ON ELEMENTS OF
ALGEBRAIC NUMBER THEORY

BY

SHILPI MANDAL

UNDER THE SUPERVISION OF

DR. BISWAJYOTI SAHA

A THESIS SUBMITTED TO
THE SCHOOL OF MATHEMATICS AND STATISTICS
IN PARTIAL FULFILLMENT OF THE REQUIREMENTS
FOR THE DEGREE OF
INTEGRATED MASTERS' IN MATHEMATICAL SCIENCES
OF
UNIVERSITY OF HYDERABAD.

हैदराबाद विश्वविद्यालय
University of Hyderabad

प्रतिष्ठित संस्थान
INSTITUTION OF EMINENCE
राष्ट्रीय अपेक्षाएँ, वैश्विक मानक
National Needs, Global Standards

UNIVERSITY OF HYDERABAD,

HYDERABAD - 500046.

JUNE, 2020

CERTIFICATE

This is to certify that **Shilpi Mandal**, with registration number **15IMMM15**, has carried out the project embodied in the present thesis titled *On Elements of Algebraic Number Theory*, towards partial fulfillment of the requirements for the award of the degree of Integrated M. Sc. in Mathematical Sciences.

Shilpi Mandal

Dr. Biswajyoti Saha (**Supervisor**)

Prof. R. Radha (**Dean, School of Maths and Stats**)

Place : School of Mathematics and Statistics, University of Hyderabad,
Hyderabad - 500046, India

Date : 19th August 2020

ACKNOWLEDGEMENT

I owe my deepest gratitude to my supervisor Dr. Biswajyoti Saha, whose support from the beginning till the end helped me develop an understanding of the subject. The encouragement at each step and a guidance towards the bigger picture of the content enabled me to advance in the project. This project would not have been successful without his clear instructions. His way of teaching and giving crystal clear insight of concepts, all the while staying rigorous, helped me a lot and will definitely prove useful in my future too. He uplifted me when necessary and motivated me to work harder and understand the values of a mentor-student relationship. I received help from Saha sir in writing each and every part of my thesis, typing in LaTeX and every aspect in my project work.

In a time when I was contemplating my choices, his support throughout the academic year and beyond, and his patience helped me both academically and personally. Due to the unfateful turn of events in 2020 maybe we did not achieve what we wanted to, but where we have reached in this project will now form the foundations of my academic life ahead.

I would like to thank the School of Mathematics and Statistics, UoH for providing the atmosphere for my professional growth.

I'd also like to thank my friends (few honorable mentions, Hridika Roy, Aditya Sarma Phukon, Alaap Hassan, Sreejani Choudhary) and my family for believing in me and helping me become this version of myself.

Contents

Chapter 1

Algebraic number fields

1.1 Elements integral over a ring

Before formally defining the notion of an algebraic number field or an algebraic integer, we will define the notion of integrality in a general context of commutative rings with unity, hereafter rings.

Definition 1.1. *Let A, B be rings such that $A \subset B$. An element $b \in B$ is called* ***integral*** *over A if it satisfies an equation of the form*

$$x^n + a_1x^{n-1} + \cdots + a_n = 0, n \geq 1,$$

with coefficients $a_i \in A$. The ring B is called ***integral*** *over A if all elements $b \in B$ are integral over A.*

Example 1.1. Let $A = \mathbb{Z}$ and $B = \mathbb{Z}[i]$. Then $i \in B$ is integral over A as it is a root of the polynomial $x^2 + 1 = 0$. Also, B is integral over A. Any $\alpha = a + ib \in B$ satisfies the polynomial $x^2 - 2ax + a^2 + b^2$.

Theorem 1.1. *Let R be a ring, A a subring of R, and $x \in R$. The following statements are equivalent:*

(i) There exists $a_0, \ldots, a_{n-1} \in A$ such that

$$x^n + a_{n-1}x^{n-1} + \cdots + a_1x + a_0 = 0 \tag{1.1}$$

(i.e., x is a root of a monic polynomial with coefficients in A).

(ii) The ring $A[x]$ is an A-module of finite-type.

(iii) There exists a subring B if R which contains A and x and which is an A-module of finite-type.

Proof. (i) ⇒ (ii)

Let M be the A-submodule of R generated by $1, x, \dots, x^{n-1}$. By (i), $x^n \in M$. Multiplying (1.1) with x^j, we obtain $x^{n+j} = -a_{n-1}x^{n+j-1} - \cdots - a_0 x^j$. Induction on j implies that $x^{n+j} \in M$, for all $j \geq 0$. As $A[x]$ is the A-module generated by $\{x^k, k \geq 0\}$, we see that $A[x] = M$.

(ii) ⇒ (iii)

Take $B = A[x]$.

(iii) ⇒ (i)

Let $\{y_1, \dots, y_n\}$ be a finite set of generators for B as a module over A, i.e., $B = Ay_1 + \cdots + Ay_n$. Since $x \in B$ and since B is a subring of R, it follows that $xy_i \in B$ for all $i = 1, \dots, n$. Therefore,

$$xy_i = \sum_{j=1}^{n} a_{ij} y_j,$$

for any $i = 1, \dots, n$; $a_{ij} \in A, 1 \leq i, j \leq n$. This means that

$$\sum_{j=1}^{n} (\delta_{ij} x - a_{ij}) y_j = 0, i = 1, \dots, n.$$

Consider this system of n homogeneous linear equations in $\{y_1, \dots, y_n\}$. Write d for the determinant $\det(\delta_{ij}x - a_{ij})$. Multiplying the above equation by the adjoint of the matrix $(\delta_{ij}x - a_{ij})$, we see that $dy_i = 0$ for every i. This means that $d \cdot b = 0$ for all $b \in B$; in particular, $d \cdot 1 = 0$, so $d = 0$. But d is clearly a monic polynomial in x, since the highest order term appears in the expansion of the product $\prod_{i=1}^{n}(x - a_{ii})$ of the entries of the principal diagonal. Thus (iii) implies (i). □

Proposition 1.1. *Let R be a ring, A a subring of R, and let $(x_i)_{1 \leq i \leq n}$ be a finite set of elements of R. If, for all i, x_i is integral over $A[x_1, \dots, x_{i-1}]$, then $A[x_1, \dots, x_n]$ is an A-module of finite-type.*

Proof. We argue by induction on n. The case $n = 1$ follows from Theorem 1.1 (ii).

Now assume that $B = A[x_1, \dots, x_{n-1}]$ is an A-module of finite-type. Then $B = \sum_{j=1}^{p} Ab_j$ for some $b_1, \dots, b_p \in B$. Writing $A[x_1, \dots, x_{n-1}, x_n] = B[x_n]$, the case $n = 1$ implies that is a B-module of finite-type. Write $B[x_n] = \sum_{k=1}^{q} Bc_k$ for some $c_1, \dots, c_q \in B[x_n]$. Then

$$A[x_1, \dots, x_n] = \sum_{k=1}^{q} Bc_k = \sum_{k=1}^{q} (\sum_{j=1}^{p} Ab_j)c_k = \sum_{j,k} Ab_jc_k$$

Thus $(b_jc_k)_{1 \leq j \leq p;\ 1 \leq k \leq q}$ is a finite set of generators for $A[x_1, \dots, x_n]$ as a module over A. □

1.2 Algebraic numbers and algebraic integers

Definition 1.2. *A complex number α is said to be* ***algebraic*** *if α is a root of a non-zero polynomial $p(x) \in \mathbb{Q}[x]$. A complex number α is called* ***transcendental*** *if α is not algebraic.*

In general, for L/K a field extension and α an element of L, we say α is **algebraic** over K if α is a root of a non-zero polynomial $p(x) \in \mathbb{K}[x]$. If every element of L is algebraic over K, then we say L is an algebraic extension, or L is algebraic over K.

Definition 1.3. *Let L be a field extension of K, α an element of L and $K[x]$ the ring of polynomials in x over K. The* ***minimal polynomial*** *of α is defined as the monic polynomial of least degree among all polynomials in $K[x]$ having α as a root. It is denoted by m_α.*

Example 1.2. $\sqrt{2}$ is algebraic over $\mathbb{Q}$ with minimal polynomial $x^2 - 2$.

Note that the minimal polynomial of an element is irreducible.

Example 1.3. Let p be a prime. Let ζ_p be a primitive p^{th}-root of unity with minimal polynomial $\frac{x^p-1}{x-1} = 1 + x + \cdots + x^{p-1}$ over $\mathbb{Q}$.

The set $\{q(x) \in \mathbb{Q}[x] \mid q(\alpha) = 0\}$ is an ideal of $\mathbb{Q}[x]$. As $\mathbb{Q}[x]$ is a principal ideal domain (PID), we have $\{q(x) \in \mathbb{Q}[x] \mid q(\alpha) = 0\} = \langle m_\alpha \rangle$; where m_α is the minimal polynomial of α . If $m_\alpha = x^n + a_1 x^{n-1} + \cdots + a_0$; where $a_i \in \mathbb{Q}$ then *degree* of α is n, denoted by $deg(\alpha)$.

Define the set $\mathbb{Q}[\alpha] := \{f(\alpha) | f(x) \in \mathbb{Q}[x]\}$.

Proposition 1.2. *Let α be an algebraic number of degree n. Then the subring $\mathbb{Q}[\alpha]$ of $\mathbb{C}$ is a field.*

Proof. Let m_α be the minimal polynomial of α. Consider the ring homomorphism

$$q : \mathbb{Q}[x] \longrightarrow \mathbb{C}$$

defined by

$$\sum_{i=0}^{m} b_i x_i \longmapsto \sum_{i=0}^{m} b_i \alpha_i$$

Kernel of q, $\mathrm{Ker}(q) = \{f(x) \in \mathbb{Q}[x] \mid f(\alpha) = 0\} = \langle m_\alpha \rangle$ is an ideal of $\mathbb{Q}[x]$.

Image of q, $\mathrm{Im}(q) = \mathbb{Q}[\alpha]$ is a subring of $\mathbb{C}$.

By the 1^{st} Homomorphism Theorem for Rings,

$$\frac{\mathbb{Q}[x]}{\langle m_\alpha \rangle} \cong \mathbb{Q}[\alpha]$$

Now we claim that $\frac{\mathbb{Q}[x]}{\langle m_\alpha \rangle}$ is a field. It is enough to show that $\langle m_\alpha \rangle$ is a maximal ideal of $\mathbb{Q}[x]$.

Let $f \notin \langle m_\alpha \rangle$, i.e., $m_\alpha \nmid f$. The ideal generated by m_α and f is a principal ideal generated by, say g.

Since $g | m_\alpha$, we have $m_\alpha = c.g$, where $c \in \mathbb{Q}[x]$. But m_α is an irreducible polynomial, so $c \in \mathbb{Q}^*$. But this is impossible because $g|f$ and $m_\alpha \nmid f$. Thus, $g \in \mathbb{Q}^*$ and $\langle g \rangle = \mathbb{Q}[x]$. Hence $\langle m_\alpha \rangle$ is maximal. □

Definition 1.4. *A subfield K of $\mathbb{C}$ is called an* ***algebraic number field*** *or simply a number field if $dim_{\mathbb{Q}}(K) < \infty$, when K is taken as a vector space over $\mathbb{Q}$. If $dim_{\mathbb{Q}}(K) = n$, then degree of K is n.*

Note that any finite extension is an algebraic extension, hence the name algebraic number field.

Example 1.4. The field $K = \mathbb{Q}[\sqrt{2}]$ is a subfield of $\mathbb{C}$. K is an algebraic number field with $dim_{\mathbb{Q}}(K) = 2$.

Example 1.5. Referring to example 1.3, $K = \mathbb{Q}[\zeta_p]$ is a number field with $dim_{\mathbb{Q}}(K) = p - 1$.

Remark 1.1. Any element α in a number field K is algebraic.

Remark 1.2. If α is an algebraic number of degree n, then $\mathbb{Q}[\alpha]$ is a number field of degree n.

Proof. Since α is an algebraic number of degree n, then $a_n\alpha^n + a_{n-1}\alpha^{n-1} + \cdots + a_0 = 0$ where $a_i \in \mathbb{Q}, a_n \neq 0$. Hence $\alpha^n = -\frac{1}{a_n}(a_{n-1}\alpha^{n-1} + \cdots + a_0)$.

Thus the span of $\{1, \alpha, \cdots, \alpha^{n-1}\}$ is $\mathbb{Q}[\alpha]$.

To show: $\{1, \alpha, \cdots, \alpha^{n-1}\}$ is linearly independent over $\mathbb{Q}$.

Proof: Suppose there exist $b_i \in \mathbb{Q}$ and not all $b_i = 0$, such that $b_0 + b_1\alpha + \cdots + b_{n-1}\alpha^{n-1} = 0$. Then $\deg(\alpha) = n - 1$, which is a contradiction to the hypothesis. □

Definition 1.5. *A complex number α is said to be an **algebraic integer** if α is a root of a monic polynomial in $\mathbb{Z}[x]$.*

Example 1.6. Let $K = \mathbb{Q}[\sqrt{2}]$. Then $\sqrt{2} \in K$ is an algebraic integer, while $\frac{2}{3} \in K$ is an algebraic number but not an algebraic integer.

Remark 1.3. An algebraic integer is an algebraic number.

Remark 1.4. An element of $\mathbb{Z}$ is an algebraic integer.

Remark 1.5. If $\alpha \in \mathbb{Q}$ is an algebraic integer, then $\alpha \in \mathbb{Z}$.

Proof. Let $\alpha = \frac{r}{s} \in \mathbb{Q}$ where $\gcd(r, s) = 1$ and α satisfies $x^n + a_1 x^{n-1} + \cdots + a_0 = 0; a_i \in \mathbb{Z}$, i.e., $\frac{r^n}{s^n} + \cdots + a_0 = 0$. Multiplying the above equation by s^n we get, $r^n + s a_1 r^{n-1} + \cdots + s^n a_0 = 0$.

So $r^n = -s(a_1 r^{n-1} + \cdots + s^{n-1} a_0)$. Hence $s|r^n$, i.e., $s|r$. Thus $s = \pm 1$ (as $\gcd(s, r) = 1$).

Thus, $\alpha \in \mathbb{Z}$. □

Remark 1.6. For any algebraic number α, there exists $m \neq 0 \in \mathbb{Z}$ such that $m\alpha$ is an algebraic integer.

Proof. If $\deg(\alpha) = n$, then there exist $a_i \in \mathbb{Q}$ such that $\alpha^n + a_1 \alpha^{n-1} + \cdots + a_n = 0$. Choose $m \in \mathbb{Z}$ such that $m a_i \in \mathbb{Z}$ for every i.

