D(\alpha) = D(1, \alpha, \cdots, \alpha^{n-1})$$

So:

$$D(\alpha) = \underbrace{\left[\prod_{1 \leq i \leq j \leq n} (\alpha^j - \alpha^i) \right]^2}_{\text{Vandermonde Determinant}}$$

Example 1.6.1. *Suppose $K = \mathbb{Q}(\sqrt{d})$, where d is square-free. The minimum polynomial of $\sqrt{d}$ over $\mathbb{Q}$ is:*

$$p(x) = x^2 - d = (x - \sqrt{d})(x + \sqrt{d})$$

Considering the embedding $\sigma_1 : Id$, $\sigma_2 : \sqrt{d} \mapsto -\sqrt{d}$, we get:

$$D(\sqrt{d}) = D(1, \sqrt{d}) = \begin{vmatrix} 1 & \sqrt{d} \\ 1 & -\sqrt{d} \end{vmatrix}^2 = (-\sqrt{d} - \sqrt{d})^2 = 4d$$

Also, $n = 2$, so:

$$D(\alpha) = \prod_{1 \leq i \leq j \leq n} (\alpha^j - \alpha_i)^2 = (-\sqrt{d} - \sqrt{d})^2 = 4d$$

Example 1.6.2. *Let $K = \mathbb{Q}\sqrt[3]{2}$. We get a minimum polynomial using the primitive cube roots of unity where $w = -\frac{1}{2} + \frac{\sqrt{3}}{2}i$.*

$$\begin{aligned} D(\alpha) &= \prod_{1 \le i \le j \le n} (\alpha^j - \alpha^i)^2 \\ &= [(w^2\sqrt[3]{2} - w\sqrt[3]{2})(w^2\sqrt[3]{2} - \sqrt[3]{2})(w\sqrt[3]{2} - \sqrt[3]{2})]^2 \\ &= -108 \end{aligned}$$

Note that $D(w_1, \cdots, w_n) = (\det((\omega_j^{(i)})_{ij}))^2$ is a symmetric function of the w's.

Theorem 1.6.1. *Let K be an algebraic number field, and $w_i \in K$.*

(a) $D(w_1, \cdots, w_n) \in \mathbb{Q}$.

(b) If $w_1, \cdots, w_n \in \mathcal{O}_K$, then $D(w_1, \cdots, w_n) \in \mathbb{Z}$

(c) $D(w_1, \cdots, w_n) \neq 0$ if and only if $w_1, \cdots, w_n$ are linearly independent.

Proof. **(a):**

$K = \mathbb{Q}(\theta)$ for some algebraic number θ. So a basis for K is $1, \theta, \cdots, \theta^{n-1}$ where $\deg_{\mathbb{Q}} K = n$. So:

$$w_j = c_{0j} + c_{1j}\theta + \cdots + c_{n-1,j}\theta^{n-1}$$

$$\begin{aligned} D(w_1, \cdots, w_n) &= (\det((w_k^{(i)})_{ij}))^2 \\ &= (\det\left(\sum_{t=0}^{n-1} c_{ij}\theta^t\right))^2 \end{aligned}$$

This is symmetric in $\theta_1, \theta_2, \cdots, \theta_n$. Since permuting θ's just permutes the rows of the matrix, let:

$$f(x_0, \cdots, x_{n-1}) = (\det\left(\sum_{t=0}^{n-1} c_{ij}x^t\right))^2 \in \mathbb{Q}[x_0, \cdots, x_{n-1}]$$

By Proposition 3, we get that $D(w_1, \cdots, w_n) = f(\theta_1, \cdots, \theta_n) \in \mathbb{Q}$.

(b):

By part (a), $D(w_1, \cdots, w_n) \in \mathbb{Q}$, but if $w_1, \cdots, w_n \in \mathcal{O}$, then we have by definition that $D(w_1, \cdots, w_n) \in \mathcal{O}$, since $\mathcal{O}$ is a ring. Thus, $D(w_1, \cdots, w_n) = \mathbb{Q} \cap \mathcal{O} = \mathbb{Z}$

(c):

For the forward direction, we prove this by the contrapositive. In other words, if $w_1, \cdots, w_n$ are not linearly independent, then $D(w_1, \cdots, w_n) = 0$. Let $w_1, \cdots, w_n$ be linearly dependent. Then, $\exists c_1, \cdots, c_n$ not all zero, from $\mathbb{Q}$ such that $\sum_{i=1}^{n} c_i w_i = 0$. Applying the embeddings of K, we get:

$$c_i w_i^{(i)} + c_2 w_2^{(i)} + \cdots + c_n w_n^{(i)} = 0$$

We know the induced matrix has a non-zero solution for $\vec{c} - (c_1, \cdots, c_n)^\top$ in $\mathbb{Z}$. Thus, the induced matrix is NOT invertible, so its determinant is 0. Thus, $D(w_1, \cdots, w_n) = 0^2 = 0$, so we have the proof of the forward direction by the contrapositive.

Now, for the converse, let $w_1, \cdots, w_n$ be linearly independent. Then, these form a basis for K over $\mathbb{Q}$. Let $K = \mathbb{Q}(\theta)$. Then, $1, \theta, \cdots, \theta^{n-1}$ is also a basis for K. Thus, there exists a change of basis matrix $C \neq 0$ such that:

$$D(1, \theta, \cdots, \theta^{n-1}) = (\det(C))^2 D(w_1, \cdots, w_n)$$

However, we are more familiar with the left side by the Vandermonde Determinant, where:

$$D(1, \theta, \cdots, \theta^{n-1}) = \prod_{1 \leq i \leq j \leq n} (\theta^{(j)} - \theta^{(i)})^2$$

Here, $\theta^{(i)} = \sigma_u(\theta)$ is the i^{th} conjugate of θ, and all the conjugates are distinct. Thus, we get that this discriminant is nonzero. Thus, $D(w_1, \cdots, w_n) \neq 0$ $\square$

2 Integral Bases

2.1 Introduction

Definition 2.1.1. *Let K be an algebraic number field. A $\mathbb{Z}$-basis for $\mathcal{O}_K$ is called an integral basis for K (but really for $\mathcal{O}_K$.*

Proposition 2.1.1. *Every $\mathbb{Z}$-basis for $\mathcal{O}_K$ is a $\mathbb{Q}$ basis for K.*

Proof. Let $w_1, \cdots w_t$ be a $\mathbb{Z}$ basis for $\mathcal{O}_K$. Let $\theta \in K$ be an algebraic number. Then, $\theta = \frac{\alpha}{m}$, where $\alpha \in \mathcal{O}_K$ is an algebraic integer, and $m \in \mathbb{Z}$. This implies that, uniquely, $\alpha = \sum_{i=1}^{t} c_i w_i$, for $c_i \in \mathbb{Z}$. Then, $\theta \in Spqn_{\mathbb{Q}}(w_1, \cdots, w_t) \implies K \subseteq Span_{\mathbb{Q}}(w_1, \cdots, w_t) \implies Span_{\mathbb{Q}}(w_1, \cdots, w_t) = K$. Suppose $w_1, \cdots, w_t$ was linearly dependent over $\mathbb{Q}$. Then, there exists $q_1, \cdots, q_t$ not all zero such that the finite linear combination sums to 0. Then, we can multiply by $n \in \mathbb{Z}$ to get this linear combination to sum to 0, which then, by the linear independence over $\mathbb{Z}$, gives rise to an obvious contradiction which then shows us that $w_1, \cdots, w_t$ is linearly independent over $\mathbb{Q}$, and so must be a $\mathbb{Q}$ basis for K. Combined with a counting argument where the sizes of these two bases are the same, we get our desired result. □

Note: Not all bases of K will be integral bases.

Example 2.1.1. *$K = \mathbb{Q}(\sqrt{5})$ has a basis $1, \sqrt{5}$. The minimum polynomial is $x^2 - 5$ which has degree 2. However, the above basis is NOT an integral basis. $\frac{1+\sqrt{5}}{2} \in \mathcal{O}_K$ has minimum polynomial $x^2 - x - 1 \in \mathbb{Z}[x]$, but this is NOT in the span of the basis over $\mathbb{Z}$. However, $\{1, \frac{1+\sqrt{5}}{2}\}$ is an integral basis, where $\mathcal{O}_K = \mathbb{Z}\left[\frac{1+\sqrt{5}}{2}\right]$.*

In general, if $K = \mathbb{Q}(\alpha)$, a basis $\{1, \alpha, \cdots, \alpha^{n-1}\}$ is not necessarily an integral basis. $\mathbb{Z}[\alpha] \subseteq \mathcal{O}_K$, but $\mathcal{O}_K \not\subseteq \mathbb{Z}[x]$ in general.

Theorem 2.1.1. *Every number field K has an integral basis.*

Proof. Let $K = \mathbb{Q}(\alpha)$, where α is an algebraic integer. $\{1, \alpha, \cdots, \alpha^{n-1}\}$ is a basis for $K/\mathbb{Q}$, $deg_{\mathbb{Q}} K = n$. Now, $D(\alpha) > 0 \in \mathbb{Z}$, because $\{1, \alpha, \cdots, \alpha^{n-1}\}$ is a linearly independent set in $\mathcal{O}_K$. Now, we select a basis $\{w_1, \cdots, w_n\}$ of K from $\mathcal{O}_K$, such that $D(w_1, \cdots, w_n)$ is minimal. We'll now show that this is an integral basis.

Suppose otherwise. There then exists $w \in \mathcal{O}_K$ such that $w = \sum_{i=1}^{n} a_i w_i$ such that $a_i \in \mathbb{Q}$ and there is at least one $a_i \in \mathbb{Q} \setminus \mathbb{Z}$. Without loss of generality, assume $a_1 \in \mathbb{Q} \setminus \mathbb{Z}$. We write $a_1 = a + r$, where $a \in \mathbb{Z}$ and $r \in \mathbb{Q} \setminus \mathbb{Z}$, $0 < r < 1$. Define $\phi_1 = w - a w_1$, $\phi_i = w_i$ otherwise. Then, by construction, $\{\phi_1, \phi_2, \cdots, \phi_n\}$ is also a $\mathbb{Q}$-basis for K,where $\phi_i \in \mathcal{O}_K$. Now, we consider a change of basis matrix C such that $\Phi = CW$. Then:

$$C = \begin{vmatrix} a_1 - a & a_2 & a_3 & \cdots & a_n \\ 0 & 1 & 0 & \cdots & 0 \\ 0 & 0 & 1 & \cdots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & 0 & \cdots & 1 \end{vmatrix}$$

Thus, $\det(C) = a_1 - a = r$, and $D(\phi) = r^2 D(w)$, where $0 < r < 1$, but this leads to a contradiction, as this gives $D(\phi) < D(w)$, a contradiction to $D(w)$ being minimal. □

Theorem 2.1.2. *Let $\alpha_1, \cdots, \alpha_n$ be a basis for K over $\mathbb{Q}$. If $D(\alpha_1, \cdots, \alpha_n)$ is square free, then $\{\alpha_1, \cdots, \alpha_n\}$ is an integral basis.*

Proof. Let $\beta_1, \cdots \beta_n$ be an integral basis for K. Then there exist $c_{ij} \in \mathbb{Z}$ such that $\alpha_i = \sum_{j=1}^{n} c_{ij}\beta_j$ for all $1 \leq\leq n$ because $\alpha_i \in \mathcal{O}_K$. Now, Let $C = (c_{ij})$. So:

$$\underbrace{D(\alpha_1, \cdots, \alpha_n)}_{\in\mathcal{N}} = \underbrace{(\det(C))^2}_{\in\mathbb{Z}} \underbrace{D(\beta_1, \cdots, \beta_n)}_{\in\mathbb{Z}}$$

We note that since the left side is square free, $\det(C) = \pm 1$, so C is invertible over $\mathbb{Z}$. This in turn implies that C is an integral change of basis matrix. □

Remark 2.1.1. *The converse is false.*

Example 2.1.2. *If $K = \mathbb{Q}(i)$, then $\mathcal{O}_K = \mathbb{Z}[i]$. We have a basis $\{1, i\}$ with nontrivial embedding $i \mapsto -i$, and minimal polynomial $x^2 + 1 = (x - i)(x - (-i))$. $D(1, i) = 4$ is not square free, but $\{1, i\}$ is an integral basis.*

Remark 2.1.2. *For two integral bases $\{\alpha_1, \cdots, \alpha_n\}$ and $\{\beta_1, \cdots, \beta_n\}$, we always get that their discriminants are the same. In other words, the discriminant of an integral basis is independent of choice of basis.*

Definition 2.1.2. *The discriminant of K, denoted D_K, Δ_K is exactly the discriminant mentioned in Remark 2.*

Example 2.1.3. *$K = \mathbb{Q}(\sqrt{5})$ has basis $\{1, \sqrt{5}\}$, but we saw that this is not an integral basis in Example 9. So what IS an integral basis here? We have from Example 9, without proof, that $\left\{1, \frac{1+\sqrt{5}}{2}\right\}$ is an integral basis.*

$$D\left(1, \frac{1+\sqrt{5}}{2}\right) = \begin{vmatrix} 1 & \frac{1+\sqrt{5}}{2} \\ 1 & \frac{1-\sqrt{5}}{2} \end{vmatrix}^2$$
$$= \left(\frac{1-\sqrt{5}}{2} - \frac{1+\sqrt{5}}{2}\right)^2 = 5$$

5 is square free, so this is an integral basis.

Definition 2.1.3. *Let K be a number field with $\mathbb{Q}$ basis $\{w_1, \cdots, w_n\}$. Let $\alpha \in K$ and let $\alpha w_i = \sum_{j=1}^{n} a_{ij} w_j$, for all $1 \leq i \leq n$, and $a_{ij} \in \mathbb{Q}$. Let $A = (a_{ij})$ be an $n \times n$ matrix. We define the trace of α, $Tr_K(\alpha)$ such that $Tr_K(\alpha) = Tr(A)$, and the norm of α, $N_K(\alpha)$ as $N_K(\alpha) = det(A)$.*

Example 2.1.4. *Consider $K = \mathbb{Q}(\sqrt{d})$, where d is square-free integer. This has a basis $\{1, \sqrt{d}\}$. Let $\alpha = a + b\sqrt{d}$, $a, b \in \mathbb{Q}$.*

$$\alpha w_1 = (a + b\sqrt{d}) = a \cdot 1 + b \cdot \sqrt{d}$$
$$\alpha w_2 = (a + b\sqrt{d})(\sqrt{d}) = (bd) \cdot 1 + a \cdot \sqrt{d}$$

So:

$$A_\alpha = \begin{pmatrix} a & b \\ bd & a \end{pmatrix}$$

This gives us that $Tr(\alpha) = 2a$, $N(\alpha) = a^2 - db^2$.

Lemma 2.1.1. *Let K be a number field, If $\alpha \in \mathcal{O}_K$, then $Tr_K(\alpha), N_K(\alpha) \in \mathbb{Z}$*

Proof. Let $w_1, \cdots, w_n$ be a basis $\mathbb{Q}$-basis for K. Let $\alpha w_i = \sum_{j=1}^{n} a_{ij} w_j$, for every $1 \leq i \leq n$, $a_{ij} \in \mathbb{Q}$. Then, let $A = (a_{ij})$.

Let $\sigma_1, \cdots, \sigma_n$ be the embeddings of K. Take σ_k of αw_i.

$$\sigma_k(\alpha w_i) = \sigma_k\left(\sum_{j=1}^{n} a_{ij} w_j\right)$$
$$\implies \sigma_k(\alpha)\sigma_k(w_i) = \sum_{j=1}^{n} a_{ij}\sigma_k(w_j)$$
$$\implies \sum_{j=1}^{n} \delta_{jk}\sigma_j(\alpha)\sigma_j(w_i) = \sum_{j=1}^{n} a_{ij}\sigma_k(w_j)$$

Now, define:

$$A_0 = (\delta_{ij}\sigma_i(\alpha))_{ij}$$
$$M = (\sigma_j(w_i))_{ij}$$

We note that $0 \neq D(w_1, \cdots, w_n) = \det(M^T)^2 = \det(M)^2 \implies M$ is invertible.

$$AM = \left(\sum_{k=1}^{n} a_{ik}\sigma_j(w_k)\right)_{ij}$$
$$MA_0 = \left(\sum_{k=1}^{n} \sigma_k(w_i)\delta_{jk}\sigma_k(\alpha)\right)_{ij}$$

Thus, by the above, we get that $AM = MA_0 \implies A_0 = M^{-1}AM \implies \det A_0 = \det A$ (and their traces are equal). Thus, the trace is the sum of the $\sigma_i(\alpha)'s$ and the norm ia the product. This gives us that the trace and norm of α are independent of choice of basis. □

Proposition 2.1.2. *Let $K = \mathbb{Q}(\alpha)$, $\alpha \in \mathcal{O}$. Let $p(x)$ be the minimum polynomial of α of degree n. Then, $D(\alpha) = (-1)^{\binom{n}{2}} N_K(p'(\alpha))$*

Proof. By the Vandermonde Determinant, $D(\alpha) = \prod_{1 \le i \le j \le n} (\alpha^{(j)} - \alpha^{(i)})^2$. On the left, we have:

$$p(x) = \prod_{i=1}^{n} (x - \sigma_i(\alpha))$$

$$p'(x) = \sum_{j=1}^{n} \prod_{i \neq j} (x - \sigma_i(\alpha)) = \sum_{j=1}^{n} \prod_{i \neq j} (x - \alpha^{(i)})$$

$$\implies p'(\alpha^{(k)}) = \sum_{j=1}^{n} \prod_{i \neq j} (\alpha^{(k)} - \alpha^{(i)}) = \prod_{i \neq k} (\alpha^{(k)} - \alpha^{(i)})$$

$$\begin{aligned} N(p'(\alpha)) &= \prod_{j=1}^{n} \sigma_j(p'(\alpha)) \\ &= \prod_{j=1}^{n} p'(\alpha^{(j)}) \\ &= \prod_{j=1}^{n} \prod_{i \neq j} (\alpha^{(j)} - \alpha^{(i)}) \\ &= \prod_{1 \le i < j \le n} (-1)^s (\alpha^{(j)} - \alpha^{(i)})^2 \\ &= (-1)^s D(\alpha) \qquad s = \binom{n}{2} \end{aligned}$$

□

Proposition 2.1.3. *If $\{\alpha_1, \cdots, \alpha_n\}$ is a basis for K over $\mathbb{Q}$, where K is a number field, then:*

$$D(\alpha_1, \cdots, \alpha_n) = det[(Tr_K(\alpha_i \alpha_j))_{ij}] \in M_n(\mathbb{Q})$$

Proof.

$$Tr_K(\alpha) = \sum_{k=1}^{n} \sigma_k(\alpha)$$

Thus,

$$Tr(\alpha_i \alpha_j) = \sum_{k=1}^{n} \sigma_k(\alpha_i \alpha_j) = \sum_{k=1}^{n} \sigma_k(\alpha_i) \sigma_k(\alpha_j)$$

Then, constructing our matrix of traces, we get that:

$$(Tr(\alpha_i \alpha_j))_{ij} = ((\sigma_j(\alpha_i))_{ij} (\sigma_i(\alpha_j)_{ij}))_{ij}$$

$$\det((Tr(\alpha_i \alpha_j)_{ij})) = \det(\sigma_i(\alpha_j)_{ij})^2 = D(\alpha_1, \cdots, \alpha_n)$$

□

2.2 Quadratic Fields

Definition 2.2.1. *A quadratic field is an algebraic number field K of degree 2 over $\mathbb{Q}$.*

Proposition 2.2.1. *All quadratic fields are of the form $\mathbb{Q}(\sqrt{d})$ for some square-free $d \in \mathbb{Z}$.*

Proof. Let $K = \mathbb{Q}(\alpha)$. for some $\alpha \in \mathcal{O}$. Since K is a quadratic field, the minimum polynomial of α is of the form $p(x) = x^2 + ax + b$, where $a, b \in \mathbb{Z}$. This gives us that:

$$\alpha = \frac{-a \pm \sqrt{a^2 - 4b}}{2}$$

Now, we write: $a^2 - 4b = r^2 d$, where d is square free. Then,

$$\alpha = \frac{-a \pm r\sqrt{d}}{2}$$

Thus, $\mathbb{Q}(\alpha) = \mathbb{Q}\left(\frac{-a \pm r\sqrt{d}}{2}\right) = \mathbb{Q}(\sqrt{d})$. □

Remark 2.2.1. *If $d < 0$, $\mathbb{Q}(\sqrt{d})$ is called an imaginary quadratic field. If $d > 0$, this is instead called a real quadratic field.*

Theorem 2.2.1. *Let $d \in \mathbb{Z}$ be square-free, and $K = \mathbb{Q}(\sqrt{d})$. Then:*

$$\mathcal{O}_K = \begin{cases} \mathbb{Z}[\sqrt{d}], & d \not\equiv 1 \pmod 4 \\ \mathbb{Z}\left[\frac{1+\sqrt{d}}{2}\right], & d \equiv 1 \pmod 4 \end{cases}$$

Proof. Note that $\mathbb{Z}[\sqrt{d}] \subseteq \mathbb{Z}\left[\frac{1+\sqrt{d}}{2}\right]$.

$$\mathbb{Z}[\sqrt{d}] = \{a + b\sqrt{d} : \ a, b \in \mathbb{Z}\}$$

Consider $p(x) = x^2 - 2dx + (a^2 - db^2)$. Then, $\alpha = a + b\sqrt{d}$ is a root of $p(x)$. So, $\mathbb{Z}[\sqrt{d}] \subseteq \mathcal{O}_K$.

$$\begin{aligned} \mathbb{Z}\left[\frac{1+\sqrt{d}}{2}\right] &= \left\{a + b\left(\frac{1+\sqrt{d}}{2}\right) : \ a, b \in \mathbb{Z}\right\} \\ &= \{a + \frac{b}{2} + \frac{b}{2}\sqrt{d} : \ a, b \in \mathbb{Z}\} \\ &= \left\{\frac{2a+b}{2} + \frac{b}{2}\sqrt{d} : \ a, b \in \mathbb{Z}\right\} \\ &= \left\{\frac{m}{2} + \frac{n}{2}\sqrt{d} : \ m, n \in \mathbb{Z} \wedge m \equiv n \pmod 2\right\} \\ &= \mathbb{Z}[\sqrt{d}] + \{\frac{m}{2} + \frac{n}{2}\sqrt{d}\} \end{aligned}$$

If $\alpha = \frac{m}{2} + \frac{n}{2}\sqrt{d}$, where m and n are both odd, and $f(x) = x^2 - mx - \frac{m^2 - dn^2}{4} \in \mathbb{Q}[x]$, then $f(\alpha) = 0$. Then, $m^2 \equiv n^2 \equiv 1 \pmod 4$. If $d \equiv 1 \pmod 4$, then $\frac{m^2 - dn^2}{4} \in \mathbb{Z}$, and so $f(x) \in \mathbb{Z}[x]$, $\alpha \in \mathcal{O}_K$. Thus, if $d \equiv 1 \pmod 4$, $\mathbb{Z}\left[\frac{1+\sqrt{d}}{2}\right] \subseteq \mathcal{O}_K$.

Now, let $\alpha = r + s\sqrt{d} \in \mathcal{O}_K$, where $r, x \in \mathbb{Q}$. Consider $g(x) = x^2 - 2rx + (r^2 - ds^2)$, then $g(\alpha) = 0$. If $s = 0$, then $\alpha = r \in \mathcal{O}_K \implies r \in \mathbb{Z} \implies \alpha \in \mathbb{Z} \subseteq \mathbb{Z}\left[\frac{1+\sqrt{d}}{2}\right]$.

Now, assume $s \neq 0$. $g(x)$ is the minimum polynomial forα. This means that $g(x) \in \mathbb{Z}[x]$, and so $2r \in \mathbb{Z}$ and $r^2 - ds^2 \in \mathbb{Z}$.

If $2r$ is even, then $r \in \mathbb{Z}$. Then, $ds^2 \in \mathbb{Z}$. Let $s = \frac{a}{b}$ where $gcd(a, b) = 1$, $b \neq 0$. Then:

$$ds^{@} = \frac{da^2}{b^2} \implies b^2 | d \implies b = \pm 1 \implies d \text{ is square free} \implies s = \pm a \in \mathbb{Z}$$

Thus, $\alpha \in \mathbb{Z}[\sqrt{d}]$.

Now, iff $2r$ is odd, $r \in \frac{1}{2}\mathbb{Z}$. In other word, $r = \frac{m}{2}$ where m is odd. $r^2 - ds^2 \in \mathbb{Z} \implies 4r^2 - 4ds^2 \implies 4ds^2 \in \mathbb{Z} \implies d(2s)^2 \in \mathbb{Z}$. By the same trick as above, we get that $2s = a \in \mathbb{Z}$.

If $s \in \mathbb{Z}$, then $r^2 = (r^2 - ds^2) + ds^2 \in \mathbb{Z} \implies r \in \mathbb{Z}$, but this contradicts $2r$ being odd. Thus, $2s$ is odd.. So, $2r$ and $2s$ both being odd means:

$$(2r)^2 - d(2s)^2 - 4(r^2 - ds^2) \equiv 0 \pmod 4$$

This implies necessarily that $d \equiv 1 \pmod 4$. In this case, $r = \frac{m}{2}$ and $s = \frac{n}{2}$ where m, n are odd, so $\alpha \in \mathbb{Z}\left[\frac{1+\sqrt{d}}{2}\right]$, and $d \equiv 1 \pmod 4$ necessarily. If $d \not\equiv 1 \pmod 4$, then we MUST be in the first case, so we get the reverse inclusion, which now gives us the equality in the statement of this theorem. □

Corollary 2.2.1. *$\mathbb{Q}(\sqrt{d})$ has an integral basis of $\{1, \sqrt{d}\}$ when $d \not\equiv 1 \pmod 4$, and $\left\{1, \frac{1+\sqrt{d}}{2}\right\}$ otherwise.*

Corollary 2.2.2.

$$D(\mathbb{Q}(\sqrt{d})) = \begin{cases} 4d, & d \not\equiv 1 \pmod 4 \\ d, & d \equiv 1 \pmod 4 \end{cases}$$

Proof. If $d \not\equiv 1 \pmod 4$, then:

$$Disc = \begin{vmatrix} 1 & \sqrt{d} \\ 1 & -\sqrt{d} \end{vmatrix} = (-2\sqrt{d})^2 = 4d$$

If $d \equiv 1 \pmod 4$, then:

$$Disc = \begin{vmatrix} 1 & \frac{1+\sqrt{d}}{2} \\ 1 & -\frac{1+\sqrt{d}}{2} \end{vmatrix} = (-\sqrt{d})^2 = d$$

□

2.3 Cyclotomic Fields

Consider a poylnomial $f(x) = x^n - 1$. The (complex) zeroes of f are called the n^{th} roots of unity, denoted $\{1, \zeta_n, \zeta_n^2 \cdots, \zeta_n^{n-1}\}$, where:

$$\zeta_n = e^{\frac{2\pi i}{n}}$$

is a primitive n^{th} root of unity. If $gcd(m, n) = 1$, then $\langle \zeta_n \rangle = \langle \zeta_n^m \rangle$. Then, Euler's totient function is $\phi(n) = |S|$, where $S = \{\zeta_n^m : \ gcd(m, n) = 1, 1 \leq m \leq n\}$.

The splitting field of f is $\mathbb{Q}[1, \zeta_n, \zeta_n^2 \cdots, \zeta_n^{n-1}] = \mathbb{Q}(\zeta_n)$. This is called the n^{th} cyclotomic field, and $[\mathbb{Q}(\zeta_n) : \mathbb{Q}] = \phi(n)$.

Example 2.3.1. *Let $n = 6$. Then:*

$$\begin{aligned} x^6 - 1 &= (x^3 - 1)(x^3 + 1) \\ &= (x-1)(x^2 + x + 1)(x+1)(x^2 - x + 1) \\ &= (x-1)\underbrace{(x+1)}_{x-\zeta_6^3}\underbrace{(x^2 + x + 1)}_{(x\zeta_6^2)(x-\zeta_6^4)}\underbrace{(x^2 - x + 1)}_{(x-\zeta_6)(x-\zeta_6^5)} \end{aligned}$$

The minimum polynomial for ζ_6 is $x^2 - x + 1$ which has degree $2 = \phi(6)$, so $[\mathbb{Q}(\zeta_n) : \mathbb{Q}] = 6$. In general, the n^{th} cyclotomic polynomial is the monic polynomial whose roots are the primitive n^{th} of unity, denoted

$$\Phi(x) = \prod_{t=1}^{n}(x - \zeta_n^t)$$

This has degree $\phi(n)$. In general, $x^n - 1 = \prod_{d|n} \Phi_d(x)$.

Remark 2.3.1. *$\Phi_n(x) \in \mathbb{Z}[x] \implies \zeta_n$ is an algebraic integer.*

Note that if $K = \mathbb{Q}(\zeta_n)$, then $O_K = \mathbb{Z}[\zeta_n]$. So, $\{1, \zeta_n, \cdots, \zeta_n^{\phi(n)-1}\}$ is an integral basis. The discriminant is:

$$D(\mathbb{Q}(\zeta_n)) = (-1)^{\phi(n)/2}\frac{n^{\phi(n)}}{\prod_{p|n} p^{\frac{\phi(n)}{p-1}}}$$

Remark 2.3.2.

$$\phi(n) = 2 \iff n \in \{3, 4, 6\}$$

Thus:

$$\mathbb{Q}(\zeta_3) = \mathbb{Q}\left(-\frac{1}{2} + \frac{\sqrt{-3}}{2}\right) = \mathbb{Q}(\sqrt{-3})$$

$$\mathbb{Q}(\zeta_6) = \mathbb{Q}\left(-\frac{1}{2} + \frac{\sqrt{-3}}{2}\right) = \mathbb{Q}(\sqrt{-3})$$

$$\mathbb{Q}(\zeta_2) = \mathbb{Q}(i) = \mathbb{Q}(\sqrt{-1})$$

are the only cyclotomic fields which are quadratic fields. In general, if m is odd, then $\mathbb{Q}(\zeta_m) = \mathbb{Q}(\zeta_{2m})$ because $-\zeta_n$ is a primitive $2m^{th}$ root of unity.