Multiplying the above equation by m^n, we get $(m\alpha)^n + (m a_1)(m\alpha)^{n-1} + \cdots + m^n a_n = 0$.

Thus, $m\alpha$ is an algebraic integer. □

Definition 1.6. *A polynomial $f = a_n x^n + \cdots + a_0 \in \mathbb{Z}[x]$ is said to be primitive if gcd$(a_0, a_1, \ldots, a_n) = 1$.*

Hence any monic polynomial in $\mathbb{Z}[x]$ is primitive. We recall the famous Gauss's lemma.

Lemma 1.1. (**Gauss**) *The product of two primitive polynomials in $\mathbb{Z}[x]$ is primitive.*

Remark 1.7. Any polynomial $f \in \mathbb{Q}[x]$ can be written in the form $f = \frac{a}{b} g$; where g is primitive, g $\in \mathbb{Z}[x]$ and a,b $\in \mathbb{Z}$ with $\gcd(a, b) = 1$. In fact, we can also ensure that the leading coefficient of g is a positive integer.

Proposition 1.3. *The following are equivalent:*

(i) α is an algebraic integer.

(ii) m_α is a monic polynomial in $\mathbb{Z}[x]$.

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

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

Proof. (i) $\Rightarrow$ (ii)

Let $f = x^n + a_1x^{n-1} + \cdots + a_n; a_i \in \mathbb{Z}$ such that $f(\alpha) = 0$. Let m_α be the minimal polynomial of $\alpha \in \mathbb{Q}[x]$.

Then $m_\alpha | f$, i.e., $f = gm_\alpha$ where $g \in \mathbb{Q}[x]$. By remark 7, $m_\alpha = \frac{a}{b}m'_\alpha$ and $g = \frac{c}{d}g'$; where $m'_\alpha, g' \in \mathbb{Z}[x]$ are primitive and $a, b, c, d \in \mathbb{Z}$ such that $\gcd(a, b) = \gcd(c, d) = 1$, also the leading coefficients of m'_α, g' are positive integers.

So, $f = \frac{ac}{bd}m'_\alpha g'$ and $m'_\alpha g'$ is also primitive (by Gauss Lemma).

Comparing the gcd of coefficients on both sides of $(bd)f = (ac)m'_\alpha g'$, we get $bd = \pm ac$ (since f is primitive). Hence $f = \pm m'_\alpha g'$. In fact, we have $f = m'_\alpha g'$, as leading coefficients of all of them are positive integers.

Since f is monic, comparing the leading coefficients of $f = m'_\alpha g'$, we get the leading coefficient of $m'_\alpha = 1$. Also, $m_\alpha = \frac{a}{b}m'_\alpha$ implies that $m'_\alpha(\alpha) = 0$. Hence $m_\alpha = m'_\alpha$ as both are monic polynomials of same degree for which α is a root.

(ii) $\Rightarrow$ (iii)

Let $\phi = x^n + a_{n-1}x^{n-1} + \cdots + a_0 \in \mathbb{Z}[x]$ be a polynomial such that $\phi(\alpha) = 0$. Then clearly $\mathbb{Z}[\alpha]$ is generated by $1, \alpha, \ldots, \alpha^{n-1}$ over $\mathbb{Z}$.

(iii) $\Rightarrow$ (iv)

Clearly, if we take $M = \mathbb{Z}[\alpha]$, then $\alpha\mathbb{Z}[\alpha] \subset \mathbb{Z}[\alpha]$.

(iv) $\Rightarrow$ (i)

Let $M = \mathbb{Z}v_1 + \cdots + \mathbb{Z}v_n \subset \mathbb{C}$ be a finitely-generated $\mathbb{Z}$-module and $\alpha \neq 0 \in \mathbb{C}$ such that $\alpha M \subset M$. Then $\alpha v_i = \sum_{j=0}^{n} a_{ij}v_j$; where $a_{ij} \in \mathbb{Z}$ for every i, j. Define $A = (a_{ij})$, then $Av = \alpha v$, i.e., α is a characteristic value of A and it satisfies the characteristic equation, which is of degree n and is monic. Since $a_{ij} \in \mathbb{Z}$, means the characteristic equation belongs to $\mathbb{Z}[x]$. Hence α is an algebraic integer of degree n. □

1.3 Ring of integers

Let K be a number field. Let $\mathcal{O}_K$ denote the set of algebraic integers in K. If α, $\beta \in \mathcal{O}_K$, then by Proposition 1.3, $\mathbb{Z}[\alpha]$, $\mathbb{Z}[\beta]$ are finitely-generated $\mathbb{Z}$-modules. Then the ring $M = \mathbb{Z}[\alpha, \beta]$ is also a finitely generated $\mathbb{Z}$-module.

Let $\gamma = \alpha \pm \beta$ or $\gamma = \alpha\beta$, then $\gamma M \subset M$ (by Proposition 1.3). Hence $\alpha \pm \beta$ and $\alpha\beta$ are in $\mathcal{O}_K$.

Definition 1.7. *Let K be a number field of degree n. The set of algebraic integers in K, denoted by $\mathcal{O}_K$, is called the* ***ring of integers of K****.*

1.3.1 Ring of integers for quadratic fields

Definition 1.8. *An algebraic number field K of degree 2 is called a* ***quadratic field****.*

Let K be a quadratic field and let $\alpha \neq 0 \in K$. Since $dim_{\mathbb{Q}}(K) = 2$; $\{1, \alpha, \alpha^2\}$ are linearly dependent over $\mathbb{Q}$, i.e., $a_0 + a_1\alpha + a_2\alpha^2 = 0$ for some $a_0, a_1, a_2 \in \mathbb{Q}$. Thus any $\alpha \in K$ is a root of an irreducible polynomial in $\mathbb{Q}[x]$ of degree at most 2.

But K should contain at least one element β whose irreducible polynomial in $\mathbb{Q}[x]$ is of degree 2, since otherwise $K = \mathbb{Q}$. Then $\{1, \beta\}$ forms a base of K over $\mathbb{Q}$, i.e., $K = \mathbb{Q}[\beta]$. Let $a_2\beta^2 + a_1\beta + a_0 = 0$; where without loss of generality, we may suppose that $a_i \in \mathbb{Z}$ and $a_2 \neq 0$.

Multiplying by $4a_2$ we get, $(2a_2\beta + a_1)^2 = a_1^2 - 4a_0a_2$. Let $\gamma = 2a_2\beta + a_1$. We have $K = \mathbb{Q}[\gamma]$.

Denoting $m := a_1^2 - 4a_0a_2 \in \mathbb{Z}$, we see that $K = \mathbb{Q}[\sqrt{m}]$. We could suppose, without loss of generality, that m is square-free.

Definition 1.9. *A quadratic field is called* ***real*** *or* ***imaginary*** *depending on $K \subset \mathbb{R}$ or not.*

A quadratic field is real, if and only if $K = \mathbb{Q}[\sqrt{m}]$ with square-free $m > 1 \in \mathbb{Z}$. Also, if K is an imaginary quadratic field, then $K \cap \mathbb{R} = \mathbb{Q}$.

Any $\alpha \in K$ is of the form $\alpha = p + q(\sqrt{m})$; $p, q \in \mathbb{Q}$. Define the conjugate $\alpha' = p - q(\sqrt{m})$. α is a root of $(x - \alpha)(x - \alpha') = x^2 - (\alpha + \alpha')x + \alpha\alpha' = x^2 - 2px + p^2 - q^2m \in \mathbb{Q}[x]$.

Let $\mathcal{O}_K$ be the ring of integers in K. Any $\alpha \in \mathcal{O}_K$ is of the form $p + q(\sqrt{m})$ for some $p, q \in \mathbb{Q}$.

(i) If $\deg(m_\alpha) = 1$, then $m_\alpha = (x - a)$ for $a \in \mathbb{Z}$.

This implies $a = p$ and $q = 0$.

Thus, $\alpha + \alpha' = 2p = 2a \in \mathbb{Z}$ and $\alpha\alpha' = p^2 - q^2m = a^2 \in \mathbb{Z}$.

(ii) If $\deg(m_\alpha) = 2$, then $m_\alpha = x^2 + cx + d \in \mathbb{Z}[x]$ for some c and d. Since α is a root of $x^2 - 2px + p^2 - q^2m \in \mathbb{Q}[x]$, implies $-c = 2p = \alpha + \alpha'$ and $d = p^2 - q^2m = \alpha\alpha'$.

Conversely, for $p, q \in \mathbb{Q}$, if $2p$ and $p^2 - q^2m$ are in $\mathbb{Z}$, then $\alpha = p + q(\sqrt{m}) \in \mathcal{O}_K$.

Thus, for $\alpha = p + q(\sqrt{m}) \in K$ to belong to $\mathcal{O}_K$, it is necessary and sufficient that $2p$ and $p^2 - q^2m$ are both in $\mathbb{Z}$.

We will use this to explicitly calculate $\mathcal{O}_K$ for quadratic fields K.

Theorem 1.2. *Let K be a quadratic field and let $\mathcal{O}_K$ be its ring of integers. Then*

$$\mathcal{O}_K = \begin{cases} \mathbb{Z} + \mathbb{Z}\big(\frac{1+\sqrt{m}}{2}\big), & \textit{if } m \equiv 1 \pmod 4 \\ \mathbb{Z} + \mathbb{Z}(\sqrt{m}), & \textit{if } m \equiv 2, 3 \pmod 4 \end{cases}$$

Proof. For $p, q \in \mathbb{Q}$, let $\alpha = p + q(\sqrt{m})$ be in $\mathcal{O}_K$, then $a = 2p$ and $b = p^2 - q^2m \in \mathbb{Z}$. Hence, $\frac{a^2 - 4q^2m}{4} \in \mathbb{Z}$. In particular, $4q^2m \in \mathbb{Z}$.

Since m is square-free, $4q^2m = (2q)^2m \in \mathbb{Z}$. If q has a denominator, then m will have to cancel out the square of the denominator. This will contradict the choice of m. Hence $2q \in Z$, and we can write $q = \frac{f}{2}$ with $f \in \mathbb{Z}$. Now, $a^2 - f^2m \equiv 0 \pmod 4$.

Case(i)

Let $m \equiv 1 \pmod 4$. Then $a^2 \equiv f^2 \pmod 4$, i.e., f and a are both even or both odd. Since $m \equiv 1 \pmod 4$, $\frac{1+\sqrt{m}}{2} \in \mathcal{O}_K$, as it is a root of $x^2 - x + \frac{1-m}{4}$.

Now $\alpha = p + q(\sqrt{m}) = \frac{a}{2} + \frac{f}{2}(\sqrt{m}) = \frac{a-f}{2} + \frac{f}{2}\big(\sqrt{m} + 1\big)$. Since a and f are both even or both odd, $a - f = 2k$ for some $k \in \mathbb{Z}$. Implies $\alpha = k + f\big(\frac{\sqrt{m}+1}{2}\big)$. Thus, $\mathcal{O}_K = \mathbb{Z} + \mathbb{Z}\big(\frac{\sqrt{m}+1}{2}\big)$.

Case(ii)

Let $m \equiv$ 2,3 $\pmod 4$, then $a^2 \equiv f^2m \pmod 4$ if and only if a and f are both even. Because, for any $a \in \mathbb{Z}$, $a^2 \equiv 0 \pmod 4$ or $a^2 \equiv 1 \pmod 4$. So in $a^2 \equiv f^2m \pmod 4$, LHS has choices $\bar{0}$ or $\bar{1}$ and RHS has choices $\bar{0}, \bar{2}$ and $\bar{3}$. So a has to be even, hence $2|f$, i.e., f is even. Hence $\alpha = p + q(\sqrt{m}) = \frac{a}{2} + \frac{f}{2}(\sqrt{m}) \in \mathbb{Z} + \mathbb{Z}(\sqrt{m})$. Thus, $\mathcal{O}_K = \mathbb{Z} + \mathbb{Z}(\sqrt{m})$. □

Chapter 2

Conjugates, norm, trace and discriminant

2.1 Conjugates

We begin with the following lemma.

Lemma 2.1. *Any monic irreducible polynomial $f \in \mathbb{Q}[x]$ is the minimal polynomial for any of its roots.*

Proof. Let $\alpha \in \mathbb{C}$ be such that $f(\alpha) = 0$. Then α is an algebraic number. Let m_α be the minimal polynomial of α. This implies $m_\alpha | f$, i.e., $f = m_\alpha g$, where $g \in \mathbb{Q}[x]$.

Now $m_\alpha \notin \mathbb{Q}$ and f is irreducible. Hence, $f = c \cdot m_\alpha$, where $c \in \mathbb{Q}$. Also since f, m_α are both monic, implies $c = 1$ and thus $f = m_\alpha$. □

Let α_1, α_2 be two algebraic numbers with the same minimal polynomial $f \in \mathbb{Q}[x]$. Then for any $g \in \mathbb{Q}[x]$, $g(\alpha_1) = 0,$ if and only if $g(\alpha_2) = 0$. So, $\phi : \mathbb{Q}[\alpha_1] \longrightarrow \mathbb{Q}[\alpha_2]$ defined by

$$\sum_{i=0}^{m} a_i \alpha_1^i \longmapsto \sum_{i=0}^{m} a_i \alpha_2^i$$

is an isomorphism of $\mathbb{Q}[\alpha_1]$ onto $\mathbb{Q}[\alpha_2]$. The mapping ϕ is identity on $\mathbb{Q}$ and takes α_1 to α_2.

Conversely, let α_1 be any algebraic number with minimal polynomial f. Let ϕ be an embedding of $\mathbb{Q}[\alpha_1]$ into $\mathbb{C}$, such that $\phi(a) = a$ for every $a \in \mathbb{Q}$.

Now let $g = \sum\limits_{i=0}^{m} a_i x^i \in \mathbb{Q}[x]$ be such that $g(\alpha_1) = 0$. Hence, $\phi(g(\alpha_1)) = \phi(0) = 0$. Now, $\phi(g(\alpha_1)) = \phi(\sum\limits_{i=0}^{m} a_i \alpha_1^i) = \sum\limits_{i=0}^{m} a_i \phi(\alpha_1)^i = g(\phi(\alpha_1))$. Thus $\phi(\alpha)$ is also a zero of g.