Remark 2.3.3. *Recall that $x^p - 1 = (x-1)(\Phi_p(x)$. Then:*

$$N(\zeta_p^t) = (-1)^{p-1}a_0 = 1$$

$$Tr(\zeta_p^t) = -a_{p-2} = -1$$

3 Dedekind Domains

3.1 Introduction

Definition 3.1.1. *A ring R satisfies the ascending chain condition (ACC) if whenever $O_0 \subseteq I_1 \subseteq I_2 \subseteq \cdots$ for ideals $I_i \subseteq R$, there exists $m \in \mathbb{Z}_{\geq 0}$ such that $I_j = I_m$ for all $j \geq m$.*

Definition 3.1.2. *A ring R satisfies the maximal condition if every nonempty set of ideals of R contains an ideal that is not properly contained in anyh other ideal in the set. Note that this maximal element does not have to contain the other ideals.*

Definition 3.1.3. *An ideal I in a commutative ring R is finitely generated if there exists a finte set $\{x_1, \cdots, x_n\}$ such that for every $a \in I$, $a = \sum_{i=1}^{n} r - Ix_i$ for some $r_i \in R$.*

Proposition 3.1.1. *Let R be a commutative ring with unity. TFAE:*

(a) Every ideal of R is finitely generated

(b) R satisfies the ACC

(c) R satisfies the maximal condition.

Proof. $(a) \implies (b)$**:** Let $I_0 \subseteq I_1 \subseteq \cdots$ be an ascending chain of ideals in R. Let $I = \bigcup_{t=1}^{\infty} I_t$. Then, I is an ideal of R. This implies I is finitely generated. Let $I = \langle x_1 . \cdots, x_n \rangle$. $x_i \in I \implies x_i \in I_{j_i}$, for some $j_i \in \mathbb{Z}_{\geq 0}$ minimal. Let $m = \max_{1 \leq i \leq n} j_i$. Then, all $x_i \subseteq I_m \implies I \subseteq I_m$. Thus, R satisfies ACC.

$(b) \implies (c)$. Suppose R does not satisfy the maximal condition. Then, R has a nonempty subset S of ideals with the property that for every ideal $I \in S$, there exists an ideal $J_I \in S$ such that $I \subset J_I$. WE can create an infinite chain of ideals in this way, thus contradicting ACC. Thus, R has the maximal condition.

$(c) \implies (a)$. Assume R has the maximal condition. Let I be an ideal of R. Let S be the set of ideals contained in I which are finitely generated. $\langle 0 \rangle \in S$, so S is nonempty. Thus, by the maximal condition, S has a maximal element, J. If $J \neq I$, then there exists $x \in I \setminus J$. Then $J + (x)$ is finitely generated and $J + (x) \subseteq I$, so $J + (x) \in S$, so $J = I$ by contradiction. □

Definition 3.1.4. *A commutative ring with unity which satisfies any of these conditions is called a Noetherian ring*

Theorem 3.1.1. *Let R be a Noetherian Ring. Then every non-zero, non-unit element of R is the product of irreducible elements (not quite UFD, because this is not necessarily unique).*

Proof. Suppose not. Then, there exists a non-zero, non-unit which is not the product of irreducibles. Let A be the set of all such elements. THen, let $S := \{(a) : a \in A\}$. So, S is nonempty. R being Noetherian means it satisfies the maximal condition, and so S has a maximal element, which we now denote (x) for some $x \in A$. So x is non-zero, non-unit, and is not the product of irreducibles. Thus, x is not irreducible, so x is reducible. Thus, $x = yz$ where y, z are non-zero, nonunits. Thus:

$$y|x \wedge z|x \implies (x) \subset (y) \wedge (x) \subset (z)$$

However, since (x) was maximal, $y, z \notin A$, so y and z are the products of irreducibles, but $x = yz$ is then a product of irreducibles, thus giving a contradiction. □

Theorem 3.1.2. *Let K be an algebraic number field. Then, every non-zero ideal of $\mathcal{O}_K$ contains a non-zero rational integer.*

Proof. Let $I \subseteq \mathcal{O}_K$ be a non-zero ideal. Let $\alpha \in I$ with minimum polynomial $p(x) = x^n + \sum_{i=0}^{n-1} a_i x^i \in \mathbb{Z}[x]$. Note, $a_0 \neq 0$ because $p(x)$ is irreducible.

$$0 = p(\alpha) = \alpha^n + \sum_{i=0}^{n-1} a_i \alpha^i$$
$$\implies a_0 = -(\alpha^n + a_{n-1}\alpha^{n-1} + \cdots + a_1\alpha) \in I$$

Thus, the constant term a_0 is a non-zero rational integer in I. □

Theorem 3.1.3. *Let K be an algebraic number field with $[K : \mathbb{Q}] = n$. Let I be a non-zero ideal of $\mathcal{O}_K$. Then, there exist $x_1, \cdots, x_n \in I$ such that $D(x_1, x_2, \cdots, x_n) \neq 0$.*

Proof. Let $K = \mathbb{Q}(\alpha)$ for some $\alpha \in \mathcal{O}_K$. So, $D(\alpha) = D(1, \alpha, \cdots, \alpha^{n-1}) \neq 0 \in \mathbb{Z}$. By the previous theorem, there exists $c \in \mathbb{Z}$ as prescribed, so let $x_1 = c$, $x_2 = c\alpha$, $\cdots$, $x_n = c\alpha^{n-1}$. For every i, $x_i \in I$ since I is an ideal. Thus:

$$D(x_1, \cdots, x_n) = (c^n)^2 D(1, \alpha, \cdots, \alpha^{n-1})$$

Thus $D(x_1, \cdots, x_n) \neq 0 \in \mathbb{Z}$. □

Theorem 3.1.4. *Let K be an algebraic number field with $[K : \mathbb{Q}] = n$. Let I be a non zero ideal of $\mathcal{O}_K$. Then, $\exists x_1, \cdots, x_n \in I$ such that all $\alpha \in I$ can be expressed uniquely as, for some $\lambda_i \in \mathbb{Z}$:*

$$\alpha = \sum_{i=1}^{n} \lambda_i x_i$$

Proof. By the previous theorem, there exist $x_1, \cdots, x_n \in I$ such that $D(x_1, \cdots, x_n) \neq 0 \in \mathbb{Z}$. Let $S = \{|D(x_1, \cdots, x_n)| : x_1, \cdots, x_n \in I$ as above. Then, S is a nonempty set of positive integers so it has a least element. Let $w_1, \cdots, w_n \in I$ be such that $|D(w_1, \cdots, w_n)|$ is minimal in S.

$D(w_1, \cdots, w_n) \neq 0 \iff w_1, \cdots, w_n$ are linearly independent, which in turn implies $w_1, \cdots, w_n$ is a $\mathbb{Q}$ basis for K. Let $\alpha \in I$. Then α can be expressed uniquely as $\sum_{i=1}^{n} \lambda_i w_i$, where all $\lambda_i \in \mathbb{Q}$. If they are all in $\mathbb{Z}$, then the theorem is done. Now, assume not all $|lambda_i \in \mathbb{Z}$. WLOG, let $\lambda_1 \in \mathbb{Q} \setminus \mathbb{Z}$. Let $\lambda_1 = n_1 + r$ where $n_1 \in \mathbb{Z}$, $0 < r < 1 \in \mathbb{Q}$. Then, let:

$$\phi_1 = \alpha - n_1 w_1$$
$$\phi_2 = w_2 \cdots \phi_n = w_n$$

Now, $\{\phi_1, \cdots, \phi_n\}$ is also a basis for K. Consider a change of basis matrix C such that $\Phi = CW$. This gives a matrix where we replace the top row of the identity matrix with $\{r, \lambda_2, \lambda_3, \cdots, \lambda_n\}$. Thus:

$$D(\phi_1, \cdots, \phi_n) = (\det C)^2 D(w_1, \cdots w_n)$$

Since C is triangular, its determinant is r, and $0 < r^2 < 1$. We also note that $\phi_i \in I$ because $w_i \in I$, and so $|D(\phi_1, \cdots, \phi_n)| \in S$. Thus, $|D(\phi_1, \cdots, \phi_n)| < |D(w_1, \cdots, w_n)|$ which is a contradiction to the minimality of $D(w_1, \cdots, w_n)|$. Thus, all the $\lambda_i \in \mathbb{Z}$, so we are done. □

Theorem 3.1.5 (Alaca Williams, 6.5.2)**.** *Let K be an algebraic number field. $\mathcal{O}_K$ is Noetherian.*

Proof. By the previous theorem, all ideals of $\mathcal{O}_K$ are finitely generated. □

Corollary 3.1.1. *Every element of $\mathcal{O}_K$ is a product of irreducibles, not necessarily uniquely.*

Example 3.1.1. *Let $K = \mathbb{Q}(\sqrt{-6})$. $\mathcal{O}_K = \mathbb{Z}[\sqrt{-6}]$. But then $10 = 2 \cdot 5 = (2 + \sqrt{-6})(2 - \sqrt{-6})$, so $\mathbb{Z}[\sqrt{-6}]$ is not a UFD.*

Definition 3.1.5. *If $A \subseteq B$ where A and B are integral domains, then $b \in B$ is integral over A if there exists a monic $f(x) \in A[x]$ such that $f(b) = 0$.*

Definition 3.1.6. *An integral domain D is integrally closed if the only elements in the field of fractions of D which are integral over D are those in D itself.*

Example 3.1.2. *All UFDs are integrally closed. (D&F p693, Example 3)*

Example 3.1.3. *Every polynomial ring over a field is integrally closed.*

Definition 3.1.7. *An integral domain D that is not a field is a Dedekind domain if:*

1. *D is Noetherian*
2. *D is integrally closed*
3. *Every prime ideal is maximal*

Example 3.1.4. *$\mathcal{O}_K$, for an algebraic number field K is a Dedekind domain.*

Example 3.1.5. *Every PID is a Dedekind Domain.*

R Noetherian $\implies$ $R[x]$ is Noetherian, but R being Dedekind does NOT imply $R[x]$ is Dedekind

Example 3.1.6. *$\mathbb{Z}$ is a Dedekind domain, but $\mathbb{Z}[x]$ is not. It is, however, Noetherian and integrally closed. (2) is a prime ideal but not maxiaml ideal, because $(2) \subset (2, x) \subset \mathbb{Z}[x]$*

Let $K = \mathbb{Q}(\sqrt{d})$, where d is a square free integer. Recall that:

$$\mathcal{O}_K = \begin{cases} \mathbb{Z}(\sqrt{d}) & d \not\equiv 1 \pmod 4 \\ \mathbb{Z}\left(\frac{1+\sqrt{d}}{2}\right) & d \equiv 1 \pmod 4 \end{cases}$$

In the case where $d < 0$, $\mathcal{O}_K$ is a Euclidean domain if and only if $d \in \{-1, -2, -3, -7, -11\}$. The Euclidean "size" function in all these cases is the norm, where $N(a + b\sqrt{d}) = a^2 + db^2 \in \mathbb{Q}$. We call these cases "Norm Euclidean".

$\mathcal{O}_K$ is a PID if and only if $d \in \{-1, -2, -3, -7, -11, -19, -43, -67, -163\}$.

Theorem 3.1.6. *Let D be a Dedekind domain. D is a PID if and only if D is a UFD. $d > 0$ is an open problem. However, $\mathcal{O}_K$ is Norm Euclidean if and only if:*

$$d \in \{2, 3, 5, 6, 7, 11, 13, 17, 19, 21, 29, 37, 41, 57, 73\}$$

$\mathcal{O}_K$ being Euclidean is an open problem. However, here is an example

Example 3.1.7. *For $d = 69$, $\mathcal{O}_K = \mathbb{Z}\left[\frac{1+\sqrt{69}}{2}\right]$ is a Euclidean domain but not norm Euclidean.*

Example 3.1.8 (2014)**.** *For $d = 14$, $\mathcal{O}_K = \mathbb{Z}[\sqrt{14}]$ is a Euclidean domain but not norm Euclidean*

Conjecture 3.1.1. *There are infinitely many real quadratic fields where $\mathcal{O}_K$ is a PID.*

Theorem 3.1.7.

1. *$\mathcal{O}_K$ is an integral domain*
2. *$Q(\mathcal{O}_K) = k$, where Q represents the field of fractions*
3. *$\mathcal{O}_K$ is integrally closed.*

Proof. K is a field, and thus is an integral domain. $\mathcal{O}_K$ is a subring, and $1_{\mathcal{O}_K} = 1_K = 1$, so $\mathcal{O}_K$ is a sub-integral domain of K.

$$Q(\mathcal{O}_K) = \left\{ \frac{a}{b} : \ a, b \in \mathcal{O}_K, b \neq 0 \right\} \subseteq K$$

$a, b \in \mathcal{O}_K \subseteq K$, which is a field, o $\frac{a}{b} = ab^{-1} \in K$.

Let $k \in K$. Then, $k = \frac{\alpha}{m}$ for some $\alpha \in \mathcal{O}_K$, $m \in \mathbb{Z} \subseteq \mathcal{O}_K$. Thus, $k \in Q(\mathcal{O}_K)$, so $K \subseteq Q(\mathcal{O}_K) \implies K = Q(\mathcal{O}_K)$.

Recall Theorem 6. The same proof can be used to show that the following are equivalent:

1. β is integral over $\mathcal{O}_K$
2. $\mathcal{O}_K[\beta]$ is a finitely generated $\mathcal{O}_K$-module
3. There is a finitely generated non-zero$\mathcal{O}_K$-submodule M such that $\beta M \subseteq M$

Let $\eta \in K = Q(\mathcal{O}_K)$ which is integral over $\mathcal{O}_K$. We want to show that $\beta \in \mathcal{O}_K$. So by the 3rd equivalence above, there exists a finitely generated non-zero $\mathcal{O}_K$-submodule M_1. Let $\{u_1, \cdots, u_n\}$ be a basis for M_1, and $\{v_1, \cdots, v_n\}$ be an integral basis for K, so it is a basis for $\mathcal{O}_K$ as a $\mathbb{Z}$-module. Then, let:

$$M = \sum_{j=1}^{n} \sum_{i=1}^{n} \mathbb{Z} v_j u_i$$

Then M is a finitely generated non-zero $\mathbb{Z}$-module in $\mathbb{C}$, so $\beta M \subseteq M$. This implies that β is integral over $\mathbb{Z}$. □

Lemma 3.1.1. *Let K be a number field. Let I be a nonzero ideal of $\mathcal{O}_K$.*

1. $I \cap \mathbb{Z} \neq \{0\}$
2. $[\mathcal{O}_K : I] < \infty$

Proof. We already saw the first. $0 \neq \alpha \in I \subseteq \mathcal{O}_K$ with minimal polynomial $p(x)$ with a_0 being the constant term. Then, $a_0 \in I \cap \mathbb{Z}$ because $p(\alpha) = 0$.

Now for the second portion of the lemma, let $\{w_1, \cdots, w_n\}$ be an integral basis for K. Let $- \neq \alpha \in I$, with minimal polynomial as above. For any w_i:

$$a_0 w_i = -(\alpha^n + a_{n-1}\alpha^{n-1} + \cdots + a_1\alpha)w_i \in I$$

Thus, $(a_0) = a_0\mathcal{O}_K = a_0 w_1\mathbb{Z} + \cdots a_0 w_n\mathbb{Z} \subseteq I$. Consider the map:

$$\phi : \mathcal{O}_K \to (\mathbb{Z}/a_0\mathbb{Z})^{\times n}$$

$$\phi : \sum_{i=1}^{n} m_i w_i \mapsto (m_1 \pmod{a_0}, m_2 \pmod{a_0}, \cdots, m_n \pmod{a_0})$$

Note that $ker\ \phi = \{\alpha = \sum_{i=1}^{n} m_u w_i : \ a_0 | m_i\} = (a_0)$. Also, ϕ is surjective, so by the first isomorphism theorem:

$$\mathcal{O}_K/(a_0) \cong (\mathbb{Z}/a_0\mathbb{Z})^{\times n}$$
$$[\mathcal{O}_K : (a_0)] = a_0^n < \infty$$

Then, $[\mathcal{O}_K : a_0] = [\mathcal{O}_K : I][I : (a_0)] < \infty \implies [\mathcal{O}_K : I] < \infty$. □

Theorem 3.1.8. *Every prime ideal in $\mathcal{O}_K$ is maximal.*

Proof. Let I be a prime ideal in $\mathcal{O}_K$. By previous lemma, $[\mathcal{O}_K : I] < \infty$. Also, $\mathcal{O}_K/I$ is an integral domain, because I is prime. Thus, $\mathcal{O}_K/I$ is a finite integral domain so it is a field. Thus, I is maximal. □

We have now proven that $\mathcal{O}_K$ is a Dedekind Domain!

Remark 3.1.1. *Recall that multiplication of ideals I, J in general in a commutative ring with unity R is:*

$$IJ = \left\{ \sum_{t=1}^{n} i_t j_t : \ i_t \in I, j_t \in J, n \in \mathbb{Z}^+ \right\} \subseteq I \cap J$$

If $I + J = R$, then $IJ = I \cap J$. If I nad J are finitely generated, then IJ is finitely generated by all possible pairs of products.

Example 3.1.9. *Let $R = \mathbb{Z}[\sqrt{-1}]$. Let $I = \langle 2, \sqrt{-10} \rangle$, and $J = \langle 7, 2 + \sqrt{-10} \rangle$. Then:*

$$IJ = \langle 14, 2(2 + \sqrt{-10}), 7\sqrt{-10}, -10 + 2\sqrt{-10} \rangle$$

$$-10 + 2\sqrt{-10} = -14 + 2(2 + \sqrt{-10}) \implies IJ = \langle 14, 2(2 + \sqrt{-10}), 7\sqrt{-10} \rangle$$

$$14 = (2 + \sqrt{-10})(2 - \sqrt{-10})$$

$$7\sqrt{-10} = (5 + \sqrt{-10})(2 + \sqrt{-10})$$

Thus,

$$IJ = \langle 2 + \sqrt{-10} \rangle$$

Note that $\mathbb{Z}[\sqrt{-10}]$ is not a UFD:

$$(2 + \sqrt{-10})(2 - \sqrt{-10}) = 14 = 2 \cdot 7$$

However, the ideals representing the above are the same ideal, since the multiplication of ideals generated by a value is simply the ideal generated by the multiplication of their values. So, consider I, J as above and $K = \langle 7, 2 - \sqrt{-10} \rangle$.

$$IJ = \langle 2 + \sqrt{-10} \rangle$$

$$IK = \langle 2 - \sqrt{-10} \rangle$$

$$JK = \langle 7 \rangle$$

$$I^2 = \langle 2 \rangle$$

Thus, $(IJ)(IK) = I^2JK \implies I^2JK = I^2JK$, so we once again get the same result as above of these generating the same ideal, and so note that I, J, and K are prime ideals in $\mathcal{O}_K$.

3.2 Fractional Ideals

Definition 3.2.1. *We recall the definition of a module. Let R be a ring, and let M be a set. M is an R-module if:*

1. *$(M, +)$ is an abelian group*
2. *There exists a map $R \times M \to M$ such that:*
   - $(r + s)M = rm + sm$
   - $(rs)m = r(sm)$
   - $r(m + n) = rm + rn$
3. *If R has unity, then $1_r m = m$*

An R-submodule of an R-module M is a subgroup N of $(M, +)$ such that $rn \in N$ for all $r \in R$, $n \in N$.

Remark 3.2.1. *If I is an ideal of a ring R, then I is an R-submodule of R as a module over itself trivially. In particular, an ideal I of $\mathcal{O}_K$ is an $\mathcal{O}_K$-submodule of $\mathcal{O}_K$.*

Definition 3.2.2. *An $\mathcal{O}_K$-submodule J of K (considered as an $\mathcal{O}_K$-module) is called a fractional ideal of $\mathcal{O}_K$ if there exists a non-zero $c \in \mathcal{O}_K$ such that $cJ \subseteq \mathcal{O}_K$.*

So, in the above definition, we essentiall extend the definition of a submodule. THe first two bullet points represent what we get from J being an $\mathcal{O}_K$-submodule, and the final bullet point shows how we get the condition of being a fractional ideal:

- $(J, +) \leq (K, +)$
- $\forall r \in \mathcal{O}_K,\ rJ \subseteq J$
- $\exists 0 \neq c \in \mathcal{O}_K :\ cJ \subseteq \mathcal{O}_K$

Example 3.2.1. *Let $K = \mathbb{Q}$. $\mathcal{O}_K = \mathbb{Z}$. Then, consider $J = \{\frac{3n}{4} :\ n \in \mathbb{Z}\}$. $(J, +) \leq (\mathbb{Q}, +)$. Clearly, $mJ \subseteq J$ for all $m \in \mathbb{Z}$. Thus, J is a $\mathbb{Z}$-submodule of $\mathbb{Q}$. Now, there exists a non-zero $c = 4$ such that $4J = 3\mathbb{Z} \subseteq \mathbb{Z}$. Thus, J is a fractional ideal of $\mathbb{Z}$.*

Remark 3.2.2.

1. *Every ideal of $\mathcal{O}_K$ is also a fractional ideal, considering $c = 1$.*
2. *Let J be a fractional ideal with $cJ \subseteq \mathcal{O}_K$. cJ is then an ideal of $\mathcal{O}_K$.*

   Proof. Then, $a = cj_1$, $b = cj_2$. Thus:

   $$a - b = cj_1 - cj_2 = c(\underbrace{j_1 - j_2}_{\in J}) \in I$$

   Let $r \in \mathcal{O}_K$. Then, $rI = rcJ = crJ \subseteq cJ = I$. Thus, I is an ideal of $\mathcal{O}_K$. □

3. *Conversely, if I is an ideal of $\mathcal{O}_K$, then $c^{-1}I$ is a fractional ideal of $\mathcal{O}_K$ for every $0 \neq c \in \mathcal{O}_K$*

   Proof. Let $J = c^{-1}I$. Then, $cJ = I \subseteq \mathcal{O}_K$. I is a subring of $|air \subseteq K$. Then, $c^{-1}I$ is also a subring of K. For any $r \in \mathcal{O}_K$, $rJ = rc^{-1}I = c^{-1}rI \subseteq c^{-1}I = J$. Thus, J is a fractional ideal of $\mathcal{O}_K$. □

   Thus, all the fractional ideals of $\mathbb{Z}$ are $\frac{1}{c}(n)$ for any $n \in \mathbb{Z}$ and $0 \neq c \in \mathbb{Z}$. We can rewrite this as:

   $$\frac{1}{c}(n) = \frac{1}{c}n\mathbb{Z} = \frac{n}{c}\mathbb{Z} = r\mathbb{Z}\ (r \in \mathbb{Q}^\times) - r\mathcal{O}_K\ (r \in K^\times)$$

4. *If $\mathcal{O}_K$ is a PID, then the fractional ideals are also principal.*

Proof. Let (d) be an ideal of $|air$. Then, $c^{-1}(d)$ is a fractional ideal for any $0 \neq c \in \mathcal{O}_K$.

$$c^{-1}(d) = c^{-1}d\mathcal{O}_K = \frac{d}{c}\mathcal{O}_K = \boxed{r\mathcal{O}_K} = (r) = \left(\frac{d}{c}\right)$$

□

Ideals of $\mathcal{O}_K$ are in a relationship with fractional ideals of $\mathcal{O}_K$ by $I \to c^{-1}I = J$ for any $0 \neq c \in \mathcal{O}_K$. Conversely, $cJ \leftarrow J$, where this is the particular c from the definition of being a fractional ideal. This c need not be unique. We can multiply fractional ideals in the same way that we multiply ideals themselves. If J_1, J_2 are fractional ideals, then $J_1J_2 = \left\{ \sum_{\text{finite sums}} j_1j_2 : \ j_1 \in J_1, j_2 \in J_2 \right\}$

Lemma 3.2.1. *Let J_1 and J_2 be fractional ideals of $\mathcal{O}_K$.*

1. *J_1 is a finitely generated $\mathcal{O}_K$-module.*
2. *J_1J_2 is a fractional ideal.*

Proof.
1. Let $0 \neq c \in \mathcal{O}_K$ such that $cJ_1 \subseteq \mathcal{O}_K$. We have also seen that cJ_1 is an ideal of $\mathcal{O}_K$. $\mathcal{O}_K$ is Noetherian, so all ideals are finitely generated. Now, let $cJ_1 = (a_1, \cdots, a_n)$. Then J_1 is generated by $c^{-1}a_1, c^{-1}a_2, \cdots, c^{-1}a_n$.
2. Let $0 \neq c, d \in \mathcal{O}_K$ such that $cJ_1 \subseteq \mathcal{O}_K$ and $dJ_2 \subseteq \mathcal{O}_K$. So cJ_1 and dJ_2 are ideals of $\mathcal{O}_K$, and $(cJ_1)(dJ_2) = (cd)(J_1J_2) \subseteq \mathcal{O}_K$. Multiplication of ideals is an ideal, so $I = (cd)J_1J_2$ is an ideal of $\mathcal{O}_K$, and thus $J_1J_2 = d^{-1}c^{-1}I$ is a fractional ideal.

□

Remark 3.2.3. *Multiplication of fractional ideals in $\mathcal{O}_K$ is commutative.*

Definition 3.2.3. *A nontrivial proper ideal P of a commutative ring R is a prime ideal if:*

$$ab \in P \implies a \in P \vee b \in P$$

Equivalently, a non-trivial proper idea P of a commutative ring R is a prime idealif, for any ideals A, B of R:

$$AB \subseteq P \implies A \subseteq P \vee B \subseteq P$$

Proof. We now prove the equivalence of the above definitions. First, assume that $ab \in P \implies a \in P \vee b \in P$. Let $AB \subseteq P$ and $A \nsubseteq P$. Let $b \in B$. Then, $Ab \subseteq AB \subseteq P$. This then means that $ab \subseteq P$, for all $a \in A$, which in turn implies by assumption that $a \in P$ for all $a \in A$, or $b \in P$. This then implies that $b \in P$, which in turn gives $B \subseteq P$.

Conversely, assume that $AB \subseteq P \implies A \subseteq P \vee B \subseteq P$. Let $ab \in P$. Then, $(a)(b) = (ab) \subseteq P$, so $(a) \subseteq P$ or $(b) \subseteq P$, and in turn, $a \in P$ or $b \in P$ as desired □

Theorem 3.2.1 (Alaca Williams, 8.2.1)**.** *Let $0 \neq I$ be an ideal of $\mathcal{O}_K$. Then there exist finitely many prime ideals of $\mathcal{O}_K$ whose product is a subset of I.*

Proof. Suppose not. Let S be the set of non-zero ideals of $\mathcal{O}_K$ which do not satisfy the theorem. $\mathcal{O}_K$ is Noetherian, so it satisfies the maximal condition, and thus S has a maximal element. So, S contains an ideal I which is not properly contained in any of the other elements of S. $I \in S$ means that I is not a prime ideal. Thus, there exist ideals $J, K \subseteq \mathcal{O}_K$ such that $JK \subseteq I$, but $J \nsubseteq I$ and $K \nsubseteq I$. Now, let $J_1 = J + I$, and $K_1 = K + I$. Recall that the sum of two ideals is the smallest ideal containing both. Then:

$$J_1K_1 = (J + I)(K + I) = JK + JI + IK + I^2 \subseteq I$$

If $I = J_1 = I + J$, then $J \subseteq I$, which reaches a contradiction. Repeating this argument, we then get that $I \neq J_1$ and $I \neq K_1$. So, $J_1K_1 \subseteq I$, $I \subset J_1$, $I \subset K_1$, so J_1, K_1 are not in S, by the maximality of I in S. However, this means J_1 and K_1 satisfy the theorem. and there exist prime ideals of $\mathcal{O}_K$ whose finite product are J_1 and K_1 respectively. However, the product of these prime ideals then sits inside $J_1K_1 \subseteq I$, which is a contradiction because $I \in S$. Thus, S is empty, and so the theorem must be true. □

3.3 Fractional Ideals of $\mathcal{O}_K$ form an Abelian Group

Theorem 3.3.1. *The non-zero fractional ideals of $\mathcal{O}_K$ form an abelian group under multiplication.*

Proof. By the lemma, multiplication is closed, and we have seen that multiplication is commutative. For associativity, we inherit the fact that multiplication of ideals is associative:

$$\begin{aligned} c_1^{-1}I_1(c_2^{-1}I_2c_3^{-1}I_3) &= c_1^{-1}I_1(c_2^{-1}c_3^{-1}I_2I_3) \\ &= c_1^{-1}c_2^{-1}c_3^{-1}I_1(I_2I_3) \\ &= c_1^{-1}c_2^{-1}c_3^{-1}(I_1I_2)I_3 \\ =&(c_1^{-1}I_1c_2^{-1}I_2)c_3^{-1}I_3 \end{aligned}$$

$\mathcal{O}_K$ is the identity element, since $(c^{-1}I)\mathcal{O}_K = c^{-1}(I\mathcal{O}_K) = c^{-1}I$.

Let $J = c^{-1}I$ be a fractional ideal for some ideal I of $\mathcal{O}_K$. Note that $0 \neq c \in \mathcal{O}_K$. Define the following:

$$I^{-1} := \{x \in K : \ xI \subseteq \mathcal{O}_K\}$$
$$J^{-1} := cI^{-1}$$

We will show that J^{-1} is the inverse of J so that $JJ^{-1} = \mathcal{O}_K$. Note that I^{-1} is a fractional ideal. Thus, $II^{-1} \subseteq \mathcal{O}_K \subseteq I^{-1}$, so II^{-1} is an ideal of $\mathcal{O}_K$. By definition, $II^{-1} = I^{-1}I$. Also, $\mathcal{O}_K \subseteq I^{1}$ by definition, so $II^{-1} \subseteq \mathcal{O}_K \subseteq I^{-1}$.

We want to examine if I^{-1} is a fractional ideal. First, we check that $(I^{-1}, +) \leq (K, +)$. Let $a, b \in I^{-1}$. Then, $aI, bI \subseteq \mathcal{O}_K$. So $(a - b)I \subseteq aI + (-b)I \subseteq \mathcal{O}_K \implies a - b \in I^{-1}$. Thus, $(I^{-1}, +) \leq (K, +)$. Now, let $r \in \mathcal{O}_K$, and $a \in I^{-1}$. Then, $raI = arI = aI \subseteq \mathcal{O}_K \implies ra \in I^{-1}$. So I^{-1} is indeed an $\mathcal{O}_K$-module.