Also, if $g(\phi(\alpha_1)) = 0$, then since ϕ is one-one, $g(\phi(\alpha_1)) = \phi(g(\alpha_1)) = 0$, implies $g(\alpha_1) = 0$. Hence, for any $g \in \mathbb{Q}[x]$, $g(\alpha_1) = 0$ if and only if $g(\phi(\alpha_1)) = 0$.

The set of all polynomials in $\mathbb{Q}[x]$ having $\phi(\alpha_1)$ as a root is precisely the ideal $\langle f \rangle$ of $\mathbb{Q}[x]$. Thus $\phi(\alpha_1)$ is an algebraic number with minimal polynomial f.

Definition 2.1. *Two algebraic numbers α_1, α_2 as above are called* ***conjugates*** *of each other, i.e., two algebraic numbers are called conjugates of each other if they are the roots of the same irreducible polynomial.*

Example 2.1. Let $\alpha = a + ib \in \mathbb{Z}[i]$, $b \neq 0$. Then the conjugate of α is the element $\alpha' = a - ib$ and both have the minimal polynomial $x^2 - 2ax + a^2 + b^2$.

Lemma 2.2. *Let K be a field of characteristic zero or a finite field, let $f \in K[x]$ be a monic irreducible polynomial of degree n. Then the n roots $x_1, \ldots, x_n$ of f are distinct.*

Proof. Let $f(x) = x^n + a_1 x^{n-1} + \cdots + a_n \in K[x]$. Let $x_1 = \alpha$ be a root of f, i.e., $\deg(\alpha) = n$ and f is its minimal polynomial. Further assume that α is a repeated root of f. Then $f'(x) = nx^{n-1} + \cdots + a_{n-1} \in K[x]$ is such that $f'(\alpha) = 0$.

Since f is the minimal polynomial of α, hence it divides any polynomial for which α is a root, i.e., $f | f'$. But $\deg(f') < \deg(f)$. This is a contradiction, provided $f' \neq 0$. This is obvious when the characteristic of the field is zero, as f is a non-constant polynomial.

Now suppose K is a finite field of characteristic p and if possible let $f' = 0$, i.e., all monomials in f have some multiples of p as their degree. So, $f(x) = g(x^p)$ for some polynomial g.

Since K is finite and of characteristic p, then $\phi : a \longmapsto a^p$ is an automorphism of K. Let L be the splitting field of f, then ϕ is also an automorphism of L. Hence, there exists $h(x)$ such that $\phi(h) = g$.

Then for $\alpha \in L$ with $f(\alpha) = 0$ also has $h(\alpha) = 0$ as $\phi(h(\alpha)) = \phi(h)\phi(\alpha) = g(\alpha^p) = f(\alpha) = 0$. Since h is of smaller degree than f, we get a contradiction to the hypothesis that f is irreducible, or equivalently f is the minimal polynomial of α. □

Theorem 2.1. *Let K be a field of characteristic zero or a finite field, let K' be an extension of finite degree n of K, and let C be an algebraically closed field containing K. Then there exists exactly n distinct K-embeddings of K' into C.*

Proof. Our assertion is true for any extension field K' of K which is of the form $K[\alpha]$ with $\alpha \in K$. In fact, the minimal polynomial m_α of α over K is then of degree n. It has n distinct roots $\alpha = x_1, x_2, \ldots, x_n$ in C.

For any $i = 1, \ldots, n$, we have then a K-embedding $\sigma_i : K' \longrightarrow C$ such that $\sigma_i(\alpha) = x_i$. These are all the embeddings because according to the discussion before Definition 2.1, if τ is an embedding different from the σ_i's, then $\tau(\alpha)$ is also a root of the minimal polynomial m_α. But m_α is of degree n and has $\alpha = x_1, x_2, \ldots, x_n$ as roots in C. Thus $\tau(\alpha) = x_i$ for some i, and therefore $\tau = \sigma_i$ for some $i = 1, 2, \ldots, n$.

We now prove the general case by induction on the degree of extension.

Let $\alpha \in K'$, $K \subset K[\alpha] \subset K'$ and put $dim_K(K[\alpha]) = q$. We may assume that $q > 1$. By the above argument, there are exactly q distinct K-embeddings $\sigma_1, \ldots, \sigma_q$ of $K[\alpha]$ into C. As $K[\sigma_i(\alpha)] \cong K[\alpha]$, it is possible to construct an extension K'_i of $K[\sigma_i(\alpha)]$ and an embedding $\tau_i : K' \longrightarrow K'_i$, which extends σ_i (result from Galois Theory).

Now, $K[\sigma_i(\alpha)]$ is a field of characteristic zero or a finite field. Note that $dim_{K[\sigma_i(\alpha)]}(K'_i) = dim_{K[\alpha]}(K') = \frac{n}{q} < n$, the induction hypothesis implies that there are exactly $\frac{n}{q}$ distinct $K[\sigma_i(\alpha)]$-embeddings θ_{ij} of K'_i into C.

Therefore the n composed mappings $\theta_{ij} \circ \tau_i$ provide $q.\frac{n}{q} = n$ K-embeddings of K' into C. They are distinct since, for $i \neq i'$, $\theta_{ij} \circ \tau_i$ and $\theta_{i'j} \circ \tau_{i'}$ differ on $K[\alpha]$. While, for $i = i'$ but $j \neq j'$, θ_{ij} and $\theta_{ij'}$ differ on K'_i.

Now for any K-embeddings of K' into C, by taking its restriction to $K[\alpha]$, we can see that all possible embeddings appear in this way. Hence this completes the proof. □

Theorem 2.2. ***(theorem of the primitive element)*** *Let K be a number field of degree n. Then there exists an element $\theta \in K$ (called a* ***primitive element****) such that $K = \mathbb{Q}[\theta]$.*

Proof. Since every algebraic extension of a field of characteristic zero is separable, the number field K is separable over $\mathbb{Q}$. Since $dim_{\mathbb{Q}}(K) = n < \infty$, then K over $\mathbb{Q}$ has finitely many intermediate fields, by considering the normal closure of K and using the fundamental theorem of Galois theory.

Now, let $\{\alpha_1 \ldots, \alpha_n\}$ be a basis of K over $\mathbb{Q}$, then $K = \mathbb{Q}(\alpha_1, \ldots, \alpha_n)$. So if we can show that any field extension generated by two elements is also generated by one element, we will be done.

Suppose $\alpha, \beta \in K$. As $c \in \mathbb{Q}$ varies, $\mathbb{Q}[\alpha + c\beta]$ varies over finitely many intermediate subfields of K over $\mathbb{Q}$. Hence, there are $c_1 \neq c_2 \in \mathbb{Q}$ such that $\mathbb{Q}[\alpha + c_1\beta] = \mathbb{Q}[\alpha + c_2\beta] := L$. Thus, $(c_1 - c_2)\beta \in L$. Therefore $\beta \in L$. Hence $\alpha \in L$.

Thus, $\mathbb{Q}(\alpha, \beta) = \mathbb{Q}[\alpha + c_1\beta]$.

We proceed inductively to show that $K = \mathbb{Q}(\alpha_1, \ldots, \alpha_n) = \mathbb{Q}(\alpha_1 + c_2\alpha_2 + \cdots + c_n\alpha_n)$ for some $c_i \in \mathbb{Q}$. □

Let K be an algebraic number field of degree n and $\sigma_1, \ldots, \sigma_n$ the n distinct embeddings of K into $\mathbb{C}$. Let $\sigma_i(K) = K^{(i)}$ and for $\alpha \in K, \sigma_i(\alpha) = \alpha^{(i)}$. The fields $K^{(1)}, \ldots, K^{(n)}$, called **conjugate fields of** K into $\mathbb{C}$, and are again number fields of degree n.

If $K^{(i)} \subset \mathbb{R}$ then we call σ_i a *real embedding* and if $K^{(i)} \not\subset \mathbb{R}$ then we call σ_i a *complex embedding.*

Remark 2.1. Complex embeddings of a number field K occur in pairs. For this, let K be a number field of degree n. By Corollary 2.2, there exists $\theta \in K$ such that $K = \mathbb{Q}[\theta]$. Let σ_i be an embedding of K into $\mathbb{C}$ such that $\sigma_i(K) \not\subset \mathbb{R}$. Since $\sigma_i(\mathbb{Q}) = \mathbb{Q}$ and $\sigma_i(\mathbb{Q}[\theta]) \not\subset \mathbb{R}$, implies $\sigma_i(\theta) = \beta \notin \mathbb{R}$. Now, $\beta = \theta_i$ for some $1 \leq i \leq n$, where $\theta_i = \sigma_i(\theta)$. Since β is a root of m_θ, then $\bar{\beta}$ is also a root of m_θ. This implies that there exists $\bar{\sigma_i}$, an embedding of K into $\mathbb{C}$, such that $\bar{\sigma_i}(\theta) = \bar{\beta}$. Since $\sigma_j, 1 \leq j \leq n$ are all the distinct isomorphisms, we get that $\bar{\sigma_i} = \sigma_j$ for some $1 \leq j \leq n$. Hence, $\bar{\sigma_i}(K) = K^{(j)}$ for some $1 \leq j \leq n$.

Let r_1 be the number of real embeddings of K and let s denote the number of complex embeddings of K. Hence $n = r_1 + s = r_1 + 2r_2$ for some $r_2 \in \mathbb{Z}_{\geq 0}$.

2.2 Norm and trace

Let K be an algebraic number field of degree n and $\{w_1, w_2, \ldots, w_n\}$ be a base of K over $\mathbb{Q}$. For any $\alpha \in K$, let $T_\alpha : K \longrightarrow K, x \longmapsto \alpha \cdot x$ be a linear map of vector spaces over $\mathbb{Q}$.

Definition 2.2. *For any $\alpha \in K$, define **trace** of α to be the trace of the linear operator T_α and denote it by $Tr_K(\alpha)$. Likewise, define **norm** of α to be the determinant of the operator T_α and denote it by $N_K(\alpha)$.*

Since $\alpha, w_j \in K$, $\alpha w_j \in K$. So $\alpha w_j = \sum\limits_{i=1}^{n} a_{ij} w_i$, for every $1 \leq j \leq n$ and $a_{ij} \in \mathbb{Q}$. Let $A_\alpha = (a_{ij})$. Then $Tr_K(\alpha) = Tr(A_\alpha)$ and $N_K(\alpha) = det(A_\alpha)$. Hence, $Tr_K(\alpha), N_K(\alpha) \in \mathbb{Q}$.

For $\alpha \in K$, $(\alpha w_j)^{(k)} = \sigma_k(\alpha w_j) = \sigma_k(\alpha)\sigma_k(w_j) = \sigma_k(\sum\limits_{i=1}^{n} a_{ij} w_i) = \sum\limits_{i=1}^{n} a_{ij} w_i^{(k)}$, for every j.

Let $\Omega = (w_j^{(k)})_{k,j} \in \mathcal{M}_n(\mathbb{C})$ with $(w_1^{(k)}, \ldots, w_n^{(k)})$ as its k^{th}-row. We know from Corollary 2.2 that there exists $\theta \in K$ such that $K = \mathbb{Q}[\theta]$. So,

$$\Omega = \begin{pmatrix} w_1^{(1)} & w_2^{(1)} & \cdots & w_n^{(1)} \\ w_1^{(2)} & w_2^{(2)} & \cdots & w_n^{(2)} \\ \vdots & \vdots & \ddots & \vdots \\ w_1^{(n)} & w_2^{(n)} & \cdots & w_n^{(n)} \end{pmatrix} = \begin{pmatrix} 1 & \theta^{(1)} & (\theta^{(1)})^2 & \cdots & (\theta^{(1)})^{n-1} \\ 1 & \theta^{(2)} & (\theta^{(2)})^2 & \cdots & (\theta^{(2)})^{n-1} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 1 & \theta^{(n)} & (\theta^{(n)})^2 & \cdots & (\theta^{(n)})^{n-1} \end{pmatrix}$$

Now, Ω is a Vandermonde matrix. Then $\det \Omega = \prod\limits_{1 \leq i < j \leq n} (\theta^{(j)} - \theta^{(i)})$. Since $i \neq j$, implies $\theta^{(i)} \neq \theta^{(j)}$. Hence $\det(\Omega) \neq 0$ and Ω is invertible.

Let

$$A_0 = (\alpha^{(i)}\delta_{ij}) = \begin{pmatrix} \alpha^{(1)} & 0 & \cdots & 0 \\ 0 & \alpha^{(2)} & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & \alpha^{(n)} \end{pmatrix}$$

Then we have $A_0\Omega = \Omega A_\alpha$. Since Ω is invertible in $\mathcal{M}_n(\mathbb{C})$, $A_0 = \Omega A_\alpha \Omega^{-1}$. Hence, A_α and A_0 are similar matrices.

Thus, $N_K(\alpha) = det(A_\alpha) = det(A_0) = \prod\limits_{i=1}^{n} \alpha^{(i)}$ and

$Tr_K(\alpha) = Tr(A_\alpha) = Tr(A_0) = \sum\limits_{i=1}^{n} \alpha^{(i)}$.

If A_α corresponds to $\alpha \in K$ and A_β to $\beta \in K$, then $A_\alpha + A_\beta$ corresponds to $\alpha + \beta$ and $A_\alpha A_\beta$ corresponds to $\alpha\beta$.

Proposition 2.1. *Let K be a number field of degree n and $\sigma : K \longrightarrow \mathbb{C}$ varies over different embeddings of K into $\mathbb{C}$, then we have*

(i)$Tr_K(x) = \sum\limits_{\sigma} \sigma(x)$,

(ii)$N_K(x) = \prod\limits_{\sigma} \sigma(x)$.

The proof of this proposition is clear from the discussions of this section.