We saw that every ideal of $\mathcal{O}_K$ contains $0 \neq c \in \mathbb{Z}$, so $c \in I \cap \mathbb{Z}$. Now, $cI^{-1} \subseteq II^{-1} \subseteq \mathcal{O}_K$. Thus, I^{-1} is a fractional ideal. Then I, I^{-1} are both fractional ideals, so their product is a fractional ideal, and since it sits inside $\mathcal{O}_K$, so II^{-1} is an ideal of $|air$. Note here that if $I_1 \subseteq I_2 \subseteq \mathcal{O}_K$ as ideals, then $\mathcal{O}_K \subseteq I_2^{-1} \subseteq I_1^{-1}$. To prove this, let $x \in I_2^{-1}$. Then, $xI_2 \subseteq \mathcal{O}_K$. $I_1 \subseteq I_2 \implies xI_1 \subseteq xI_2 \subseteq \mathcal{O}_K \implies x \in I_1^{-1}$.

Now, we claim that if I is a non-zero proper ideal of $\mathcal{O}_K$, then $\mathcal{O}_K \subset I^{-1}$. Note here that $\mathcal{O}_K^{-1} = \mathcal{O}_K$, and $\{0\}^{-1} = K$. We saw already that $\mathcal{O}_K \subseteq I^{-1}$. Thus, it suffices to show that $\mathcal{O}_K \neq I^{-1}$ when I is proper. Let S be the set of all proper ideals. S then has a maximal element, since $\mathcal{O}_K$ ie Noetherian, and

this maximal element must be a maximal ideal. Therefore, $I \in S$ is either a maximal ideal or contained in a maximal ideal. So there exists a maximal ideal M of $\mathcal{O}_K$ such that $I \subseteq M \subseteq \mathcal{O}_K$. By the ABOVE CONCLUSION, it suffices to show that $\mathcal{O}_K \subset M^{-1} \subseteq I^{-1}$ for a maximal ideal M. So we need to find an element in $M^{-1} \setminus \mathcal{O}_K$. Let $0 \neq a \in M$. By PREVIOUS THEOREM, (a) contains a product of prime ideals. Let $p_1 p_2 \cdots p_r \subseteq (a) \subseteq M$ for r minimal. M maximal implies that M is prime, and in turn, $p_i \subseteq M$ for some i. Without loss of generality, assume $p_r \subseteq M$. So $p_r \subseteq M \subset \mathcal{O}_K$, but p_r is prime, and thus maximal since we are in a Dedekind Domain. Thus, $p_r = M$. We know that $p_1 \cdots p_{r+1} \not\subseteq (a)$ by the minimality of r. There then exists $b \in p_1 \cdots p_{r-1} \setminus (a)$. Now, consider $bM \subseteq p_1 \cdots p_{r-1} p_r \subseteq (a)$. Thus, $a^{-1}bM \subseteq a^{-1}(a) = \mathcal{O}_K$. Thus, $a^{-1}b \in M^{-1}$. If $a^{-1}b \in \mathcal{O}_K$, then $b \in a\mathcal{O}_K = (a)$, but we picked b from the complement of (a) so we get a contradiction, and thus $a^{-1}b \in M^{-1} \setminus \mathcal{O}_K$, so $\mathcal{O}_K \subset M^{-1} \subseteq I^{-1}$ as desired.

We now claim that if I is a non-zero ideal of $|air$ and $IS \subseteq I$ for some ideal SS of K, then $S \subseteq \mathcal{O}_K$. We must show that if $Is \in I$ for $s \in S$, then $s \in \mathcal{O}_K$. $\mathcal{O}_K$ is Noetherian, so every ideal, I in particular, is finitely generated, so $I = (a_1, a_2, \cdots, a_n)$ for some $0 \neq a_i \in I$.

$$Is \subseteq I \implies a_i s = \sum_{j=1}^{n} b_{ij} a_j \qquad b_{ij} \in \mathcal{O}_K$$

Let $B = (b_{ij})$. Then, $s[a_1\ a_2\ \cdots\ a_n]^\top = B[a_1\ a_2\ \cdots\ a_n]^\top$. Then, $(B - sI_n)[a_1\ a_2\ \cdots\ a_n]^\top = \vec{0}$, and since $a_i \neq 0$, we get $\det(B - sI_n) = 0$. Thus, s is a root of the polynomial $\det(B - xI_n) \in \mathcal{O}_K[x]$. s is then integral over $\mathcal{O}_K$. However, $\mathcal{O}_K$ is integrally closed, so $s \in \mathcal{O}_K \implies S \subseteq \mathcal{O}_K$ as desired.

We now claim that if P is a maximal ideal of $\mathcal{O}_K$, then $PP^{-1} = \mathcal{O}_K$. By the first claim here, PP^{-1} is an ideal of $\mathcal{O}_K$ and $\mathcal{O}_K \subseteq P^{-1}$.Thus, $P\mathcal{O}_K \subseteq PP^{-1} \implies P \subseteq PP^{-1}$. Thus, $P \subseteq PP^{-1} \subseteq \mathcal{O}_K$. Since P is maximal, $P = PP^{-1}$ or $PP^{-1} = \mathcal{O}_K$. If $P = PP^{-1}$, then $P^{-1} \subseteq \mathcal{O}_K$ by the 3rd proposition ($IS \subseteq I$), and so $P^{-1} = \mathcal{O}_K$, which is a contradiction to $\mathcal{O}_K \subset P^{-1}$ from the second proposition. Thus, we must have that $PP^{-1} = \mathcal{O}_K$ as desired.

Finall, we claim that $II^{-1} = \mathcal{O}_K$ for all ideals I of $\mathcal{O}_K$. Suppose not. Let S be the set of ideals which do not satisfy the condition. $\mathcal{O}_K$ is Noetherian, so S has a maximal element, and call this I. Thus, $II^{-1} \subset \mathcal{O}_K$. By the previous claim, I is not a maximal ideal. Thus, I is contained in a maximal ideal, which we denote as M. So $I \subset M \subset \mathcal{O}_K$. Thus, $\mathcal{O}_K \subseteq M^{-1} \subset I^{-1} \implies \underbrace{I\mathcal{O}_K}_{=I} \subset IM^{-1} \subset II^{-1} \subset \mathcal{O}_K$. In particular,$IM^{-1} \subset \mathcal{O}_K$. This is a product of fractional ideals, which is itself a fractional ideal, and since it is a fractional ideal in $\mathcal{O}_K$, IM^{-1} is then a proper ideal of $\mathcal{O}_K$. We also saw that $I \subset IM^{-1}$, but recall that I is the maximal element of S, so $IM^{-1} \notin S \implies$:

$$\begin{aligned}
(IM^{-1})(IM^{-1})^{-1} = II^{-1} = \mathcal{O}_K &\implies I(M^{-1}(IM^{-1})^{-1}) = \mathcal{O}_K \\
&\implies M^{-1}(IM^{-1})^{-1} \subset I^{-1} \\
&\implies \mathcal{O}_K = IM^{-1}(IM^{-1})^{-1} \subseteq I^{-1} \subset \mathcal{O}_K
\end{aligned}$$

We thus get that $\mathcal{O}_K \subset \mathcal{O}_K$, a contradiction, and so S must be empty, and we get our desired result that $II^{-1} = \mathcal{O}_K$ for all ideals I of $|air$.

Now, let $J = c^{-1}I$ be a fractional ideal, for an ideal I and a non-zero $c \in \mathcal{O}_K$. Define $J^{-1} = cI^{-1}$. Then,

$$JJ^{-1} = c^{-1}IcI^{-1} = c^{-1}cII^{-1} = II^{-1} = \mathcal{O}_K$$

□

3.4 Prime Factorization of ideals of $\mathcal{O}_K$

Theorem 3.4.1. *Let K be a number field. Every non-zero proper ideal of $\mathcal{O}_K$ can be written as a product of prime ideals uniquely up to the order of factors.*

Proof. We first prove existence. Suppose not. Let S be the set of ideals which are counterexamples to the statement of the theorem. S contains a maximal element I. Thus, I is not a prime ideal, and so I is not a maximal ideal. There exists a maximal ideal M such that $I \subset M \subset \mathcal{O}_K \subset M^{-1} \subset I^{-1}$. Thus, $I \subset IM^{-1} \subset II^{-1} = \mathcal{O}_K$. Si $I \subset IM^{-1} \subset \mathcal{O}_K$. IM^{-1} is thus an ideal of $\mathcal{O}_K$ as per the same argument we saw above, and $IM^{-1} \notin S$, since it properly contains I. There then exist prime ideals $p_1, \cdots, p_r$ such that $IM^{-1} = \prod_{i=1}^{r} p_i \implies I = p_1 \cdots p_r M$, but M is maximal, and thus is prime, so I is a product of prime ideals. Thus, we achieved a contradiction, and have our desired result that every ideal is a product of prime ideals.

Now, for uniqueness. Suppose not. Then, we once again denote the set S to be the set of all counterexamples and have a maximal element I. Let $I = p_1 p_2 \cdots p_r = q_1 q_2 \cdots q_s$. Then, $p_1 \cdots p_r \subseteq q_1$ and so on, so $p_i \subseteq q_i$ for some $i \in \{1, \cdots, r\}$. Without loss of generality, let $p_1 \subseteq q_1$. However, since p_1 and q_1 are both prime, they are both maximal ideals, and so $p_1 = q_1 \implies p_1^{-1} = q_1^{-1}$. Thus, $Ip_1^{-1} = p_2 p_3 \cdots, p_r = q_2 q_3 \cdots q_s$. Now, $\mathcal{O}_K \subseteq p_1^{-1} \implies I \subset Ip_1^{-1} \subseteq p_1 p_1^{-1} = \mathcal{O}_K$. This gives that Ip_1^{-1} is an ideal of $\mathcal{O}_K$ and I is contained properly in it , so $Ip_1^{-1} \notin S$, and thus satisfies the uniqueness part of the theorem. This means there exist some ordering such that $p_i = q_i$ for $i \in \{2, \cdots, r\}$, and so along with $p_1 = q_1$, we get that I satisfies the uniqueness. Thus, S is empty, and we have the result we wanted. □

Definition 3.4.1. *We write $I|J$ if there exists an ideal L such that $J = IL$.*

Remark 3.4.1.

1. *If $I|J$, then $J \subseteq I$.*
2. *If P is a prime ideal, we saw that:*

$$(IJ \subseteq P \implies I \subseteq P \vee J \subseteq P) \iff (P|IJ \implies P|I \vee P|J)$$

3. *We write $I|a$ if $I|(a)$*

Definition 3.4.2. *A common divisor of ideals I and J is an ideal K such that $K|I$ and $K|J$. K is a gcd of I and J if whenever K' is a common divisor of I and J, then $K'|K$. In particular, $gcd(I, J) = I + J$ is the smallest ideal containing both I and J.*

Remark 3.4.2. *In $\mathcal{O}_K$, where $I = \prod_{i=1}^{r} p_i^{n_i}$, $J = \prod_{i=1}^{r} p_i^{m_i}$, $gcd(I, J) = \prod_{i=1}^{r} p_i^{\min n_i, m_i}$*

Definition 3.4.3. *We denote $lcm(I, J)$ to be the largest ideal divisible by I and J. Thus, $K = lcm(I, J)$ if $I|K$ and $J|K$. and if $I|K'$ and $J|K'$, then $K|K'$. In particular, this is $I \cap J$.*

Definition 3.4.4. *Let I be an ideal of $\mathcal{O}_K$. We define the <u>norm</u> of I in $\mathcal{O}_K$ as*

$$N(I) := |\mathcal{O}_K / I| = [\mathcal{O}_K : I]$$

Remark 3.4.3.

1. *We saw earlier that $[\mathcal{O}_K : I] < \infty$*
2. *We also saw that every non-zero ideal of $\mathcal{O}_K$ has a $\mathbb{Z}$ basis $\{x_1, \cdots, x_n\}$ where $n = [K : \mathbb{Q}]$.*

Theorem 3.4.2. *Let $\{a_1, \cdots, a_n\}$ be a $\mathbb{Z}$-basis for I, a non-zero ideal of $\mathcal{O}_K$*

a) $N(I) = \left|\frac{D(a_1,\cdots,a_n)}{D_K}\right|^{\frac{1}{2}}$

b) If $I = (a)$ for some $0 \neq a \in I \subseteq \mathcal{O}_K$, then $N(I) = |N_K(a)|$.

Proof. a) In general, in a finite abelian group G, with basis $\{w_1, \cdots, w_n\}$ and H a finite abelian subgroup with basis $\{a_1, \cdots, a_n\}$ then there exist $c_{ij} \in \mathbb{Z}$ such that $\alpha_1 = \sum_{j=1}^{n} c_{ij} w_j$, then $[G : H] = |\det(c_{ij})_{ij}|$. So if $G = \mathcal{O}_K$ and $H = I$, then $D(a_1, \cdots, a_n) = (\det C)^2 D(w_1, \cdots, w_n) = [\mathcal{O}_K : I]^2 D_K$, which gives us the desired result (mod algebraic operations).

b) Note that $(a) = a\mathcal{O}_K = \{ac_1w_1 + \cdots + ac_nw_n : \ c_i \in \mathbb{Z}\}$. where $\{w_1, \cdots, w_n\}$ is an integral basis for $\mathcal{O}_K$. Thus, $\{aw_1, \cdots, aw_n\}$ is a $|Z$ basis for (a). Now, choose $c_{ij} \in \mathbb{Z}$ such that $aw_i = \sum_{j=1}^{n} c_{ij} w_j$ for all $1 \leq i \leq n$. Then, $N((a)) = |\det(c_{ij})_{ij}|$, but by definition, $N_K(a) = \det(c_{ij})_{ij}$, so $N((a)) = |N_K(a)|$. □

Remark 3.4.4. *If I, J are ideals of $\mathcal{O}_K$ such that $J \subseteq I$ and $I|J$, then $[\mathcal{O}_K : J] = [\mathcal{O}_K : I][I : J] \implies N(J) = N(I)\underbrace{[I : J]}_{<\infty} \implies N(I)|N(J)$. Conversely, let $N(I)|N(J)$. Then, $[\mathcal{O}_K : I]|\mathcal{O}_K : J]$, so $[I : J] \geq 1 \implies J \subseteq I$. In summary:*

$$I|J \iff N(I)|N(J)$$

Theorem 3.4.3. *Let I and J be non-zero ideals of $\mathcal{O}_K$. Then:*

$$N(IJ) = N(I)N(J)$$

Proof. Note that if I or J is $\mathcal{O}_K$. Without loss of generality, let $J = \mathcal{O}_K$. Noting that $N(\mathcal{O}_K) = [\mathcal{O}_K : \mathcal{O}_K] = 1$, we have that $N(I\mathcal{O}_K) = N(I) = N(I) \cdot 1 = N(I)N(J)$

Now, let $I, J \neq \mathcal{O}_K$. Let $J = P$, a prime ideal. we want to show that $N(IP) = N(I)N(P)$. Now, $IP \subset I \subset \mathcal{O}_K$. $IP \neq I$ due to unique factorization of prime ideals.

$$N(IP) = [\mathcal{O}_K : IP] = [\mathcal{O}_K : I][I : IP] = N(I)[I : IP]$$

Thus, it suffices to show that $[\mathcal{O}_K : P] = N(P) = [I : IP]$. Let $a \in I \setminus IP$. Consider the homomorphism $f : \mathcal{O}_K \to I/IP$ which maps $x \mapsto xa + IP$. The plan here is to use the First Isomorphism Theorem.

$\ker f = \{x \in \mathcal{O}_K : \ xa + IP = IP\}$. If $x \in P$, then $xa + IP \subseteq IP$. Thus, $P \subseteq \ker f \subseteq \mathcal{O}_K$. Given that P is a maximal ideal and that $1 \notin \ker f$, we get that $P \subseteq \ker f \subset \mathcal{O}_K \implies \ker f = P$. Now, $Im(f)$ is a subring of I/IP and $Im(f) = K/IP$ for some $IP \subseteq K \subseteq I$. We note that $Im(f)$ is an ideal of I/IP, so K is an ideal of $\mathcal{O}_K$ contained in J. Now we get that $IP \neq K$ because $Im(f) = K/IP = \{id\}$. Now if $I = P_1P_2 \cdots P_r$ is a prime factorization of I, then:

$$\begin{aligned}
P_1P_2 \cdots P_rP \subset K \subseteq P_1P_2 \cdots P_r &\implies K = P_1P_2 \cdots P_rK' && (P \subset K' \subseteq \mathcal{O}_K) \\
&\implies K' = \mathcal{O}_K && (P \text{ is maximal}) \\
&\implies K = P_1P_2 \cdots P_rI \\
&\implies Im(f) = I/IP \\
&\implies f \text{ is surjective}
\end{aligned}$$

Thus, the First Isomorphism Theorem, $\mathcal{O}_K/P \cong I/IP$, so $N(P) =]I : IP]$, so $N(IP) = N(I)N(P)$. Now, if J is instead a product of primes, we use the multiplicativity of the norm to get the same result □

Theorem 3.4.4. *Let I be a non-zero ideal of $\mathcal{O}_K$ where $[K:\mathbb{Q}] = n$.*

a) If $N(I)$ is a prime number, then I is a prime ideal. Note that the converse is false.

b) $N(I) \in I$.

c) If P is a prime ideal, then P divides exactly one prime number p and $N(P) = p^t$, $1 \leq t \leq n$. This prime p is called the prime below P. Conversely, P is a prime ideal above p. If $(p) = P_1^{e_1} P_2^{e_2} \cdots P_r^{e_r}$, then each P_i is a prime ideal above p. p is the prime below each P_i. t is called the inertial degree of P in $\mathcal{O}_K$.

Proof. a) Let $N(I) = p$ where p is a prime number. Let $I \subseteq J \subseteq \mathcal{O}_K$. Then:

$$[\mathcal{O}_K : I] = [\mathcal{O}_K : J][J : I]$$

Given that $N(I)$ is prime, either $[\mathcal{O}_K : J] = 1 \implies J = \mathcal{O}_K$ or $[J : I] = 1 \implies J = I$. This gives that I is maximal, and thus prime as an ideal.

b) Let $m = N(I) = [\mathcal{O}_K : I] = |\mathcal{O}_K / I|$. This then implies that $m(a + I) = id_{\mathcal{O}_K/I} = I \iff ma + I = I \iff ma \in I$. In particular, for a choice $a = 1$, $m \in I$, so $N(I) \in I$.

c) Let P be a prime ideal of $\mathcal{O}_K$. Then, $P \cap \mathbb{Z}$ is a prime ideal of $\mathbb{Z}$. Let $P \cap \mathbb{Z} = (p)$ for some prime number p. Then, $(p) \subseteq P \implies P|p \iff P|(p)$. We now want to show that p is unique. Let $q \neq p$ be a prime number such that $P|q \implies (q) \subseteq P$. So, $p \in P$ and $q \in P$, and so $\langle p, q \rangle \subseteq P$, but p and q are relatively prime integers, There then exist $u, v \in \mathbb{Z}$ such that $pu + qv = 1$. Thus, $1 \in \langle p, q \rangle \subseteq P \implies P = \mathcal{O}_K$. This is clearly a contradiction, so $p = q$.

Now, let $N(P) = m = p_1 p_2 \cdots p_r$ where the primes are not necessarily distinct. By Part (b), $N(P) \in P$, so $(N(P)) \subseteq P$, so we get that $(p_1 p_2 \cdots p_r) \subseteq P \implies (p_1)(p_2) \cdots (p_r) \subseteq P$. However, since P is a prime ideal, $(p_i) \subseteq P$ for some p_i. Then, $P|(p_i) \implies N(P)|N((p_i)) = N(p_i) = p_i^n$. We then get that $N(p)|p^n$ so $N(P) = p^t$ for some $1 \leq t \leq n$. Now, $(p_i) \subseteq P \implies P|p_i$. p_i is then the prime below P, which we called p, and so $N(P) = p^t$.

□

Corollary 3.4.1. *a) Every non-zero ideal in $\mathcal{O}_K$ has only finite many ideal divisors.*

b) A non-zero integer rational integer belongs to only finitely many ideals.

c) Only finitely many ideals have a given norm.

Proof. a) This follows from unique factorization into prime ideals.

b) If $n \in I$ for some $n \in \mathbb{Z}$, then $(n) \subseteq I \implies I|(n)$. However, by part (a), only finitely many such ideals cam exist.

c) From Theorem 2.7.4, we get that $N(I) \in I$. If infinitely many ideals have norm N, then $I|N$ for infinitely many I, which is a contradiction to Part (b) above. Thus, we have our desired result.

□

Remark 3.4.5. *If P is a prime ideal of $\mathcal{O}_K$, then P is a maximal ideal as well. Thus, $\mathcal{O}_K/P$ is a field, and $|\mathcal{O}_K/P| = \mathcal{N}(P) = p^t$ for some $1 \leq t \leq n = [K:\mathbb{Q}]$.*

Theorem 3.4.5. *Let K be an algebraic number field with $[K : \mathbb{Q}] = n$. Let P be a prime ideal and $\langle P \rangle = \prod_{i=1}^{g} P_i^{e_i}$, its unique prime ideal factorization. Let t_i be the inertial degree of P_i. Then, $\sum_{i=1}^{g} e_i t_i = n$*

Proof. We begin by noting that $\mathcal{N}(\langle P \rangle) = \mathcal{N}(P_1^{e_1} P_2^{e_2} \cdots P_g^{e_g}) \implies p^n = \prod_{i=1}^{g} p^{t_i e_i} = p^{\sum_{i=1}^{n} t_i e_i} \implies n = \sum_{i=1}^{g} t_i e_i$. □

Definition 3.4.5. *g as defined in Theorem 2.7.5 is called the decomposition number of p in $\mathcal{O}_K$. We note that $g \leq n$.*

Definition 3.4.6. *e_i from Theorem 2.7.5 is called the $ramificationindex$ of P_i over $\mathcal{O}_K$. We note that $e_i \leq n$. If $e_i > 1$ for some $1 \leq i \leq g$, then p ramifies in $\mathcal{O}_K$. If $e_i = 1$ for all $1 \leq i \leq g$, then p is unramified in $\mathcal{O}_K$. Further here, if $g = 1$, then p is inert in $\mathcal{O}_K$, which indicates that $\langle p \rangle$ is a prime ideal. If $g > 1$, then we say p splits completely in $\mathcal{O}_K$.*

Theorem 3.4.6 (Dedekind)**.** *Let K be an algebraic number field, and let p be a prime number. p ramifies in $\mathcal{O}_K$ if and only if $p | D_K$.*

Proof. For the forward direction, we use Section 5.4 from Murty, Esmonde. □

Example 3.4.1. *Let $K = \mathbb{Q}(\sqrt{d})$, where d is a square free integer. Recall that:*

$$D_K = \begin{cases} 4d, & d \not\equiv 1 \pmod 4 \\ d, & d \equiv 1 \pmod 4 \end{cases}$$

Thus, if $d \not\equiv 1 \pmod 4$, $2 | D_K$. Then, 2 ramifies in $\mathcal{O}_K$ in this case, so $\langle 2 \rangle = P^2$ with $\mathcal{N}(P) = 2$. $[K : \mathbb{Q}] = 2 \implies g \leq 2$, so the only possibilities are:

$$(p) = P_1 P_2 \qquad \textit{(splits completely)}$$

$$(p) = P^2 \qquad \textit{(ramified)}$$

$$(p) = P \qquad \textit{(inert)}$$

Lemma 3.4.1. *Let I, J be non-zero ideals of $\mathcal{O}_K$. Then, $\exists \alpha \in I$ such that $\alpha I^{-1} + J = \mathcal{O}_K$*[4].

Proof. Let $J = P_1 \cdots P_r$, its prime factorization,and let $I_i = I P_1 \cdots P_{i-1} P_{i+1} \cdots P_r \subseteq I$. Choose, for every $i \in \{1, \cdots, r\}$, $\alpha_i \in I_i \setminus I_i P_i$[5]. Let $\alpha = \sum_{i=1}^{r} \alpha_i \in I$.

We want to show that $\alpha \notin I P_i$, for every i. Suppose not. Suppose $\alpha \in I P_i$ for some i. For $1 \leq j \leq r$, $i \neq j$, $\alpha_j \in I_j = I \underbrace{P_1 \cdots P_{j-1} P_{j+1} \cdots P_r}_{\text{contains } P_i} \subseteq I P_i$. $\alpha_i = \underbrace{\alpha}_{\in I P_i} - \sum_{k \neq i} \alpha_k$. Each of these terms are in $I P_i$, so $\alpha_i \in I P_i$. Thus, $(\alpha_i) \subseteq I P_i /$ and $(\alpha_i) \subseteq I_i$. So $I P_i | (\alpha_i)$ and $I_i = I P_1 P_2 \cdots P_{i-1} P_{i+1} \cdots P_r | (\alpha_i)$. This implies that $I_i P_i | (\alpha_i)$, so $\alpha_i \in I_i P_i$, a contradiction to how we constructed these α_i's. Our assumption that $\alpha \in I P_i$ is

[4] Note that $\alpha \in I$ and $I I^{-1} = \mathcal{O}_K$, so $\alpha I^{-1} \subseteq \mathcal{O}_K$, not only as a subset but as an ideal as well

[5] Note here that $I_i P_i \neq I_i$ by unique factorization

then false, so $\alpha \notin IP_i$ for all $i \in \{1, \cdots, r\}$.

$$\begin{aligned}
\alpha \notin IP_i &\implies \alpha \in I \setminus IP_i \\
&\implies \alpha I^{-1} \in \mathcal{O}_K \setminus P_i \\
&\implies \alpha I^{-1} \not\subseteq P_i \\
&\implies P_i \subset P_i + \alpha I^{-1} \subseteq \mathcal{O}_K \\
&\implies P_i + \alpha I^{-1} = \mathcal{O}_K && \text{(Since } P_i \text{ is maximal)} \\
&\implies \exists a_i \in \alpha I^{-1},\ b_i \in P_i \text{ such that } a_i + b_i = 1 \\
&\implies b_i = 1 - a_i \\
&\implies \prod_{i=1}^{r} b_i = \prod_{i=1}^{r}(1 - a_i) = 1 - \underbrace{f(a_1 a_2 \cdots a_r)}_{\in \alpha I^{-1}} && f \in \mathbb{Z}[x_1 x_2 \cdots x_n] \\
&\implies \alpha I^{-1} + J = \mathcal{O}_K
\end{aligned}$$

□

Theorem 3.4.7. *Let $I \neq 0$ be an ideal of $\mathcal{O}_K$. Let $0 \neq \beta \in I$. There then exists $\alpha \in I$ such that $I = \langle \alpha, \beta \rangle$.*

Proof. Let $J = \beta I^{-1}$ be an ideal of $\mathcal{O}_K$. Then, from Lemma 2.7.1, there exists $\alpha \in I$ such that $\alpha I^{-1} + J = \mathcal{O}_K$, so $\alpha I^{-1} + \beta I^{-1} = \mathcal{O}_K \implies \alpha\mathcal{O}_K + \beta\mathcal{O}_K = I \implies \langle \alpha, \beta \rangle = I$. □

Theorem 3.4.8 (Dedekind)**.** *Let K be an algebraic number field of degree n with $\mathcal{O}_K = \mathbb{Z}[\theta]$ for some $\theta \in \mathcal{O}_K$. Let $f(x)$ be the minimal polynomial of θ. Let p be a prime number and let $f + p(x)$ be the reduction of $f(x) \pmod p$. If $f_p(x) = \prod_{i=1}^{g} f_i(x)^{e_i}$ is the unique factorization of $f_p(x)$ in $\mathbb{Z}_p[x]$ into monic polynomials. Then, $\langle p \rangle = \prod_{i=1}^{g} P_i^{e_i}$ where $P_i = \langle p, f_i(\theta) \rangle$ are disctinct prime ideals with $N(P_i) = p^{deg(f_i(x)}$.*

Proof. See Theorem 5.1.1 in Murty, Esmonde, or Theorems 10.3.1, 10.5.1 in Alaca, Williams. In the latter, we can replace $\mathcal{O}_K = \mathbb{Z}(\theta)$ with the condition $p \not| [\mathcal{O}_K : \mathbb{Z}(|theta)]$. □

Example 3.4.2. *Factor (18) into prime ideals in $\mathbb{Z}[\sqrt{-17}]$. Note that if $K = \mathbb{Q}(\sqrt{-17})$, then $-17 \equiv 3 \pmod 4 \implies \mathcal{O}_K = \mathbb{Z}[\sqrt{-17}]$. The minimal polynomial for $\theta = \sqrt{-17}$ is $f(x) = x^2 + 17$. We also note that $(18) = (2)(3)^2$. We now use Dedekind's Theorem to factor (2) and (3).*

In the $p = 2$ case, $f(x) = x^2 + 17 \implies f_2(x) = x^2 + 1 = (x + 1)^2 \in \mathbb{Z}_2[x]$. each of these factors is now irreducible, so $(2) = P_1^2$, where $P_1 = \langle 2, \sqrt{-17} + 1 \rangle$. In the $p = 3$ case, $f(x) = x^2 + 17 \implies f_3(x) = x^2 + 2 = (x+1)(x+2) \in \mathbb{Z}_3[x]$. Then, $(3) = P_2 P_3$, where $P_2 = \langle 3, \sqrt{-17} + 1 \rangle$ and $P_3 = \langle \sqrt{-17} + 2 \rangle$. Then, $(18) = P_1^2 P_2^2 P_3^2$. Now, for something completely different! Let's not use Dedekind's Theorem.

Note once again that $(18) = (2)(3)^2$ and $(18) = (1 + \sqrt{-17})(1 - \sqrt{-17})$. Let $\langle 18 \rangle = \prod_{i=1}^{g} P_i^{e_i}$. be a unique prime factorization. Then, $P_i | (18) \implies P_i | (2)(3)^2 \implies (2)(3)^2 \subseteq P_i$, for every i. Thus, $(2) \in P_i$ or $(3) \in P_i$. We can also do this for the other factorization to show that $(1 + \sqrt{-17})(1 - \sqrt{-17}) \subseteq P_i \implies (1 + \sqrt{-17}) \subseteq P_i \vee (1 - \sqrt{-17}) \subseteq P_i$. Thus, any prime ideal in the factorization of (18) must contain the above conditions. Let $P = \langle 2, 1 + \sqrt{-17} \rangle = \langle 2, 1 - \sqrt{-17} \rangle$. $P | (2) \implies N(P) | N(2) \implies = 2^2 = 4$. Similarly, $N(P) | N(1 + \sqrt{-17}) = 18 \implies N(P) | 2$. If $N(P) = 1$, this means $P = \mathcal{O}_K$, which is clearly true since P is maximal, so $N(P) = 2$. Then, we are guaranteed that P is a prime ideal. Let S be another prime ideal containing (2). Then, $9 \cdot 2 = 18 \implies 9 \in S$, and $18 = (1 + \sqrt{-17})(1 - \sqrt{-17}) \in S$ implies that either $1 + \sqrt{-17}$ or $1 - \sqrt{-17}$ belongs to S since S is prime. Then, $(2, 1 \pm \sqrt{-17}) = P \subseteq S$, but since P and S are both prime, we have that $P = S$. P is thus the only prime ideal containing (2). Then.