The trace and norm in a tower of fields satisfies the following:

Corollary 2.1. *(Transitivity of trace and norm) In a tower of finite field extensions $\mathbb{Q} \subset K \subset L$, one has*

$$Tr_{K/\mathbb{Q}} \circ Tr_{L/K} = Tr_{L/\mathbb{Q}}; \; N_{K/\mathbb{Q}} \circ N_{L/K} = N_{L/\mathbb{Q}}.$$

Proof. Let $m = dim_K(L)$ and $d = dim_{\mathbb{Q}}(K)$, as in the field diagram below.

$$\begin{tikzcd}
L \\
K \arrow[u, hook] \\
\mathbb{Q} \arrow[u, hook]
\end{tikzcd}$$

To prove the transitivity of trace, let $\{e_1, \ldots, e_m\}$ be a K-base of L and $\{f_1, \ldots, f_d\}$ be a $\mathbb{Q}$-base of K. Then a $\mathbb{Q}$-base of L is

$$\{e_i f_j \big| \; 1 \leq i \leq m; \; 1 \leq j \leq d\}$$

For $\alpha \in L$, let

$$\alpha e_j = \sum_{i=1}^{m} c_{ij} e_i, \; c_{ij} f_s = \sum_{r=1}^{d} (b_{ij})_{rs} f_r,$$

for $c_{ij} \in K$ and $(b_{ij})_{rs} \in \mathbb{Q}$. Thus, $\alpha(e_j f_s) = \sum\limits_i \sum\limits_r (b_{ij})_{rs} e_i f_r$. Using the above bases for L over K, K over $\mathbb{Q}$ and L over $\mathbb{Q}$, we have the following matrices

$$[A_\alpha]_{L/K} = (c_{ij}),\ [A_\alpha]_{K/\mathbb{Q}} = ((b_{ij})_{rs}),\ [A_\alpha]_{L/\mathbb{Q}} = ([A_\alpha]_{K/\mathbb{Q}}),$$

where the field extension in the subscript indicates what extension is being used for that matrix. Also, the last matrix is a block matrix. Using these matrices,

$$Tr_{K/\mathbb{Q}}(Tr_{L/K}(\alpha)) = Tr_{K/\mathbb{Q}}(\sum_i c_{ii}) = \sum_i Tr_{K/\mathbb{Q}}(c_{ii})$$

$$= \sum_i \sum_r (b_{ii})_{rr} = Tr_{L/\mathbb{Q}}(\alpha).$$

A similar calculation holds for the norm. □

Regular representation of K with respect to the base $\{w_1, \dots, w_n\}$ of K is the map $\phi : K \longrightarrow \mathcal{M}_n(\mathbb{Q})$, which takes $\alpha \longmapsto A_\alpha$. ϕ is a homomorphism of rings. If $\alpha, \beta \in K$, then $Tr_K(\alpha + \beta) = Tr_K(\alpha) + Tr_K(\beta)$ and $N_K(\alpha\beta) = N_K(\alpha)N_K(\beta)$.

Let $\alpha \in K$ be an algebraic number and $m_\alpha = x^m + a_1 x^{m-1} + \cdots + a_m \in \mathbb{Q}[x]$ be the minimal polynomial of α. Now, α is of degree m, and $\mathbb{Q}[\alpha]$ has $\{1, \alpha, \dots, \alpha^{m-1}\}$ as a base over $\mathbb{Q}$.

Let $A_\alpha \in \mathcal{M}_m(\mathbb{Q})$ correspond to α in the regular representation of $\mathbb{Q}[\alpha]$ with respect to the base $\{1, \alpha, \dots, \alpha^{m-1}\}$ of $\mathbb{Q}[\alpha]$ over $\mathbb{Q}$. Let $\{\beta_1, \dots, \beta_l\}$ be a base of K considered as a vector space over $\mathbb{Q}[\alpha]$.

An elaboration of the above corollary in the case of $\mathbb{Q} \subset \mathbb{Q}[\alpha] \subset K$ can be seen as below.

$dim_{\mathbb{Q}}(K) = dim_{\mathbb{Q}[\alpha]}(K) \cdot dim_{\mathbb{Q}}(\mathbb{Q}[\alpha]) = l \cdot m = n$. Then $\{\beta_i \alpha_j \mid 1 \leq j \leq m; 1 \leq i \leq n\}$ forms a base for K over $\mathbb{Q}$. Let B_α correspond to α in the regular representation of K with respect to this $\mathbb{Q}$-base. Then,

$$B_\alpha = \begin{pmatrix} A_\alpha & 0 & \cdots & 0 \\ 0 & A_\alpha & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & A_\alpha \end{pmatrix} \in \mathcal{M}_n(\mathbb{Q})$$

So, $Tr_K(B_\alpha) = l \cdot Tr(A_\alpha)$ and $N_K(\alpha) = det(B_\alpha) = det(A_\alpha)^l$. Also each A_α is a $m \times m$ matrix as $\deg(\alpha) = m$. So, the matrix A_α gets repeated l many times, where $dim_{\mathbb{Q}[\alpha]}(K) = l$.

Now suppose, α is an algebraic integer,then $m_\alpha = x^m + a_1x^{m-1} + \cdots + a_m \in \mathbb{Z}[x]$ is the minimal polynomial of α. Hence, the matrix of endomorphism $T_\alpha : \mathbb{Q}[\alpha] \longrightarrow \mathbb{Q}[\alpha]$ is,

$$A_\alpha = \begin{pmatrix} 0 & 0 & \cdots & 0 & -a_m \\ 1 & 0 & \cdots & 0 & -a_{m-1} \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & \cdots & 1 & -a_1 \end{pmatrix}_{m\times m}$$

Hence, all the elements of A_α are in $\mathbb{Z}$, hence $Tr(A_\alpha)$ and $Tr(B_\alpha) = l.Tr(A_\alpha) = l \cdot a_1$ are integers. Thus for an algebraic integer $\alpha \in K$, $Tr_K(\alpha) \in \mathbb{Z}$. Similarly, $N_K(\alpha) = det(B_\alpha) = det(A_\alpha)^l \in \mathbb{Z}$.

Let $\theta \in K$ be a primitive element. Then in the matrix,

$$\Omega = \begin{pmatrix} 1 & \theta^{(1)} & (\theta^{(1)})^2 & \cdots & (\theta^{(1)})^{n-1} \\ 1 & \theta^{(2)} & (\theta^{(2)})^2 & \cdots & (\theta^{(2)})^{n-1} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 1 & \theta^{(n)} & (\theta^{(n)})^2 & \cdots & (\theta^{(n)})^{n-1} \end{pmatrix}$$

the first row is $\{1, \theta, \ldots, \theta^{n-1}\}$, which is a base for K over $\mathbb{Q}$. Similarly, $\{1, \theta^{(2)}, \ldots, (\theta^{(2)})^{n-1}\}$ is a base for $\sigma_2(K) = K^{(2)}$ over $\mathbb{Q}$, and the i^{th}-row of Ω is a base for $K^{(i)}$ over $\mathbb{Q}$.

Example 2.2. Let $K = \mathbb{Q}[\alpha]$, where $\alpha = \sqrt{2}$. Then $m_\alpha = x^2 - 2 \in \mathbb{Z}[x]$ and $\{1, \sqrt{2}\}$ is a base for K over $\mathbb{Q}$.

Under the endomorphism $T_\alpha : \mathbb{Q}[\alpha] \longrightarrow \mathbb{Q}[\alpha]$, $1 \longmapsto \sqrt{2}$ and $\sqrt{2} \longmapsto 2$. Thus,

$$A_\alpha = \begin{pmatrix} 0 & 2 \\ 1 & 0 \end{pmatrix}$$

Hence, $Tr_K(\alpha) = Tr(A_\alpha) = 0$ and $N_K(\alpha) = det(A_\alpha) = -2$.

Example 2.3. Let $K = \mathbb{Q}[\sqrt{2}, \sqrt{3}]$ and let $\alpha = \sqrt{2}$. Then, $\{1, \sqrt{2}, \sqrt{3}, \sqrt{6}\}$ forms a base for K over $\mathbb{Q}$. Under the endomorphism T_α, $1 \longmapsto \sqrt{2}$; $\sqrt{2} \longmapsto$

2; $\sqrt{3} \longmapsto \sqrt{6}$ and $\sqrt{6} \longmapsto 2\sqrt{3}$. Then,

$$A_\alpha = \begin{pmatrix} 0 & 2 \\ 1 & 0 \end{pmatrix} \text{ and } B_\alpha = \begin{pmatrix} A_\alpha & 0 \\ 0 & A_\alpha \end{pmatrix} = \begin{pmatrix} 0 & 2 & 0 & 0 \\ 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 2 \\ 0 & 0 & 1 & 0 \end{pmatrix}$$

Hence, $Tr_K(\alpha) = Tr(B_\alpha) = 2.Tr(A_\alpha) = 0$ and $N_K(\alpha) = det(B_\alpha) = det(A_\alpha)^2$ $= (-2)^2 = 4$.

For any $a \in \mathbb{Q}$ and $\alpha \in K$, $Tr_K(a \cdot \alpha) = a \cdot Tr_K(\alpha)$; $Tr_K(a) = n \cdot a$; $N_K(a) = a^n$ and $N_K(a \cdot \alpha) = a^n \cdot N_K(\alpha)$.

2.3 Integral base

Before defining an integral base of $\mathcal{O}_K$, we need a few results from linear algebra on bilinear forms.

Definition 2.3. *Let V be a vector space over a field K. By a **K-linear form** or simply a linear form on V, we mean a linear transformation from V to K.*

Definition 2.4. *Let V be a vector space over a field K. A **bilinear form** B on V is a mapping $B : V \times V \longrightarrow K$ such that for any fixed $y \in V$, the mappings B'_y, B''_y of V into K, defined by $B'_y(x) = B(x,y)$ and $B''_y(x) = B(y,x)$ respectively, are linear forms on V.*

Definition 2.5. *A bilinear form $B(x,y)$ on V is **non-degenerate** if, for any fixed $y \neq 0 \in V$, the linear form $B'_y \neq 0$, i.e., $B'_y(x) = B(x,y) \neq 0$ for some x; and also the linear form $B''_y \neq 0$.*

Let K be a number field of degree n and let $\alpha \in K$. The mapping $\alpha \longmapsto Tr_K(\alpha)$ is a $\mathbb{Q}$-linear mapping of K into $\mathbb{Q}$. Define a bilinear form $B(x,y) = Tr_K(xy)$ for any $x, y \in K$, on the $\mathbb{Q}$-vector space K.

Proposition 2.2. *The bilinear form $B(x,y) = Tr_K(xy)$ for $x, y \in K$ is non-degenerate.*

Proof. Let $x \neq 0 \in K$. Then $B''_x(y) = B(y,x) = Tr_K(xy) \neq 0$ as for $y = x^{-1}$, $B''_x(y) = Tr_K(xy) = Tr_K(1) = n$. Similarly, $B'_x(y) = B(x,y) \neq 0$. □

Let V be a vector space of dimension n over a field K. Then we have

Proposition 2.3. *Let $B(x,y)$ be a non-degenerate bilinear form on V. Then for any base $\alpha_1, \alpha_2, \ldots, \alpha_n$ of V, there exists a base $\beta_1, \ldots, \beta_n$ of V such that $B(\alpha_i, \beta_j) = \delta_{ij}$ for $1 \leq i,j \leq n$, where δ_{ij} denotes the Kronecker delta function.*

The proof of this proposition uses the dual space V^* of the vector space V and Noether's homomorphism theorem to come up with a dual base.

Noether's homomorphism theorem states that, for $f : R \longrightarrow S$, be a surjective ring homomorphism, the following diagram is commutative:

$$\begin{tikzcd}
R \arrow[rr, "f"] \arrow[dr, "g"'] & & S \\
& R/Kerf \arrow[ur, "\cong"'] &
\end{tikzcd}$$

where $g : R \longrightarrow R/Kerf$ is the usual map.

Proposition 2.4. *Let M be a finitely-generated $\mathbb{Z}$-module and let $\alpha_1, \alpha_2, \ldots,$ α_n be a system of generators of $\mathbb{Z}$-module M. Let N be a submodule of M. Then, there exist $\beta_1, \beta_2, \ldots, \beta_m$, $(m \leq n)$ in N that generate N over $\mathbb{Z}$ and have the following form,*

$$\beta_i = \sum_{i \leq j} k_{ij}\alpha_j$$

with $k_{ij} \in \mathbb{Z}$; $k_{ii} \geq 0$ and $1 \leq i \leq m$.

The proof of this proposition is by induction on the rank n of M as a $\mathbb{Z}$-module. The implication of this proposition will prove crucial in finding an integral base and the norm of an ideal.

Now, let K be a number field of degree n.

Corollary 2.2. *For any $\mathbb{Q}$-base $w_1, w_2, \ldots, w_n$ of K, there exists a base $w'_1, w'_2, \ldots, w'_n$ of K such that $Tr_K(w_i, w'_j) = \delta_{ij}$.*

Theorem 2.3. *Let K a number field of degree n and $\mathcal{O}_K$ be the ring of algebraic integers in K. Then there exist a $\mathbb{Q}$-base $\beta_1, \cdots, \beta_n$ of K such that $\beta_i \in \mathcal{O}_K$ and $\mathcal{O}_K = \mathbb{Z}\beta_1 + \mathbb{Z}\beta_2 + \cdots + \mathbb{Z}\beta_n$.*

Proof. Let $w_1, w_2, \cdots, w_n$ be a $\mathbb{Q}$-base of K. Then there exists $m \neq 0 \in \mathbb{Z}$ such that $mw_1, mw_2, \cdots, mw_n \in \mathcal{O}_K$.

So without loss of generality, we can assume that $w_1, w_2, \cdots, w_n \in \mathcal{O}_K$.

Let $w'_1, w'_2, \ldots, w'_n$ of K for which $Tr_K(w_i, w'_j) = \delta_{ij}$ for all i, j. We know, for any $z \in \mathcal{O}_K$, $z = \sum_{i=1}^{n} a_i w'_j$, where $a_i \in \mathbb{Q}$.

Since $zw_i \in \mathcal{O}_K$,the $Tr_K(zw_i) \in \mathbb{Z}$. Hence, $Tr_K(zw_i) = a_i \in \mathbb{Z}$. Thus, $\mathcal{O}_K \subset \mathbb{Z}w'_1 + \mathbb{Z}w'_2 + \cdots + \mathbb{Z}w'_n$. By the previous proposition, there exist $\beta_1, \beta_2, \ldots, \beta_m \in \mathcal{O}_K$, $(m \leq n)$; such that $\mathcal{O}_K = \mathbb{Z}\beta_1 + \cdots + \mathbb{Z}\beta_m$.

Claim : $m = n$

Proof : The $\mathbb{Q}$-linear span, $L_{\mathbb{Q}}(\beta_1, \beta_2, \ldots, \beta_m) \subset K$. Also, any $\alpha \in K$ is of the form $\alpha = \sum_{i=1}^{n} b_i w_i$, where $b_i \in \mathbb{Q}$. But each $w_i \in \mathcal{O}_K$ and thus can be written as a $\mathbb{Z}$-linear combination of β_i's.

Hence, $K \subset L_{\mathbb{Q}}(\beta_1, \beta_2, \ldots, \beta_m)$. This implies, $n = dim_{\mathbb{Q}}(K) \leq m \leq n$. Hence, $m = n$. Also, $\beta_1, \beta_2, \ldots, \beta_n$ are $\mathbb{Q}$-linearly independent and thus, the sum $\mathcal{O}_K = \mathbb{Z}\beta_1 + \cdots + \mathbb{Z}\beta_n$, is a direct sum.

Further, any set of elements $\beta_1, \beta_2, \ldots, \beta_n$ as above, forms a $\mathbb{Q}$-base of K. □

Definition 2.6. *The set $\{\beta_1, \beta_2, \cdots, \beta_n\}$, with $\beta_1, \beta_2, \cdots, \beta_n$ as above are said to be an* ***integral base*** *of $\mathcal{O}_K$.*

Example 2.4. Referring to Theorem 1.2, let K be a quadratic field and let $\mathcal{O}_K$ be its ring of integers. Then

$$\mathcal{O}_K = \begin{cases} \mathbb{Z} + \mathbb{Z}\left(\frac{1+\sqrt{m}}{2}\right), & \text{if } m \equiv 1 \pmod 4 \\ \mathbb{Z} + \mathbb{Z}(\sqrt{m}), & \text{if } m \equiv 2, 3 \pmod 4 \end{cases}$$

The $\{1, \frac{1+\sqrt{m}}{2}\}$ and $\{1, \sqrt{m}\}$ forms an integral base for $K = \mathbb{Q}[\sqrt{m}]$ when $m \equiv 1 \pmod 4$ and $m \equiv 2, 3 \pmod 4$, respectively.

Definition 2.7. *Any ideal I of the ring of integers $\mathcal{O}_K$ of a number field K is called an* ***integral ideal****.*

Remark 2.2. Let I be any non-zero integral ideal in K. Then $I \cap \mathbb{Z} \neq \{0\}$.

Proof. If $\alpha \neq 0 \in I$ and if $\alpha^r + a_1\alpha^{r-1} + \cdots + a_r = 0$, where $a_i \in \mathbb{Z}$ and $a_r \neq 0$, because for any $\alpha \in \mathcal{O}_K$, the minimal polynomial m_α of α always has a constant term. Then $a_r = -\alpha(a_{r-1} + \cdots + \alpha^{r-1}) \in \mathbb{Z}$. Thus, for any $\alpha \in K$, there exists $a \neq 0 \in \mathbb{Z}$ such that $a \cdot \alpha \in I$. □

If $\beta_1, \beta_2, \ldots, \beta_n$ are as in the theorem, then Proposition 2.4 tells us that for any integral ideal I, there exist $\alpha_1, \alpha_2, \ldots, \alpha_m \in I$, $(m \leq n)$; such that $I = \mathbb{Z}\alpha_1 + \cdots + \mathbb{Z}\alpha_m$. As in the Theorem 2.3, we must have $m = n$. The α_i are said to be an *integral base of I*. Further, we may choose the α_i so that $\alpha_i = \sum\limits_{j \geq i} p_{ij}\beta_j$, where $p_{ij} \in \mathbb{Z}$.

Remark 2.3. As in the Theorem 2.3, any elements $\alpha_1, \alpha_2, \ldots, \alpha_n$ such that $I = \mathbb{Z}\alpha_1 + \cdots + \mathbb{Z}\alpha_n$, form a $\mathbb{Q}$-base of K. In particular, any non-zero ideal of I contains n elements which are linearly independent over $\mathbb{Q}$. Also if $\alpha_i = \sum\limits_{j \geq i} p_{ij}\beta_j$, then $p_{ii} \neq 0$. Let $P = (p_{ij})$. This forms the change of basis matrix. Any any change of basis matrix is invertible, which implies $p_{ii} \neq 0$ and hence without loss of generality can be taken to be > 0.

Remark 2.4. If $I \neq \{0\}$ is an ideal of $\mathcal{O}_K$, then there exists a non-zero $a \in \mathbb{Z}$ such that $a\mathcal{O}_K \subset I \subset \mathcal{O}_K$. Now if, $\mathcal{O}_K = \mathbb{Z}\beta_1 + \cdots + \mathbb{Z}\beta_n$, then $a\mathcal{O}_K = \mathbb{Z}a\beta_1 + \cdots + \mathbb{Z}a\beta_n$ so that $\frac{\mathcal{O}_K}{a\mathcal{O}_K}$ is of order a^n. Therefore, $\frac{\mathcal{O}_K}{I}$ is finite.

The a in this remark is an uniform a for the whole of $\mathcal{O}_K$. To find this a, consider the β_i as above. Now for each i, there exists $m_i \neq 0 \in \mathbb{Z}$ such that $m_i\beta_i \in I$. Since, $\mathcal{O}_K = \mathbb{Z}\beta_1 + \cdots + \mathbb{Z}\beta_n$, then for any $\alpha \in \mathcal{O}_K$, $a = \prod\limits_{i=1}^{n} m_i \neq 0$ is such that $a\alpha \in I$, i.e., $a\mathcal{O}_K \subset I \subset \mathcal{O}_K$.

Also, consider only $\mathbb{Z}\beta_1$ and $\mathbb{Z}a\beta_1$. Now for any $k \in \frac{\mathbb{Z}\beta_1}{\mathbb{Z}a\beta_1}$ means there exists $0 \leq l < a$ such that $k = l\beta_1 + \mathbb{Z}a\beta_1$, implies l has a choices. Hence, $\left|\frac{\mathcal{O}_K}{a\mathcal{O}_K}\right| = a^n$.

Remark 2.5. If J is a prime ideal in $\mathcal{O}_K$, then J contains exactly one prime number $p > 0$ of $\mathbb{Z}$. For this let $a = p_1p_2 \dots p_k$ in $J \cap \mathbb{Z}$ with primes $p_1, \dots, p_k \in \mathbb{Z}$. Since J is a prime ideal, at least one $p_i \in J$. If p, q are distinct primes in J, then by Bezout's identity, there exists $x, y \in \mathbb{Z}$ such that $px + qy = 1 \in J$, which implies $J = \mathcal{O}_K$. This is a contradiction to the choice of J.

2.4 Discriminant

Before we define the discriminant of a number field, we'll define it for the general case of rings.

Let B be a ring and let A be a subring of B such that B is a free A-module of finite rank n (for example, A can be a field and B a finite extension of degree n of A). For $x \in B$, multiplication T_x by x, (i.e., $y \mapsto xy$) is an endomorphism of the A-module B.

We call *trace* (respectively, *norm*) of $x \in B$, relative to B and A, the trace (respectively, determinant) of the endomorphism T_x of multiplication by x.

The *trace* (respectively, *norm*) of x is denoted by $Tr_{B/A}(x)$. They are elements of A.

Definition 2.8. *Let B be a ring and let A be a subring of B such that B is a free A-module of finite rank n. For $\{x_1, x_2, \dots, x_n\} \subset B$ be any set of n elements in B. We call $D(x_1, x_2, \dots, x_n) = det(Tr_{B/A}(x_ix_j)) \in A$ as the **discriminant of** $\{x_1, x_2, \dots, x_n\}$.*

Proposition 2.5. *If $\{y_1, y_2, \dots, y_n\} \subset B$ is another set of elements of B such that $y_i = \sum\limits_{j=1}^{n} a_{ij}x_j$ with $a_{ij} \in A$, then*

$$D(y_1, y_2, \dots, y_n) = (det(a_{ij}))^2 D(x_1, x_2, \dots, x_n).$$

Proof. $Tr(y_py_q) = Tr(\sum\limits_i a_{pi}x_i \sum\limits_j a_{qj}x_j) = Tr(\sum\limits_i \sum\limits_j a_{pi}a_{qj}x_iy_j)$

$= \sum\limits_{i,j} a_{pi}a_{qj}Tr(x_ix_j)$, since trace is a linear map.

So, the matrix equation is

$$(Tr(y_py_q))_{n\times n} = (a_{pi})_{n\times n}(Tr(x_ix_j))_{n\times n}{(a_{qj})^T}_{n\times n}$$

Applying *det* on the above matrix equation,

$$D(y_1, y_2, \dots, y_n) = det(A.Tr(x_i x_j).A^T) = (detA)^2.D(x_1, x_2, \dots, x_n).$$

□

Proposition 2.5 implies that the matrix (a_{ij}) which expresses one base in terms of another, has an inverse with entries in A. Therefore, both $det(a_{ij})$ and $det(a_{ij})^{-1}$ are units in A.

Definition 2.9. *Let B be a ring and let A be a subring of B such that B is a free A-module of finite rank n. Define* ***discriminant of B over A*** *as,*

$$\mathscr{D}_{B/A} := \textit{principal ideal generated by discriminant of any base of } B \textit{ over } A.$$

Proposition 2.6. *Suppose that $\mathscr{D}_{B/A}$ contains an element which is not a zero-divisor. Then, $\{x_1, \dots, x_n\} \subset B$ is a base for B over A if and only if $D(x_1, \dots, x_n)$ generates $\mathscr{D}_{B/A}$.*

Proof. (⇒:) By definition of $\mathscr{D}_{B/A}$.

(:⇐) Let $\{x_1, x_2, \dots, x_n\} \subset B$, $d = D(x_1, x_2, \dots, x_n)$ be such that $\mathscr{D}_{B/A} = D(x_1, x_2, \dots, x_n) \cdot A = d \cdot A$. Let $\{e_1, e_2, \dots, e_n\}$ be a base of B over A. Put $d' = D(e_1, e_2, \dots, e_n)$ and $x_i = \sum\limits_{j=1}^{n} a_{ij} e_j$ with $a_{ij} \in A$ for every i, j.

Then, $d = (det(a_{ij}))^2 \cdot d'$ by Proposition 2.5. By hypothesis, $d \cdot A = \mathscr{D}_{B/A} = d' \cdot A$, which implies there exists a non-zero $b \in A$ such that $d' = b \cdot d$.

Thus, $d(1 - b(det(a_{ij}))^2 = 0$. We know that d is not a zero-divisor, since otherwise every element of $d \cdot A = \mathscr{D}_{B/A}$ will be a zero-divisor.

Hence, $1 - b.det(a_{ij})^2 = 0$, which implies $det(a_{ij})^2 = \frac{1}{b} \neq 0$.

If $det(a_{ij}) = k$, then $k^2 = \frac{1}{b}$ and $k^2, b \in A$ are units, implying k is also an unit in A, i.e., $det(a_{ij})$ is invertible in A. Consequently, $\{x_1, x_2, \dots, x_n\}$ is a base for B over A. □

Lemma 2.3. *(lemma of Dedekind) Let G be a group, C a field, and let $\sigma_1, \dots, \sigma_n$ be distinct homomorphisms of G into the multiplicative group C^*. Then the σ_i's are linearly independent over C, i.e., $\sum u_i \sigma_i(g) = 0$ for every $g \in G$ implies that $u_i = 0$ for every i.*

Proof. Suppose that the σ_i's are linearly dependent. Consider a non-trivial relation $\sum\limits_i u_i\sigma_i = 0$ and $u_i \in C$, such that the number q of the u_i's which are non-zero, is minimum. This means that any zero linear combination of σ_i's with less than q summands will have all the coefficients equal to zero.

After renumbering, we may suppose that

$$u_1\sigma_1(g) + u_2\sigma_2(g) + \cdots + u_q\sigma_q(g) = 0, \text{for every } g \in G. \tag{2.1}$$

We have $q \geq 2$ since the σ_i's are not zero. For $g, h \in G$, we see that

$$u_1\sigma_1(hg) + u_2\sigma_2(hg) + \cdots + u_q\sigma_q(hg) \tag{2.2}$$

$$= u_1\sigma_1(h)\sigma_1(g) + u_2\sigma_2(h)\sigma_2(g) + \cdots + u_q\sigma_q(h)\sigma_q(g) = 0.$$

Multiplying equation (2.1) by $\sigma_1(h)$ and subtracting from equation (2.2) it follows that

$$u_2(\sigma_1(h) - \sigma_2(h))\sigma_2(g) + \cdots + u_q(\sigma_1(h) - \sigma_q(h))\sigma_q(g) = 0.$$

This holds for every $g \in G$ and since q has been chosen as small as possible, we get that

$$u_2(\sigma_1(h) - \sigma_2(h)) = 0; \text{which implies } \sigma_1(h) = \sigma_2(h); \text{for every } h \in G.$$

But this contradicts the fact that σ_i's are all distinct. □

Proposition 2.7. *Let K be a number field of degree n and let $\sigma_1, \sigma_2 \ldots, \sigma_n$ be the n distinct embeddings of K into $\mathbb{C}$. Then, if $\{x_1, \ldots, x_n\}$ is a base for K over $\mathbb{Q}$, then*

$$D(x_1, \ldots, x_n) = det(\sigma_i(x_j))^2 \neq 0.$$

Proof. $D(x_1, \ldots, x_n) = det(Tr(x_ix_j)) = det(\sum\limits_k \sigma_k(x_ix_j)) = det(\sum\limits_k \sigma_k(x_i)\sigma_k(x_j))$

$= det(BB^T) = det(B) \cdot det(B^T) = det(B)^2 = det(\sigma_k(x_i))^2$, where

$B = (\sigma_k(x_i))_{n\times n}$.

It remains to show that $det(B) \neq 0$.

Suppose that $det(B) = 0$. Let T_B be the linear transformation associated to the matrix B. Then T_B is not injective, i.e., the $Nullity(T_B) > 0$. Hence, there exists a non-trivial vector $u = (u_1, u_2, \ldots, u_n) \in \mathbb{C}^n$ such that $B \cdot u = 0$, i.e., $\sum\limits_{i=1}^{n} u_i\sigma_i(x_j) = 0$, for every j.

By linearity, $\sum\limits_{i=1}^{n} u_i\sigma_i(x) = 0$ for every $x \in K$. This contradicts the *lemma of Dedekind.*

□

2.4.1 Discriminant of quadratic fields

Let K be a quadratic number field and let $\mathcal{O}_K$ be its ring of integers.

Definition 2.10. *Let I be an integral ideal and $\{\alpha_1, \alpha_2\}$ be an integral base of I. Define **discriminant of I** $= \triangle(I) = \triangle(\alpha_1, \alpha_2) = (\alpha_1\alpha_2' - \alpha_1'\alpha_2)^2$, i.e., the square of the det$\left(\begin{smallmatrix} \alpha_1 & \alpha_2 \\ \alpha_1' & \alpha_2' \end{smallmatrix}\right)$.*

From the first proposition of previous section, it is clear that the above definition is independent of integral base.