$(2) = P^e \implies N(2) = N(P)^e \implies 4 = 2^e \implies e = 2.$

Now, Let $P_1 = \langle 3, 1 + \sqrt{-17} \rangle$*, and* $P_2 = \langle 3, 1 - \sqrt{-17} \rangle$*, noting that* $P_1 \neq P_2$*. As above,* $(3) \subseteq P \implies N(P)|9$*. Consider* $\phi : \mathbb{Z}[\sqrt{-17}] \to \mathbb{Z}_3$*, where* $a + b\sqrt{-17} \mapsto a - b \pmod 3$*.* ϕ *is a surjective homomorphism.* $ker\phi = P_1$*. By the First Isomorphism Theorem,* $\mathcal{O}_K/P \cong \mathbb{Z}_3 \implies N(P_1) = 3$ *so* P_1 *is prime. Similarly,* P_2 *is a prime ideal using* $\phi_2 : \mathcal{O}_K \to \mathbb{Z}_3$ *where* $\phi_2 : a + b\sqrt{-17} \mapsto a + b \pmod 3$*. We then have* $P_1P_2 = \langle 9, 3(1 + \sqrt{-17}), 3(1 - \sqrt{-17}), 18 \rangle = \langle 3 \rangle$*. Thus, we get our result that* $(18) = P^2(P_1P_2)^2 = P^2P_1^2P_2^2$*, as we saw from Dedekind's Theorem.*

Theorem 3.4.9. *Let* K *be an algebraic number field.* $\mathcal{O}_K$ *is a UFD id and only if* $\mathcal{O}_K$ *is a PID.*

Proof. The backwards direction is trivially true. Now, assume $\mathcal{O}_K$ is a UFD. Every ideal in $\mathcal{O}_K$ is a product of prime ideals. It suffices to show that all prime ideals are principal. Let $0 \neq P$ be a prime ideal where $N(P) = n \in \mathbb{Z}^+$. and $N(P) \in P$. Thus, $P|(n)$. $n \in \subseteq \mathcal{O}_K$ means that n has a unique factorization, since $\mathcal{O}_K$ is a UFD. Then, there exist $a_1 \cdots a_s$ such that $(n) = (a_1)(a_2) \cdots (a_s)$ so $P|(a_i)$ for some (a_i). Recalling that all irreducibles are prime in a UFD, we then have that (a_i) is a prime ideal. However, by unique factorization, $P = (a_i)$, so P is principal. □

4 Factorization of primes in quadratic number fields

4.1 Introduction

Definition 4.1.1. *Let p be a prime number. $0 \neq a \in \mathbb{Z}$ is called a quadratic residue $\pmod p$ if there exists $x \in \mathbb{Z}$ such that $x^2 \equiv a \pmod p$. Otherwise, we say that a is a quadratic non-residue.*

Example 4.1.1. *Consider $p = 5$*

x	$[x^2]_5$
1	1
2	4
3	4
4	1

Thus, the residues are 1 and 4, and the non-residues are 2 and 3.

In general, for an odd prime p, there are exactly $\frac{p-1}{2}$ residues and non-residues each.

Theorem 4.1.1 (Euler's Criterion)**.** *Let p be an odd prime. Let $a \in \mathbb{Z}$ such that $gcd(a, p) = 1$. a is a quadratic residue $\pmod p$ if and only if $a^{\frac{p-1}{2}} \equiv 1 \pmod p$*

Definition 4.1.2. *Let p be an odd prime. The Legendre Symbol $\left(\frac{a}{p}\right)$ is defined as:*

$$\left(\frac{a}{p}\right) = \begin{cases} 0, & \text{if } p|a \\ +1, & \text{if } a \text{ is a quadratic residue} \\ 1, & \text{if } a \text{ is a -quadratic non-residue} \end{cases}$$

Proposition 4.1.1. *1) $a^{\frac{p-1}{2}} \equiv \left(\frac{a}{p}\right) \pmod p$*

2) $\left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right)\left(\frac{b}{p}\right)$

3) If $a \equiv b \pmod p$, then $\left(\frac{a}{p}\right) = \left(\frac{b}{p}\right)$

Theorem 4.1.2. *Let p be an odd prime.*

$$\left(\frac{-1}{p}\right) = \begin{cases} +1, & p \equiv 1 \pmod 4 \\ -1, & p \equiv 3 \pmod 4 \end{cases}$$

$$\left(\frac{2}{p}\right) = \begin{cases} +1, & p \equiv 1, 7 \pmod 8 \\ -1, & p \equiv 3, 5 \pmod 8 \end{cases}$$

Proof. The first proof follows immediately from Euler's Criterion. The second follows from Gauss' Lemma, which states that if p is an odd prime, and $gcd(a, p) = 1$, n is the number of integers in $S = \{a, 2a, 3a, \cdots, \left(\frac{p-1}{2}\right)a\}$. Then, $\left(\frac{a}{p}\right) = (-1)^n$. □

Theorem 4.1.3 (Quadratic Reciprocity)**.** *If p and q are odd primes, then:*

$$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{\frac{p-1}{2}\cdot\frac{q-1}{2}}$$

Example 4.1.2. 317 *and* 727 *are both prime.*

$$\begin{aligned}
\left(\frac{317}{727}\right) &= \left(\frac{727}{317}\right) && (317 \equiv 1 \pmod 4)\\
&= \left(\frac{93}{317}\right) && (727 \equiv 93 \pmod{317})\\
&= \left(\frac{3}{317}\right)\left(\frac{31}{317}\right)\\
&= \left(\frac{317}{3}\right)\left(\frac{317}{13}\right)\\
&= \left(\frac{2}{3}\right)\left(\frac{7}{31}\right)\\
&= -\left(\frac{7}{31}\right)\\
&= \left(\frac{31}{7}\right)\\
&= \left(\frac{3}{7}\right) = -1
\end{aligned}$$

Here, we recall that given an algebraic number field K where $[K:\mathbb{Q}] = 2$, we have a prime factorization as follows:

$$\langle p\rangle = P_1^{e_1}\cdots P_g^{e_g}$$

In this case, $N(P_i) = p^{t_i}$ for some $1 \le t_i \le n$, and so $\sum_{i=1}^{g} e_i t_i = n \implies g \le n \wedge e_i \le n$.

Example 4.1.3. *Consider $K = \mathbb{Q}[\sqrt{d}]$, where d is square free, so $n = [K:\mathbb{Q}] = 2$. Thus, $g \le 2$, so $g = 1$ or $g = 2$. First, let us consider the case where $g = 2$.*

$$\langle p\rangle = P_1^{e_1}P_2^{e_2} \implies e_i = t_i = 1 \implies \langle p\rangle = P_1P_2$$

Also, note in the above that $N(P_i) = p$. In this case, p splits completely.

Now, consider $g = 1$. $\langle p\rangle = P_1^{e_1}$ and $e_1t_1 = 2$. Thus, either $\langle P\rangle = P^2$ and $\mathcal{N}(P) = p$ (and in this case, p ramifies), or $\langle p\rangle = P$ and $\mathcal{N}(P) = p^2$, and in this case, p is inert.

Theorem 4.1.4. *Let p be an odd prime. Let $K = \mathbb{Q}(\sqrt{d})$, where d is square free. Then:*

1) $\left(\frac{d}{p}\right) = 1 \iff \langle p\rangle = P_1P_2,\ \mathcal{N}(P_i) = p$ *(Splits completely)*

2) $\left(\frac{d}{p}\right) = 0 \iff \langle p\rangle = P^2,\ N(P) = p$ *(ramifies)*

3) $\left(\frac{d}{p}\right) = -1 \iff \langle p\rangle = P,\ N(P) = p^2$ *(inert)*

Proof. Refer to 10.2.1 from Alaca, Williams, or 7.4.2 from Esmonde, Murty. We know there are only 3 possible cases for the factorization of $\langle p\rangle$ which are mutually exclusive, and there are only 3 possible values for $\left(\frac{d}{p}\right)$. Thus, it suffices only to prove the forward direction in each case, since we are essentially proving a bijection between finite sets by only proving injectivity.

1) Let $\left(\frac{d}{p}\right) = 1$. Then, there exists $x \in \mathbb{Z}$ such that $d \equiv x^2 \pmod{p}$ and $gcd(x,p) = 1$ (otherwise $p|x \implies p|d \implies \left(\frac{d}{p}\right) = 0$). Let $P_1 = \left\langle p, x+\sqrt{d}\right\rangle$ and $P_2 = \left\langle x-\sqrt{d}\right\rangle$. Then:

$$P_1P_2 = \left\langle p^2, p(x+\sqrt{d}), p(x-\sqrt{d}), x^2-d\right\rangle = \langle p\rangle \underbrace{\left\langle p, x-\sqrt{d}, x+\sqrt{d}, \frac{x^2-d}{p}\right\rangle}_{=I}$$

Note that $2x = (x+\sqrt{d})(x-\sqrt{d}) \in I$, and also $p \in I$. Now, we also note that $gcd(2x,p) = 1 \implies 1 \in I \implies I = \mathcal{O}_K$. Thus, $P_1P_2 = \langle p\rangle \mathcal{O}_K = \langle p\rangle$. We now examine whether P_1 and P_2 are prime.

$\langle p\rangle = P_1P_2 \implies p^2 = N(\langle p\rangle) = N(P_1P_2) = N(P_1)N(P_2)$. $N(P_i) \neq 1$ since $P_i \neq \mathcal{O}_K$, so the only factorization here is that $N(P_1) = N(P_2) = p$, which implies P_1 and P_2 are prime ideals. Now it remains to show that these are distinct. Suppose $P_1 = P_2$. Then, $2x = (x+\sqrt{d})(x-\sqrt{d}) \in P_1 = P_2$. Then, we get that $2x \in P_1 \cap \mathbb{Z}$, so $p|2x$, which is a contradiction, since $gcd(x,p) = 1$ and $p \not| 2$. Thus, P_1 and P_2 are indeed distinct.

2) Let $\left(\frac{d}{p}\right) = 0$. In other words, $p|d$. Let $P = \left\langle p.\sqrt{d}\right\rangle$. Then, $P^2 = \left\langle p^2, p\sqrt{d}, d\right\rangle = \langle p\rangle \left\langle p, \sqrt{d}, \frac{d}{p}\right\rangle$. Now, we note that $gcd(p, \frac{d}{p}) = 1$ because otherwise, $p^2|d$ but d is square-free. Thus, $1 \in I \implies I = \mathcal{O}_K$. Thus, $P^2 = \langle p\rangle \mathcal{O}_K = \langle p\rangle$. Taking norms, we get $N(P^2) = p^2 \implies N(P) = p$, and thus P is a prime ideal.

3) Finally, let $\left(\frac{d}{p}\right) = -1$. We want to show that $\langle p\rangle$ is a prime ideal. Suppose not. Then, we have only 2 possibilities. $\langle p\rangle = P_1P_2$ or $\langle p\rangle = P_3^2$. In each of these cases, $N(P_i) = p$. Recalling the definition of the norm of an ideal, this gives $|\mathcal{O}_K/P_i| = p$, and $p \in P_i$. Note that $1, 2, \cdots, p-1 \notin P_i$ by definition of the cosets. Otherwise, $1 = gcd(t,p) \in P_i \implies P_i = \mathcal{O}_K$, which provides a contradiction. Let $t_1 \neq t_2$ where $1 \leq t_1, t_2 \leq p-1$. Suppose for the sake of contradiction that these generate the same coset. That is, $t_1 + P_i = t_2 + P_2$. Thus, $t_1 - t_2 \in P_i$. However, $1 \leq |t_1 - t_2| \leq p-1$, which we should earlier to be false. Thus, $0, \cdots, p-1$ form a complete set of representatives for $\mathcal{O}_K/P_i = \{P_i, 1+P_i, \cdots, (p-1)+P_i\}$. Consider $\sqrt{d} \in \mathcal{O}_K$. The coset $\sqrt{d} + P_i$ must be $t + P_i$ for some $1 \leq t \leq p-1$. We can exclude $t = 0$ because this would mean $\sqrt{d} \in P_i \implies d \in P_i \implies p_d \implies \left(\frac{d}{p}\right) = 0 \neq -1$. Now, we get that $\sqrt{d}-t \in P_i \implies (\sqrt{d}+t)(\sqrt{d}-t) \in P_i \implies d-t^2 \in P_i \implies d-t^2 \in P_i \cap \mathbb{Z} = pZ \implies p|d-t^2 \implies d \equiv t^2 \pmod{p} \implies \left(\frac{d}{p}\right) = 1$. We thus get a contradiction here, so we MUST have that $\langle p\rangle = P$ is prime.

□

In summary, we get that:

$$\langle p\rangle = \begin{cases} \left\langle p, x+\sqrt{d}\right\rangle \left\langle p, x-\sqrt{d}\right\rangle, & \left(\frac{d}{p}\right) = 1 \\ \left\langle p, \sqrt{d}\right\rangle^2, & \left(\frac{d}{p}\right) = 0 \\ \langle p\rangle \text{ prime}, & \left(\frac{d}{p}\right) = -1 \end{cases}$$

Definition 4.1.3 (Part of Kronecker Symbol)**.**

$$\left(\frac{a}{2}\right) = \begin{cases} 0, & a \text{ is even} \\ 1, & a \equiv \pm 1 \pmod{8} \\ -1, & a \equiv 3, 5 \pmod{8} \end{cases}$$

Theorem 4.1.5. *Let $p = 2$, $K = \mathbb{Q}(\sqrt{d})$, where d is square free.*

1) $d \equiv 1 \pmod{8} \iff (2) = P_1P_2, N(P_i) = 2$. $P_1 = \left\langle 2, \frac{1+\sqrt{d}}{2}\right\rangle$ and $P_2 = \left\langle 2, \frac{1-\sqrt{d}}{2}\right\rangle$

2) $d \equiv 2, 3 \pmod 4 \iff \langle 2 \rangle = P^2,\ N(P) = 2.\ P = \left\langle 2, \sqrt{d} \right\rangle$

3) $d \equiv 5 \pmod 8 \iff (2)$ *is prime*

Proof. Refer to Theorem 10.2.1 in Alaca Williams, and Theorem 7.4.5, in Esmonde, Murty. □

Let $K = \mathbb{Q}(\sqrt{d})$ with discriminant D_K. Then:

1) $\left(\frac{D_K}{p}\right) = 1 \iff \langle p \rangle = P_1 P_2,\ \mathcal{N}(P_i) = p$ (Splits completely)

2) $\left(\frac{D_K}{p}\right) = 0 \iff \langle p \rangle = P^2,\ N(P) = p$ (ramifies)

3) $\left(\frac{D_K}{p}\right) = -1 \iff \langle p \rangle = P,\ N(P) = p^2$ (inert)

5 Hecke Characters

5.1 Multiplicative characters of a finite (abelian) group

Let G be a finite group with $|G| = n$.

Definition 5.1.1. *A multiplicative character is a function $\chi : G \to \mathbb{C}^\times$ satisfying $\chi(ab) = \chi(a)\chi(b)$ for all $a, b \in G$.*

Remark 5.1.1. *χ is a group homomorphism.*

Example 5.1.1. *We have the trivial (or principal) character $1_G : G \to \mathbb{C}^\times$, where $1_G(a) = 1$ for all $a \in G$. This has the following properties:*

- $\chi(e_G) = 1$
- If $a^r = e$, for some $r \in \mathbb{Z}^+$, then $\chi(a^r) = \chi(e) = 1 \implies \chi(a)^r = 1$
- $\overline{\chi(a)} = \chi(a)^{-1}$
- $\chi(a)$ is an n^{th} root of unity for some n.

Remark 5.1.2. *Let $\widehat{G} = \{\chi : g \to \mathbb{C}^\times : \ \chi \text{ is a homomorphism}\}$ be the set of all multiplicative characters of G. Define an operation on $\widehat{G}$ by:*

$$\chi_1\chi_2(a) = \chi_1(a)\chi_2(a), \qquad \forall a \in G$$

By this operation, $\widehat{G}$ is an abelian group with identity 1_G. It also turns out that:

$$\chi^{-1}(a) = \chi(a^{-1}) = \chi(a)^{-1} = \overline{\chi(a)}$$

Theorem 5.1.1. *If G is abelian, then $G \cong \widehat{G}$.*

Remark 5.1.3. *The following are some orthogonal relations, given an abelian group G of order n.*

1. *For any $\chi \in \widehat{G}$*
$$\sum_{a \in G} \chi(a) = \begin{cases} n, & \chi = 1_G \\ 0, & else \end{cases}$$
2. *For any $a \in G$*
$$\sum_{\chi \in \widehat{G}} \chi(a) = \begin{cases} n, & a = e \\ 0, & else \end{cases}$$

Remark 5.1.4. *We have a special case where $G = \mathbb{F}_{p^r}^\times$, where p is prime. In this case, $|G| = p^r - 1$, so $\chi(a)$ is a $(p^r - 1)^{th}$ root of unity.*

5.2 Dirichlet Characters

The motivation behind Dirichlet Characters comes from turning a multiplicative character into an arithmetic function.

Definition 5.2.1. *An arithmetic function or number-theoretic function is a function f such that $f : \mathbb{Z} \to \mathbb{C}$ or more commonly, $f : \mathbb{Z}^+ \to \mathbb{C}$.*

Let $2 \leq K \in \mathbb{Z}^+$. Let $G = (\mathbb{Z}/k\mathbb{Z})^\times$. If $k = 1$, $G = \{1\} \implies \widehat{G} = \{1_G\}$.

Now, consider the case where $k = 3$. $G = \{1, 2\}$. Then, $\widehat{G} = \{1 + G, \chi : \ \chi^2 = 1_G\}$, where $\chi(1) = 1$ ad $\chi(2) = -1$.

Let $k = 4$. $G = \{1, 3\}$. Same as the $k = 3$ case.

Let $k = 5$. $G = \{1, 2, 3, 4\}$. Then, $\widehat{G} = \{1_G, \chi_2, \chi_3, \chi_4\}$.

	1	2	3	4
1_G	1	1	1	1
χ_2	1	i	$-i$	-1
χ_3	1	-1	-1	1
χ_4	1	$-i$	i	-1

The moral of the story is that χ maps into roots of unity.

Remark 5.2.1. *Noe that $|(\mathbb{Z}/k\mathbb{Z})^\times| = \phi(k)$.*

Definition 5.2.2. *A Dirichlet character $\pmod{k \in \mathbb{Z}^+}$ is a function $\chi : \mathbb{Z} \to \mathbb{C}^\times$ satisfying:*

1) $\chi(m) = 0$ if $gcd(m, k) > 1$

2) $\chi(m + k) = \chi(m), \ \forall m \in \mathbb{Z}$

3) $\chi(m_1 m_2) = \chi(m_1)\chi(m_2), \ \forall m_1, m_2 \in \mathbb{Z}$

Remark 5.2.2. *Every Dirichlet character corresponds to a multiplicative character of $(\mathbb{Z}/k\mathbb{Z})^\times$, so there are $\phi(k)$ Dirichlet characters $\pmod{k}$. If $gcd(m, k) = 1$, then $\chi(m)$ is a $\phi(k)^{th}$ root of unity.*

Definition 5.2.3. *A character of order 2 is called a quadratic character. In other words, $\chi^2 = 1_G$ and $\chi(a) = \pm 1$*

Remark 5.2.3. *In correspondence with Remark 5.1.3, the following are some orthogonal relations.*

1. *For χ, a Dirichlet character $\pmod{k}$,*

$$\sum_{a \in \mathbb{Z}/k\mathbb{Z}} \chi(a) = \begin{cases} \phi(k), & \phi = 1_G \\ 0, & else \end{cases}$$

2. *For $a \in \mathbb{Z}$*

$$\sum_{\chi \pmod{k}} \chi(a) = \begin{cases} \phi(k), & a \equiv 1 \pmod{k} \\ 0, & else \end{cases}$$

Example 5.2.1. *Let $k = 4$. Then, $\phi(k) = 2/$*

	0	1	2	3
χ_1	0	1	0	1
χ_2	0	1	0	-1

Let $k = 8$. Let $\phi(k) = 4$. Note that $\widehat{G} \cong V_4$.

	0	1	2	3	4	5	6	7
ψ_1	0	1	0	1	0	1	0	1
ψ_2	0	1	0	1	0	-1	0	-1
ψ_3	0	1	0	-1	0	1	0	-1
ψ_4	0	1	0	-1	0	-1	0	1

Note that $\psi_3(a) = \chi_2(a)$. This gives us that ψ_3 is induced by χ_2. IF ψ is a Dirichlet character $\pmod n$ and there exists $d|n$ such that $\phi(a) = \phi(b)$ when $a \equiv b \pmod d$, then ψ is induced by a Dirichlet character $\pmod d$.

Definition 5.2.4. *We call a Dirichlet character primitive if it is not induced by a Dirichlet character with lower modulus. Collecting characters in this way is an equivalence relation. In other words, two Dirichlet characters are equivalent if they can be induced by the same character. The conductor of the class is the modulus of the character with the least modulus in the class.*

Remark 5.2.4. *If the conductor of a Dirichlet character is equal to its modulus, then the character is primitive.*

Definition 5.2.5. *Let $s \in \mathbb{C}$, and let χ be a Dirichlet character. Then, the Dirichlet L-function is defined as:*

$$L(s, \chi) = \sum_{n=1}^{\infty} \chi(n) n^{-s}$$

Remark 5.2.5.

- *$L(s, \chi)$ converges absolutely for $Re(s) > 1$.*
- *If χ is trivial, then this is the Riemann zeta function, which has a simple pole at $s = 1$.*
- *For non-trivial χ, $L(s, \chi)$ is entire.*
- *$L(s, \chi)$ has an analytic continuation to the whole plane.*
- *For $Re(s) > 1$, we have the Euler Product as follows:*

$$L(s, \chi) = \prod_{p \text{ prime}} (1 - \chi(p) p^{-s})$$

5.3 Hecke Characters

Let K be an algebraic number field with ring of integers $\mathcal{O}_K$. Let $[K:\mathbb{Q}] = n$. We denote $\mathfrak{F}_K$ as the group of fractional ideals of K, $\{c^{-1}I : \ 0 \neq c \in \mathcal{O}_K, I \text{ an ideal of } \mathcal{O}_K\}$. We denote $\mathfrak{P}_K$ to be the subgroup of principal fractional ideals, $\{\langle\alpha\rangle : \ \alpha \in K\}$, where $\langle\alpha\rangle = \{r\alpha : \ r \in \mathcal{O}_K\}$.

Remark 5.3.1. *Note that* $\alpha \in K \implies \alpha = \frac{d}{c}$ *for some* $d \in \mathcal{O}_K$ *and* $c \neq 0$. *Then:*

$$\begin{aligned}\langle\alpha\rangle &= \{r\alpha : \ r \in \mathcal{O}_K\} \\ &= \{r\frac{d}{c} : \ r \in \mathcal{O}_K\} \\ &= c^{-1}\{rd : \ r \in \mathcal{O}_K\} \\ &= c^{-1}\langle d\rangle\end{aligned}$$

Thus, every principal fractional ideal is of the form $c^{-1}I$ *where* I *is a principal ideal of* $\mathcal{O}_K$.

Remark 5.3.2. *If* $\mathcal{O}_K$ *is a PID, then all ideals are principal, and so* $\mathfrak{F}_K = \mathfrak{P}_K$.

Remark 5.3.3.

$$\mathfrak{P}_K = \{c^{-1}\langle d\rangle : \ 0 \neq c, d \in \mathcal{O}_K, \langle d\rangle \ \text{ a principal ideal of } \mathcal{O}_K\}$$

Note that $\langle d\rangle^{-1} = \{x \in K : \ x\langle d\rangle \in \mathcal{O}_K\}$, *by definition is the inverse of* $\langle d\rangle$ *in* $\mathfrak{F}_K$.

Theorem 5.3.1.

$$\langle d\rangle^{-1} = \left\langle \frac{1}{d} \right\rangle = \left\langle d^{-1} \right\rangle$$

Proof. Clearly, $\left\langle \frac{1}{d} \right\rangle \subseteq \langle d\rangle^{-1}$. Conversely, let $x \in \langle d\rangle^{-1}$. Then, $x \in K$ and $x\langle d\rangle \subseteq \mathcal{O}_K$. Since $x \in K$, we have that $x = \frac{a}{b}$ where $a, b \in \mathcal{O}_K$, $b \neq 0$, and $\frac{a}{b}\langle d\rangle \subseteq \mathcal{O}_K$. We then have $\left\langle \frac{ad}{b} \right\rangle \subseteq \mathcal{O}_K$. $[ad, b] \sim [t, 1]$ for some $t \in \mathcal{O}_K$, where $\sim$ is a relation similarly to forming $\mathbb{Q}$ from $\mathbb{R}$. Then, $ad - bt = 0 \implies ad = bt \implies x = \frac{a}{b} = \frac{t}{d} \in \left\langle \frac{1}{d} \right\rangle$. Thus, $\langle d\rangle^{-1} = \left\langle \frac{1}{d} \right\rangle = \left\langle d^{-1} \right\rangle$ as desired. □

Corollary 5.3.1. $\mathfrak{P}_K$ *is a subgroup of* $\mathfrak{F}_K$

Proof.

$$\langle\alpha\rangle\langle\beta\rangle^{-1} = \langle\alpha\rangle\left\langle\beta^{-1}\right\rangle = \left\langle\alpha\beta^{-1}\right\rangle \in \mathfrak{P}_K \implies \mathfrak{P}_K \leq \mathfrak{F}_K$$

□

Remark 5.3.4. *Let* I *be an ideal of* $\mathcal{O}_K$. *Let* $I = P_1P_2\cdots P_r$ *be the unique prime ideal factorization of* I, *where* P_i*'s are not necessarily distinct. Let* $J = c^1I$ *with* $0 \neq c \in \mathcal{O}_K$ *be a fractional ideal. Then,* $cJ = I = P_1P_2\cdots P_r \implies (c)J = P_1P_2\cdots P_r$. *Now, let* $(c) = P_{r+1}P_{r+2}\cdots P_s$ *be the unique prime ideal factorization of* (c), *which is an ideal of* $\mathcal{O}_K$. *This means that* $(c)^{-1} = P_{r+1}^{-1}P_{r+2}^{-1}\cdots P_s^{-1}$ *because* $\mathfrak{F}_K$ *is commutative. Thus,* $J = (c)^{-1}P_1\cdots P_r = P_1\cdots P_rP_{r+1}^{-1}\cdots P_s^{-1}$. *The upshot here is that every fractional ideal has a unique factorization into prime ideals once we allow negative powers. In other words,*

$$J = \prod_i P_i^{e_i} \qquad e_i \in \mathbb{Z}, P_i \text{ prime ideals of } \mathcal{O}_K$$

Remark 5.3.5. *Let* $J_1 = \prod_{i=1}^s P_i^{e_i}$ *and* $J_2 = \prod_{i=1}^s P_i^{f_i}$ *be fractional ideals. Then:*

$$gcd(J_1, J_2) = J_1 + J_2 = \prod_{i=1}^s P_i^{\min(e_i, f_i)}$$

$$lcm(J_1, J_2) = J_1 \cap J_2 = \prod_{i=1}^s P_i^{\max(e_i, f_i)}$$

So, J_1 *and* J_2 *are relatively prime iff* $gcd(J_1, J_2) = (1)$, *so there is no prime ideal appearing in both factorizations.*

6 Notes to Update

6.1 31 October 2022

Remark 6.1.1. *Constructed Dirichlet characters as a special case of Hecke characters*

Let $K = \mathbb{Q}, \mathcal{O}_K = \mathbb{Z}, (m) \subset \mathcal{O}_K$ an ideal, χ a Dirichlet Character:

$$\chi : (\mathbb{Z}/m\mathbb{Z})^\star \to \mathbb{C}^\star$$
$$\simeq \chi : K(\mathfrak{f})/K_1(\mathfrak{f}) \to \mathbb{C}^\star$$

Where

$$\Psi_\infty : K^\star \to \mathbb{C}^\star : \alpha \mapsto \chi(\text{sgn}(\alpha))$$

6.2 7 November 2022

More generally,

$$(\mathcal{O}_K/\mathfrak{f})^\star \simeq K(\mathfrak{f}/K_q(\mathfrak{f}))$$

So in general we can define a multiplicative character

$$\Psi_{\text{finite}} : K(\mathfrak{f})/K_1(\mathfrak{f}) \to \mathbb{C}^\star$$

By:

$$\Psi_{\text{finite}}(\alpha K_1(\mathfrak{f})) = \Psi((\alpha))/\Psi_\infty(\alpha)$$

Example 6.2.1.

$K = \mathbb{Q}(\sqrt{-1}) = \mathbb{Q}(i)$

$$\implies \mathcal{O}_K = \mathbb{Z}[\sqrt{-1}] = \mathbb{Z}[i](PID)$$
$$D_k = -4 \because -1 \not\equiv 1 \mod 4$$
$$\implies \mathfrak{F}_K = \mathfrak{P}_K \mathfrak{F}_K(\mathfrak{f}) = \mathfrak{P}_K(\mathfrak{f})$$
$$\textit{now, let } \mathfrak{f} := (1) = \mathcal{O}_K$$
$$\implies \mathfrak{F}_K = \mathfrak{P}_K = \mathfrak{F}_K(\mathfrak{f}) = \mathfrak{P}_K(\mathfrak{f})$$
$$= \{c^{-1} < d > | c, d \in \mathbb{Z}[\sqrt{-1}] \setminus \{0\}\}$$
$$= \{(\alpha) | \alpha \in \mathbb{Q}[i] \setminus \{0\}\}$$

So

$$K(\mathfrak{f}) = \{\frac{d}{c} | c, d \in \mathbb{Z}[\sqrt{-1}] \setminus \{0\}\}$$

$$K_1(\mathfrak{f}) = \{\frac{d}{c} | c, d \in \mathbb{Z}[\sqrt{-1}] \setminus \{0\}, d - c \in \mathcal{O}_K\} = K(\mathfrak{f})$$

...

Remark 6.2.1. *Hecke characters also have an associated L-series*