If $I = \mathcal{O}_K$, we write $d = d_K = \triangle(\mathcal{O}_K)$ and call it the *discriminant* of the field $K = \mathbb{Q}[\sqrt{m}]$. Then,

$$d_K = \begin{cases} m, & \text{if } m \equiv 1 \pmod 4 \\ 4m, & \text{if } m \equiv 2, 3 \pmod 4 \end{cases}$$

Proposition 2.8. *For a quadratic field K with discriminant d, we have $K = \mathbb{Q}[\sqrt{d}]$ and further $\{1, \frac{d+\sqrt{d}}{2}\}$ is an integral base of the ring $\mathcal{O}_K$ of algebraic integers in K.*

The proof of this proposition is immediate from the calculations of Theorem 1.2.

Corollary 2.3. *The discriminant uniquely determines a quadratic field.*

2.5 Cyclotomic fields

Definition 2.11. *Any number field generated over $\mathbb{Q}$ by roots of unity is called a* ***cyclotomic field****.*

Given a prime $p \in \mathbb{Z}$, let $\zeta = \zeta_p$ be a primitive $p - th$ root of unity. ζ is a root of the polynomial $X^p - 1$. Since $\zeta \neq 1$, it is also a root of the *cyclotomic polynomial* $\frac{X^p-1}{X-1} = X^{p-1} + \cdots + X + 1$.

To show that the cyclotomic polynomial is irreducible over $\mathbb{Q}$, we'll use *Eisenstein's irreducibility criterion.* Recall Eisenstein's irreducibility criterion, for a principal ideal domain A, a prime p in A and $F(X) = X^n + a_{n-1}X^{n-1} + \cdots + a_1X + a_0 \in A[X]$ such that $p|a_i$, for $0 \leq i \leq n-1$ and $p^2 \not| a_0$, then $F(X)$ is irreducible over the field of fractions of A.

Theorem 2.4. *For any prime number $p \in \mathbb{Z}$, the cyclotomic polynomial $X^{p-1} + X^{p-2} + \cdots + x + 1$ is irreducible in $\mathbb{Q}[X]$.*

Proof. Substitute $X = Y + 1$. Then,

$$X^{p-1}+\cdots+X+1 = \frac{X^p-1}{X-1} = \frac{(Y+1)^p-1}{Y} = \sum_{j=1}^{p-1}\binom{p}{j}y^{j-1}+Y^{p-1} = F_1(Y).$$

If $F_1(Y)$ is irreducible, then so is the cyclotomic polynomial. Observe that, p divides each of the binomial coefficients $\binom{p}{j}$ and that p^2 does not divide the constant term.

Therefore, by Eisenstein's irreducibility criterion, $F_1(Y)$ is irreducible. □

The previous theorem implies that $\mathbb{Q}[\zeta]$ is of the degree $p-1$ over $\mathbb{Q}$. Thus $\{1, \zeta, \ldots, \zeta^{p-2}\}$ is a base for $\mathbb{Q}[\zeta]$ over $\mathbb{Q}$. The aim of this section is to show that the ring of integers of the cyclotomic field $\mathbb{Q}[\zeta]$ is $\mathbb{Z}[\zeta]$. First we need to calculate some norms and traces.

The conjugates of ζ are ζ^j, where $1 \leq j \leq p-1$. The irreducibility of the cyclotomic polynomial implies that $Tr(\zeta^j) = -1$ for $j = 1, 2, \ldots, p-1$. Also note that $Tr(1) = p - 1$.

Thus, $Tr(1-\zeta) = Tr(1-\zeta^2) = \cdots = Tr(1-\zeta^{p-1}) = p$. While, $N(\zeta - 1) = (-1)^{p-1}p$. So, $N(1-\zeta) = p$. But, $N(1-\zeta)$ is a product of the conjugates of $(1-\zeta)$, hence

$$p = (1-\zeta)(1-\zeta^2)\ldots(1-\zeta^{p-1}). \tag{2.3}$$

Let $\mathcal{O}_K$ be the ring of integers in $K = \mathbb{Q}[\zeta]$. So, $\mathcal{O}_K$ contains ζ and its powers.

Claim 1: $(1-\zeta)\mathcal{O}_K \cap \mathbb{Z} = p\mathbb{Z}$.

Proof of Claim 1: From equation 2.3, $p \in (1-\zeta)\mathcal{O}_K$. Thus, $p\mathbb{Z} \subset (1-\zeta)\mathcal{O}_K \cap \mathbb{Z}$.

Now suppose $(1-\zeta)\mathcal{O}_K \cap \mathbb{Z} \neq p\mathbb{Z}$. Since $p\mathbb{Z}$ is a maximal ideal in $\mathbb{Z}$, $(1-\zeta)\mathcal{O}_K \cap \mathbb{Z} = \mathbb{Z}$, i.e. $(1-\zeta)$ is a unit in $\mathcal{O}_K$.

So, the conjugates $(1-\zeta^j)$ of $(1-\zeta)$ are also units in $\mathcal{O}_K$. Thus, from (**??**), p is also a unit in $\mathbb{Z} \cap \mathcal{O}_K$. This is a contradiction.

Therefore, $(1-\zeta)\mathcal{O}_K \cap \mathbb{Z} = p\mathbb{Z}$.

Claim 2: For any $y \in \mathcal{O}_K$, $Tr(y(1-\zeta)) \in p\mathbb{Z}$.

Proof of Claim 2: Each conjugate $y_j(1-\zeta^j)$ of $y(1-\zeta)$ is a multiple (in $\mathcal{O}_K$) of $(1-\zeta^j)$, which itself is a multiple of $(1-\zeta)$.

Since trace is the sum of the conjugates, we have, $Tr(y(1-\zeta)) \in (1-\zeta)\mathcal{O}_K$. Also, the trace of an algebraic integer $\in \mathbb{Z}$.

Therefore, $Tr(y(1-\zeta)) \in (1-\zeta)\mathcal{O}_K \cap \mathbb{Z} = p\mathbb{Z}$.

Theorem 2.5. *Let $p \in \mathbb{Z}$, a prime and ζ a primitive $p-th$ root of unity in $\mathbb{C}$. Then the ring $\mathcal{O}_K$ of integers of the cyclotomic field $K = \mathbb{Q}[\zeta]$ is $\mathbb{Z}[\zeta]$, and $\{1, \zeta, \ldots, \zeta^{p-2}\}$ is a base for $\mathcal{O}_K$ as a $\mathbb{Z}$-module.*

Proof. Let $x = a_0 + a_1\zeta + \cdots + a_{p-2}\zeta^{p-2}$, where $a_i \in \mathbb{Q}$, be an element in $\mathcal{O}_K$. Then,

$$x(1-\zeta) = a_0(1-\zeta) + \cdots + a_{p-2}(\zeta^{p-2} - \zeta^{p-1}).$$

Taking traces and making use of the previous discussion in this section, we obtain, $Tr(x(1-\zeta)) = a_0 Tr(1-\zeta) = a_0 p$.

So, $pa_0 \in p\mathbb{Z}$ and thus, $a_0 \in \mathbb{Z}$. Also $\zeta^{-1} = \zeta^{p-1}$ implies $\zeta^{-1} \in \mathcal{O}_K$. So,

$$(x - a_0)\zeta^{-1} = a_1 + a_2\zeta + \cdots + a_{p-2}\zeta^{p-3} \in \mathcal{O}_K.$$

By the same argument as before, $a_1 \in \mathbb{Z}$.

Applying the same argument successively, we conclude that each $a_i \in \mathbb{Z}$. □

Remark 2.6. The results of this section extend to the case of cyclotomic fields $\mathbb{Q}[t]$, where t is a primitive $p^r - th$ root of unity (p- prime). Such a field is of degree $p^{r-1}(p-1)$, and its ring of integers is $\mathbb{Z}[t]$. The minimal polynomial of t over $\mathbb{Q}$ is

$$\frac{X^{p^r} - 1}{X^{p^{r-1}} - 1} = X^{p^{r-1}(p-1)} + \cdots + X^{p^{r-1}} + 1.$$

2.5.1 Discriminant of a cyclotomic field

Let p be an odd prime and let ζ be a primitive $p - th$ root of unity. Let $K = \mathbb{Q}[\zeta]$ be the $p - th$ cyclotomic field and denote the conjugates of ζ by $\zeta = \zeta_1, \zeta_2, \ldots, \zeta_{p-1}$. So we have

$$F(X) = \frac{X^p - 1}{X - 1} = \prod_{i=1}^{p-1}(X - \zeta_i).$$

The discriminant can be computed (using the integral base $\{1, \zeta, \ldots, \zeta^{p-2}\}$) as follows:

$$D(1, \zeta, \ldots, \zeta^{p-2}) = \det(\sigma_l(\zeta^k))^2 = \prod_{i<j}(\sigma_i(\zeta) - \sigma_j(\zeta))^2 = \prod_{i<j}(\zeta_i - \zeta_j)^2,$$

as it is the determinant of a Vandermonde matrix. So we have

$$D(1, \zeta, \ldots, \zeta^{p-2}) = (-1)^{\frac{p-1}{2}} \prod_{i \neq j}(\zeta_i - \zeta_j).$$

Note that

$$F'(X) = \sum_i \prod_{i \neq j}(X - \zeta_j),$$

so,

$$\prod_{i \neq j}(\zeta_i - \zeta_j) = \prod_i F'(\zeta_i) = N_{K/\mathbb{Q}}(F'(\zeta)).$$

To compute this norm, we take the derivative on both sides of $(X-1)F(X) = X^p - 1$. Substitute $X = \zeta$ and take norm to get

$$N(\zeta - 1)N(F'(\zeta)) = N(p\zeta^{p-1}) = N(p)N(\zeta^{p-1}) = p^{p-1}.$$

The norm $N(\zeta - 1)$ is given by

$$N(\zeta - 1) = \prod_i(\zeta_i - 1) = \prod_i(1 - \zeta_i) = p.$$

Thus, $D(1, \zeta, \ldots, \zeta^{p-2}) = (-1)^{\frac{p-1}{2}} p^{p-2}$.

Chapter 3

Fractional ideals and Dedekind's theorem

3.1 Norm of an ideal and fractional ideals

Let K be a number field of degree n and let $\mathcal{O}_K$ be its ring of integers.

Definition 3.1. *For any ideal $I \neq \{0\}$ of $\mathcal{O}_K$, the number of elements in the residue class ring $\mathcal{O}_K/I$ is called the* ***norm of I****, denoted by $N(I)$.*

If $I = \{0\}$, then $N(I) = 0$. Clearly, $N(\mathcal{O}_K) = 1$. For a proper ideal I, $N(I) > 1$.

Proposition 3.1. *Let I be a non-zero integral ideal and let $\mathcal{O}_K = \mathbb{Z}\beta_1 + \cdots + \mathbb{Z}\beta_n$. Then there exist $\alpha_i = \sum\limits_{j \geq i} p_{ij}\beta_j$, where $p_{ij} \in \mathbb{Z}$ and $p_{ii} > 0$ such that $I = \mathbb{Z}\alpha_1 + \cdots + \mathbb{Z}\alpha_n$. Also, $N(I) = \prod\limits_{i=1}^{n} p_{ii}$.*

Proof. By remarks of Chapter 2, Section 3, I has an integral base $\{\alpha_1, \alpha_2, \ldots, \alpha_n\}$ of the required form. Let $\eta = \eta(x_1, \ldots, x_n) = \sum\limits_{i=1}^{n} x_i\beta_i$, $0 \leq x_i < p_{ii}$, $x_i \in \mathbb{Z}$.

Claim : The set $S = \{\eta(x_1, \ldots, x_n) | 0 \leq x_i < p_{ii}\}$ of $p_{11}p_{22}\ldots p_{nn}$ many elements form a complete system of residues of $\mathcal{O}_K$ modulo I.

Proof of the claim : If $\zeta = \sum\limits_{i=1}^{n} c_i\beta_i = c_1\beta_1 + \cdots + c_n\beta_n \in \mathcal{O}_K$, $c_i \in \mathbb{Z}$ and we set $\mathcal{O}_i \coloneqq \mathcal{O}_K \cap (\mathbb{Z}\beta_{i+1} + \cdots + \mathbb{Z}\beta_n)$. Now, $\alpha_1 = p_{11}\beta_1 + p_{12}\beta_2 + \cdots + p_{1n}\beta_n$. By division algorithm, write $c_1 = m_1p_{11} + x_1$ such that $0 \leq x_1 < p_{11}$. So, $\zeta_1 = \zeta - x_1\beta_1 - m_1\alpha_1 \in \mathcal{O}_1$. We can, in the same way find $m_2 \in \mathbb{Z}$, $0 \leq x_2 < p_{22}$ with

$$\zeta_2 = \zeta_1 - x_2\beta_2 - m_2\alpha_2 \in \mathcal{O}_2.$$

Continuing this way, we find $\zeta = \sum\limits_{i=1}^{n}(m_i\alpha_i + x_i\beta_i)$, where $m_i \in \mathbb{Z}$ and $0 \leq x_i < p_{ii}$. So, S generates $\mathcal{O}_K/I$. This completes the proof of the claim.

Now we want to show that the $\eta \in S$ are all distinct modulo I. So, let $\sum\limits_{i=1}^{n} x_i\beta_i = \sum\limits_{i=1}^{n} y_i\beta_i \in \mathcal{O}_K/I$ and $0 \leq x_i, y_i < p_{ii}$. This implies

$$\sum_{i=1}^{n}(x_i - y_i)\beta_i \in I.$$

Now since $I = \langle \alpha_1, \ldots, \alpha_n \rangle$, we have

$$\sum_{i=1}^{n}(x_i - y_i)\beta_i = \sum_{i=1}^{n} k_i\alpha_i, \text{ where } k_i \in \mathbb{Z}.$$

Also,

$$\begin{aligned} \alpha_1 &= p_{11}\beta_1 + p_{12}\beta_2 + \cdots + p_{1n}\beta_n \\ \alpha_2 &= p_{22}\beta_2 + \cdots + p_{2n}\beta_n \\ &\vdots \\ \alpha_n &= p_{nn}\beta_n \end{aligned}$$

So, $k_1\alpha_1 + \cdots + k_n\alpha_n = k_1(p_{11}\beta_1 + \cdots + p_{1n}\beta_n) + \cdots + k_n(p_{nn}\beta_n)$. So, $x_1 - y_1 = k_1p_{11}$. This implies, $p_{11}|x_1 - y_1$. Now, $0 \leq x_1, y_1 < p_{11}$ implies $x_1 - y_1 < p_1$. Hence, $x_1 - y_1 = 0$, i.e., $k_1 = 0$ (since $p_{11} \neq 0$). Similarly, $k_i = 0$ for every $1 \leq i \leq n$ and $x_i = y_i$. This completes the proof. □

Lemma 3.1. *Let K be a number field of degree n and let $\alpha \neq 0 \in \mathcal{O}_K$. Then $N(\langle \alpha \rangle) = |N_K(\alpha)|$.*

Proof. If $\mathcal{O}_K = \mathbb{Z}\beta_1 + \cdots + \mathbb{Z}\beta_n$, then by the previous proposition, there exist $\alpha_i = \sum\limits_{j \geq i} p_{ij}\beta_j$, where $p_{ij} \in \mathbb{Z}$ and $p_{ii} > 0$ such that $\langle \alpha \rangle = \mathbb{Z}\alpha_1 + \cdots + \mathbb{Z}\alpha_n$.

Also, $N(\langle\alpha\rangle) = \prod_{i=1}^{n} p_{ii}$. Since $\langle\alpha\rangle = \mathbb{Z}\alpha\beta_1 + \cdots + \mathbb{Z}\alpha\beta_n$, we can write

$$\alpha\beta_i = \sum_{j=1}^{n} r_{ij}\alpha_j, \ 1 \leq i \leq n.$$

Let $R = (r_{ij})$, then R is a base change matrix and hence invertible i.e. $\det(R)$ is an invertible integer, in other words $\det(R) = \pm 1$. Also, $P = (p_{ij})$ is an upper triangular matrix and $det(P)$ is product of the diagonal entries.

Now,

$$\alpha_j = \sum_{k \geq j} p_{jk}\beta_k$$

implies,

$$\alpha\beta_i = \sum_{j=1}^{n} r_{ij} \sum_{k \geq j} p_{jk}\beta_k.$$

Taking regular representation of α with respect to the base $\beta_1, \ldots, \beta_n$, we have

$$N_K(\alpha) = det(RP) = det(R) \times det(P) = \pm det(P).$$

But,

$$\pm det(P) = \pm \prod_{i=1}^{n} p_{ii} = \pm N(\langle\alpha\rangle)$$

Thus, $N(\langle\alpha\rangle) = |N_K(\alpha)|$. □

Definition 3.2. *By a **fractional ideal** in K we mean an $\mathcal{O}_K$-submodule I of K for which there exists $m \neq 0 \in \mathbb{Z}$ such that $mI \subset \mathcal{O}_K$.*

Any ideal in $\mathcal{O}_K$ is trivially a fractional ideal. For any ideal L in $\mathcal{O}_K$ and for any $b \neq 0 \in \mathbb{Z}$, $b^{-1}L$ is a fractional ideal in K. Any ideal in $\mathcal{O}_K$ is called an *integral ideal* in K.

Any fractional ideal I can be written as $a^{-1}J$, for $a \neq 0 \in \mathbb{Z}$ and an integral ideal J. If I, J are fractional ideals in K, then for a suitable $c \in \mathbb{Z}, c \neq 0$, cI and cJ are both integral ideals and the sum $I + J$ and product $I \cdot J$ are therefore fractional ideals in K.

3.2 Dedekind domain

Definition 3.3. *An integral domain A is said to be **integrally closed** if its integral closure in its field of fractions $Q(A)$ is A itself, i.e., if $x \in Q(A)$ is an integral element over A, then $x \in A$.*

Example 3.1. Any principal ideal domain is integrally closed.

Definition 3.4. *An integral domain A is called a **Dedekind domain** if it is Noetherian, integrally closed, and if every non-zero prime ideal of A is maximal.*

We recall that a ring R is called *Noetherian* if it satisfies any of the following three equivalent conditions:

(N1) If $I_1 \subset I_2 \subset \cdots \subset I_n \subset I_{n+1} \subset \cdots$ is an increasing sequence of ideals in R, then there exists $m_0 \in \mathbb{N}$ such that $I_m = I_{m+1}$ for every $m \geq m_0$.

(N2) Any non-empty set $\mathcal{S}$ of ideals of R contains a maximal element, i.e., an ideal $I \in \mathcal{S}$ such that $I \not\subset J$ for any $J \in \mathcal{S}$.

(N3) Any ideal I in R is finitely generated.

The ring $\mathbb{Z}$, and more generally any principal ideal ring is a Dedekind domain.

Claim: The ring of integers $\mathcal{O}_K$ of a number field K is a Dedekind domain.

(D1) Every non-zero prime ideal of $\mathcal{O}_K$ is maximal.

Let I be a prime ideal in $\mathcal{O}_K$, then $\mathcal{O}_K/I$ is an integral domain. Now, $N(I) < \infty$, i.e., $\left|\mathcal{O}_K/I\right| < \infty$. Hence $\mathcal{O}_K/I$ is a field, as any finite integral domain is a field, implying I is a maximal ideal.

(D2) $\mathcal{O}_K$ is integrally closed.

We know, any number field is a subfield of $\mathbb{C}$. We have also seen that $\alpha \in \mathbb{C}$ is integral over $\mathcal{O}_K$ if and only if there exists a non-zero finitely-generated $\mathcal{O}_K$-module $M \subset \mathbb{C}$ with $\alpha M \subset M$.

So, M is finitely-generated over $\mathcal{O}_K$ and moreover, $\mathcal{O}_K$ is finitely-generated over $\mathbb{Z}$. Hence, M is finitely-generated over $\mathbb{Z}$. Thus α is integral over $\mathbb{Z}$ and hence lies in $\mathcal{O}_K$.

(D3) $\mathcal{O}_K$ is Noetherian.

We know that, if A is a Noetherian ring and $f : A \longrightarrow B$ makes B an A-algebra so that B is a finitely-generated A-module under multiplication $a \cdot b := f(a)b$, then B is a Noetherian ring. Hence, $\mathcal{O}_K$ is Noetherian.

Interest in Dedekind domains arises from the fact that the ring of integers of a number field is a Dedekind domain, but not always a principal ideal domain.

Example 3.2. Consider the ring of integer $\mathcal{O}_K = \mathbb{Z}[\sqrt{-5}]$ in $K = \mathbb{Q}[\sqrt{-5}]$. Observe that

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

The norms of the four factors are, respectively, 6, 6, 4, and 9.

Note that $1+\sqrt{-5}$ can have no non-trivial divisor in $\mathcal{O}_K$, since the norm of such a divisor would have to be a non-trivial divisor of 6. This is impossible, because the equations $a^2 + 5b^2 = 2$ and $a^2 + 5b^2 = 3$ have no solutions in $\mathbb{Z}$.

If $\mathcal{O}_K$ were principal, the prime element $1+\sqrt{-5}$, which divides the product $2 \cdot 3$, would have to divide either 2 or 3. But then, taking norms, we see that 6 would divide 4 or 9, which is not the case. Moreover, this example shows that for $K = \mathbb{Q}[\sqrt{-5}]$, $\mathcal{O}_K$ is not an UFD as well.

3.3 Unique factorisation of ideals

This brings us to the fundamental theorem of Dedekind, which says that even though we might not have unique factorisation of elements in the ring of integers of a number field, but we will nevertheless have unique factorisation of ideals.

Theorem 3.1 (Dedekind). *Any ideal of the ring $\mathcal{O}_K$ of algebraic integers in a number field K can be written as the product of prime ideals in $\mathcal{O}_K$, determined uniquely up to order.*

We need a few lemmas before we prove the theorem.

Lemma 3.2. *Any proper ideal $I \subset \mathcal{O}_K$ contains a product of prime ideals in $\mathcal{O}_K$.*

Proof. Let $\mathcal{S} = \{I \subset \mathcal{O}_K | \text{I does not contain a product of prime ideals}\}$. Suppose $\mathcal{S} \neq \phi$, then $\mathcal{S}$ contains a maximal element, say I_0. Clearly, I_0 cannot be prime, i.e., there exists $x_1, x_2 \in \mathcal{O}_K$ such that $x_1x_2 \in I_0$ but $x_1, x_2 \notin I_0$.

Let I_i $(i = 1, 2)$ be the ideal generated by I_0 and x_i. Then $I_0 \subsetneq I_1$ and $I_0 \subsetneq I_2$. By the maximality of I_0 in $\mathcal{S}$, $I_i \notin \mathcal{S}$.

Hence, $I_1 \supset P_1 P_2 \ldots P_r$ and $I_2 \supset Q_1 Q_2 \ldots Q_s$, where $P_1, \ldots, P_r, Q_1, \ldots, Q_s$ are prime ideals in $\mathcal{O}_K$. Since $I_1 I_2 \subset I_0$, we have $P_1 \ldots P_r Q_1 \ldots Q_s \subset I_0$. This is a contradiction. Therefore, $\mathcal{S} = \phi$. □

Lemma 3.3. *Any non-zero prime ideal $P \subset \mathcal{O}_K$ is invertible, i.e., there exists a fractional ideal P^{-1} in K such that $PP^{-1} = \mathcal{O}_K$.*

Proof. Let P be a non-zero prime ideal in $\mathcal{O}_K$. Let P^{-1} be the set $\{x \in K | xP \subset \mathcal{O}_K\}$. It is easy to see that P^{-1} is an $\mathcal{O}_K$-module with $\mathcal{O}_K \subset P^{-1}$.

Since there exists $n \neq 0 \in \mathbb{Z} \cap P$, we have $nP^{-1} \subset PP^{-1} \subset \mathcal{O}_K$. Hence P^{-1} is a fractional ideal in K. Now, $P \subset PP^{-1} \subset \mathcal{O}_K$. Since P is maximal, either $PP^{-1} = \mathcal{O}_K$ or $P = PP^{-1}$.

If $PP^{-1} = \mathcal{O}_K$, then we are done. If $P = PP^{-1}$, then every $x \in P^{-1}$ satisfies $xP \subset P$. We know P is a finitely-generated $\mathbb{Z}$-module, implying $x \in \mathcal{O}_K$. This implies $P^{-1} \subset \mathcal{O}_K$, i.e., $P^{-1} = \mathcal{O}_K$. We will show that $P^{-1} = \mathcal{O}_K$ is not possible.

Let $x \in P$, then $x\mathcal{O}_K \neq \mathcal{O}_K$, because x is a non-unit, i.e., $x\mathcal{O}_K$ is a proper integral ideal and by the previous lemma, there exist prime ideals $P_1, P_2, \ldots, P_r$ in $\mathcal{O}_K$ such that $P_1 P_2 \ldots P_r \subset x\mathcal{O}_K$.

Let r be chosen such that $x\mathcal{O}_K$ doesn't contain a product of $r-1$ prime ideals in $\mathcal{O}_K$. Such an r can be chosen because if it does not exist, then we can keep reducing the number of prime ideals in the product and end up getting an empty product inside $x\mathcal{O}_K$, i.e., $\mathcal{O}_K \subset x\mathcal{O}_K$, which is a contradiction.

Now, $P \supset x\mathcal{O}_K \supset P_1 P_2 \ldots P_r$. So P divides one of the P_i, say P_1, i.e., $P_1 \subset P$. But $P = P_1$. Now, $P_2 P_3 \ldots P_r \not\subset x\mathcal{O}_K$. Hence, there exists $b \in P_2 P_3 \ldots P_r$ and $b \notin x\mathcal{O}_K$, implying $x^{-1}b \notin \mathcal{O}_K$.

But $bx^{-1}P \subset P_2 P_3 \ldots P_r (x^{-1}\mathcal{O}_K) P = x^{-1}\mathcal{O}_K P_1 P_2 P_3 \ldots P_r \subset x^{-1}\mathcal{O}_K \cdot x\mathcal{O}_K = \mathcal{O}_K$. Thus, $bx^{-1} \in P^{-1} = \mathcal{O}_K$. This is a contradiction. Hence, $P^{-1} \neq \mathcal{O}_K$. Thus, $PP^{-1} = \mathcal{O}_K$. □

Proof of Dedekind's theorem. We will deal with the case of proper integral ideals only, because the ideal $\mathcal{O}_K$ can be written as an empty product of prime ideals in $\mathcal{O}_K$.

(i) Existence of a factorisation:

Let $\mathcal{S}$ be the set of proper ideals of $\mathcal{O}_K$, which cannot be factorised into prime ideals. Suppose $\mathcal{S} \neq \phi$, then by property (N2), $\mathcal{S}$ contains a maximal ideal, say $I_0 \subset \mathcal{O}_K$. This implies I_0 is not prime.

Property (N3) implies that there exists a prime ideal $P \subset \mathcal{O}_K$ such that $I_0 \subset P$. Also, lemma 3.3 tells us that there exists a fractional ideal P^{-1} in K such that $PP^{-1} = \mathcal{O}_K$.

Therefore, $I_0P^{-1} \subset PP^{-1} = \mathcal{O}_K$. But if $I_0P^{-1} = P_1P_2 \dots P_r$, for prime ideals P_i in $\mathcal{O}_K$, then $I_0 = PP_1P_2 \dots P_r$. This is a contradiction. Hence, $I_0P^{-1} \in \mathcal{S}$. But this contradicts the maximality of I_0. Thus, $\mathcal{S} = \phi$.

(ii) Uniqueness of factorisation:

Let I be a proper ideal in $\mathcal{O}_K$ and

$$I = P_1P_2 \dots P_r = Q_1Q_2 \dots Q_s$$

where P_i, Q_j are all prime ideals in $\mathcal{O}_K$. Since $Q_1 | \prod_{i=1}^{r} P_i$, this implies $Q_1 | P_i$ for some $1 \leq i \leq r$. Say $Q_1 | P_1$. But Q_1, P_1 are both maximal. Hence, $Q_1 = P_1$. Now by lemma 3.3,

$$\begin{aligned} Q_1^{-1}I &= Q_1^{-1}Q_1Q_2 \dots Q_s = Q_2Q_3 \dots Q_s \\ Q_1^{-1}I &= P_1^{-1}P_1P_2 \dots P_r = P_2P_3 \dots P_r \end{aligned}$$

Thus, $Q_2Q_3 \dots Q_s = P_2P_3 \dots P_r$. By repeating the arguments above, in finitely many steps, we can thus prove that $r = s$, and the factorisation is unique up to order. □

Corollary 3.1. *Any fractional ideal I in K can be uniquely written in the form*

$$I = \frac{Q_1Q_2 \dots Q_s}{P_1P_2 \dots P_r}$$

where Q_i, P_j are prime and $Q_i \neq P_j$ for every i, j.

Proof. Choose $c \neq 0 \in \mathbb{Z}$ such that $cI \subset \mathcal{O}_K$. So, there exists an integral ideal J such that $J = cI$. Now, as $c \in \mathbb{Z} \subset \mathcal{O}_K$, $\langle c \rangle$ is proper ideal of $\mathcal{O}_K$.

Write $\langle c \rangle = P_1P_2 \dots P_r$ and $J = Q_1Q_2 \dots Q_{s'}$. If any $Q_i = P_j$, then cancel them by multiplying with their inverse ideal, viz., Q_i^{-1}. □

Corollary 3.2. *Given any fractional ideal $I \neq \{0\}$ in K there exists a fractional ideal I^{-1} such that $I \cdot I^{-1} = \mathcal{O}_K$.*

Proof. Since I is a fractional ideal in K, there exists $c \neq 0 \in \mathbb{Z}$ such that $cI \subset \mathcal{O}_K$. So, $J = cI$ is an integral ideal. Hence, $J = P_1P_2 \dots P_r$, where P_i's are prime.

Now each P_i has an inverse P_i^{-1} in K such that $P_iP_i^{-1} = \mathcal{O}_K$. So, $P_1^{-1} \dots P_r^{-1}J$ $= \mathcal{O}_K$. Hence, $c \cdot P_1^{-1}P_2^{-1} \dots P_r^{-1}I = \mathcal{O}_K$. Take $c \cdot P_1^{-1}P_2^{-1} \dots P_r^{-1} = I^{-1}$. Now, I^{-1} is an $\mathcal{O}_K$-submodule of K.

To show I^{-1} is a fractional ideal, we need to find $m \neq 0 \in \mathbb{Z}$ such that $mI^{-1} \subset \mathcal{O}_K$. Since each P_i^{-1} is a fractional ideal in K, there exist $m_i \neq 0 \in \mathbb{Z}$ such that $m_iP_i^{-1} \subset \mathcal{O}_K$. Then $m = \prod_{i=1}^{r} m_i \in \mathbb{Z}$ is as required. □

Remark 3.1. Let $I = P_1^{a_1} \dots P_r^{a_r}$; $J = P_1^{b_1} \dots P_r^{b_r}$ be integral ideals. $P_1, \dots, P_r$ are prime ideals and $a_i, b_j \in \mathbb{Z}_{\geq 0}$, where $P_i^0 = \mathcal{O}_K$. Then the $gcd(I, J) :=$ $P_1^{c_1} \dots P_r^{c_r}$, where $c_i = \min(a_i, b_i)$ and $lcm(I, J) = P_1^{d_1} \dots P_r^{d_r}$, where $d_i =$ $\max(a_i, b_i)$ for $1 \leq i \leq r$.

By definition of lcm, $I|lcm(I, J)$ and $J|lcm(I, J)$. Hence, $lcm(I, J) \subset I,\ J$. Thus, $lcm(I, J) \subset I \cap J$. Also, $I \cap J = P_1^{e_1} \dots P_r^{e_r}$, where $e_i \geq d_i$, for every i, implying $I \cap J \subset lcm(I, J)$. Therefore, $lcm(I, J) = I \cap J = P_1^{d_1} \dots P_r^{d_r}$, where $d_i = \max(a_i, b_i)$.

Further, $gcd(I, J) =$ smallest ideal dividing I and $J = I + J$.

We know, $I \subset I + J$ and $J \subset I + J$, then $I + J$ is a divisor of both I and J. Now let K be any divisor of I and J. Hence,$I, J \subset K$, i.e, $I + J \subset K$, i.e., $K|(I + J)$. Therefore, $I + J$ is the gcd of I and J.

Lemma 3.4. *For any two integral ideals I and J, there exists a $w \in \mathcal{O}_K$ such that $gcd(IJ, \langle w \rangle) = I$.*

Proof. Let $I = P_1^{a_1} \dots P_r^{a_r}$, $J = P_1^{b_1} \dots P_r^{b_r}$, where $a_i, b_i \in \mathbb{Z}_{\geq 0}$ and $P_1, \dots, P_r$ are all prime ideals dividing I and J.

We can find an element $\pi_i \in P_1^{a_1+1} \dots P_{i-1}^{a_{i-1}+1}P_i^{a_i}P_{i+1}^{a_{i+1}+1} \dots P_r^{a_r+1}$, but $\pi_i \notin$ $P_1^{a_1+1} \dots P_{i-1}^{a_{i-1}+1}P_i^{a_i+1}P_{i+1}^{a_{i+1}+1} \dots P_r^{a_r+1}$ (since $P_i \neq \mathcal{O}_K$).

Take $w = \sum\limits_{i=1}^{r} \pi_i$. Clearly, $P_i^{a_i+1}$ divides π_j for $i \neq j$, and $P_i^{a_i}$ is the highest power of P_i dividing π_i. Hence, $P_i^{a_i}$ and no higher power of P_i divides w, implying that $gcd(IJ, \langle w \rangle) \subset I$.

Now, look at the prime ideal decomposition, $\langle w \rangle = P_1^{\alpha_1} \dots P_r^{\alpha_r} Q_1^{s_1} \dots Q_t^{s_t}$. So $\alpha_i = a_i$ for every i and $IJ = P_1^{a_1+b_1} \dots P_r^{a_r+b_r}$. So, $gcd(IJ, \langle w \rangle) \supset I$. Hence, $gcd(IJ, \langle w \rangle) = I$. □

Remark 3.2. Given any integral ideal I, there exists $t \neq 0 \in \mathbb{Z}$ such that $J = tI^{-1} \subset \mathcal{O}_K$, i.e., $IJ = t\mathcal{O}_K$. By the previous lemma, $I = gcd(IJ, \langle w \rangle) = gcd(t\mathcal{O}_K, w\mathcal{O}_K) = t\mathcal{O}_K + w\mathcal{O}_K$, i.e., any integral ideal can be generated over $\mathcal{O}_K$ by two algebraic integers in K.

The multiplicativity of norm can now be proved for ideals as well.

Lemma 3.5. *Let I, J be integral ideals. Then $N(IJ) = N(I)N(J)$.*

Proof. Let $\lambda = N(I)$ and $\mu = N(J)$. Let $\xi_1, \xi_2, \dots, \xi_\lambda$ and $\eta_1, \eta_2, \dots, \eta_\mu$ be a complete set of representatives of $\mathcal{O}_K/I$ and $\mathcal{O}_K/J$, respectively.

By the previous lemma, there exists $w \in \mathcal{O}_K$ such that $gcd(IJ, \langle w \rangle) = I$.

Claim : $\lambda\mu$ elements $\xi_i + w\mu_j$ for $1 \leq i \leq \lambda$; $1 \leq j \leq \mu$, form a complete set of representatives of $\mathcal{O}_K/IJ$.

Proof of the claim : (i) Suppose $\xi_i + w\mu_j \equiv \xi_k + w\mu_l \pmod{IJ}$. Thus,

$$(\xi_i - \xi_k) + w(\eta_j - \eta_l) \equiv 0 \pmod{IJ}$$
$$(\xi_i - \xi_k) + w(\eta_j - \eta_l) \in IJ \subset I.$$

We know, $gcd(IJ, \langle w \rangle) = I$, implies $w \in \mathcal{O}_K$. Thus, $w(\eta_j - \eta_l) \in I$, i.e., $(\xi_i - \xi_k) \in I$ and $i = k$.

Hence, $w(\eta_j - \eta_l) \in IJ$. So, $\eta_j - \eta_l \in J$ and $j = l$.

(ii) Given any $x \in \mathcal{O}_K$, there exists a unique ξ_i $(1 \leq i \leq \lambda)$ such that $x \in \xi_i + I$ in $\mathcal{O}_K/I$.

Now, $I = (IJ, \langle w \rangle) = IJ + \langle w \rangle$, then $x - \xi_i = w\eta + y$ with $y \in IJ$. So,

$$x - \xi_i \equiv w\eta_j \pmod{IJ} \text{ for some } \eta_j$$
$$x \equiv \xi_i + w\eta_j \pmod{IJ}.$$

□

In view of this and Corollary 3.1 we can extend the definition of norm integral ideals to *norm fractional ideals.* For a fractional ideal I, we define its norm

$$N(I) = \frac{N(Q_1)N(Q_2)\ldots N(Q_s)}{N(P_1)N(P_2)\ldots N(P_r)}$$

where $I = \frac{Q_1Q_2\ldots Q_s}{P_1P_2\ldots P_r}$ is the prime factorisation of I.

3.4 Factorisation of rational primes in quadratic fields

For the remaining part of this chapter, K will always stand for a quadratic field $\mathbb{Q}[\sqrt{t}]$ with discriminant d. We need to set up a few notations before we proceed.

The mapping $\sigma : K \longrightarrow K$ such that $\sigma(\alpha) = \alpha'$, where $\alpha = x + y\sqrt{d}$ and $\alpha' = x - y\sqrt{d}$ for $x, y \in \mathbb{Q}$, may be seen as an automorphism of K.

Let $\alpha \in K$ and $\alpha = \alpha'$ implies $\alpha \in \mathbb{Q}$ and conversely.

For any subset S of K, denote by S' the image of S under this automorphism. We know $\sigma^2 = Id$. Let I be a fractional ideal in K. So, there exists $m \neq 0 \in \mathbb{Z}$ such that $mI \subset \mathcal{O}_K$. Then $\sigma(mI) \subset \sigma(\mathcal{O}_K) = \mathcal{O}_K$, i.e., $m \cdot \sigma(I) \subset \mathcal{O}_K$. This shows that I' is a fractional ideal in K.

It is easy to see that $N(I) = N(I')$, where I is a fractional ideal in K.

For this, without loss of generality, we can assume I to be an integral ideal. Consider the ring homomorphism,

$$\begin{aligned} \varphi : \mathcal{O}_K/I &\longrightarrow \mathcal{O}_K/I' \\ \alpha + I &\longmapsto \alpha' + I' \end{aligned}$$

This map is well-defined as $\alpha - \beta \in I$ implies $(\alpha - \beta)' = \alpha' - \beta' \in I'$. Now $Ker(\varphi) = \{\alpha + I | \alpha' + I' = I'\} = \{\alpha + I | \alpha' \in I'\} = \{\alpha + I | \alpha \in I\}$, as σ is an automorphism. Hence φ is injective.

Now for $\alpha + I' \in \mathcal{O}_K/I'$ consider $\alpha' + I \in \mathcal{O}_K/I$ to see that $\varphi(\alpha' + I) = \alpha + I'$. Hence φ is an isomorphism of rings. Therefore,

$$|\mathcal{O}_K/I| = |\mathcal{O}_K/I'|,$$

i.e., $N(I) = N(I')$.

This proof also shows that for a prime ideal P of $\mathcal{O}_K$, P' is also a prime ideal of $\mathcal{O}_K$.

Let $p \in \mathbb{Z}$ be a rational prime and consider the integral ideal $p\mathcal{O}_K$. Let its prime factorisation be

$$p\mathcal{O}_K = P_1 \cdots P_r;$$

where $P_1, \dots, P_r$ are prime ideals in $\mathcal{O}_K$. So,

$$N(p\mathcal{O}_K) = N_K(p) = p^2 = N(P_1) \cdots N(P_r).$$

This shows $p\mathcal{O}_K$ has at most two prime factors (they may be the same though), i.e. we have the following scenarios : $p\mathcal{O}_K = P$, or $p\mathcal{O}_K = P^2$, or $p\mathcal{O}_K = PQ$, with $P \neq Q$ (as we shall see later in this case Q is nothing but P'). Depending on the various possibilities we have the following definition.

Definition 3.5. *Let $p \in \mathbb{Z}$ be a prime.*

(i) If $p\mathcal{O}_K = PQ$, with $P \neq Q$, then p ***splits in K****.*

(ii) If $p\mathcal{O}_K = P^2$, then p is ***ramified in K****.*

(iii) If $p\mathcal{O}_K = P$, then p ***remains a prime in K****.*

For an odd prime p, the following proposition gives a classification according to their type of factorisation. For this we first recall the definition of the Legendre symbol.

Definition 3.6 (Legendre symbol)**.** *For an odd prime p,*

$$\left(\frac{d}{p}\right) := \begin{cases} 0 & \textit{if } d \equiv 0 \bmod p, \\ +1 & \textit{if } d \textit{ is a square} \bmod p, \\ -1 & \textit{if } d \textit{ is not a square} \bmod p. \end{cases}$$

Proposition 3.2. *If p is an odd prime, then*

(i) $p\mathcal{O}_K = P^2$, P prime, if and only if $(\frac{d}{p}) = 0$,

(ii) $p\mathcal{O}_K = PP'$, $P \neq P'$, P prime if and only if $(\frac{d}{p}) = +1$,

(iii) $p\mathcal{O}_K = P$, P prime if and only if $(\frac{d}{p}) = -1$,

where $(\frac{d}{p})$ is the Legendre symbol.

Proof. (i) Let $p\mathcal{O}_K = P^2$, P prime. Then there exists $\pi = m + n(\frac{d+\sqrt{d}}{2}) \in P$ and $\pi \notin P^2 = p\mathcal{O}_K$ and $m, n \in \mathbb{Z}$.

Now, since $\pi^2 = \left(\frac{2m+nd+n\sqrt{d}}{2}\right)^2 = (2m+nd)^2 + dn^2 + 2n(2m+nd)\sqrt{d}$, $\pi^2 \in p\mathcal{O}_K$ implies $p|(2m+nd)^2 + dn^2$ and $p|n(2m+nd)$.

If $p|n$, then $p|(2m+nd)^2$, i.e., $p|(2m+nd)$. So, $p|m$, as p is an odd prime. So, $p|m$ and $p|n$ then $p|gcd(m,n)$. Hence, $\pi \in p\mathcal{O}_K$. This is a contradiction. Thus, $p|(2m+nd)$ and $p \not| n$. Also since $p|dn^2$, hence $p|d$. Therefore, $(\frac{d}{p}) = 0$.

Conversely, let $(\frac{d}{p}) = 0$. Consider the ideal $P = p\mathcal{O}_K + \sqrt{d}\mathcal{O}_K$. Then $P^2 = p^2\mathcal{O}_K + p\sqrt{d}\mathcal{O}_K + d\mathcal{O}_K \subset p\mathcal{O}_K$. Now we show $p \in P^2$. We know, $p^2 \in P^2$ and $d \in P^2$. Thus, $gcd(d, p^2) \in P^2$.

Now, $gcd(d,p^2) \neq p^2$, because otherwise, d is either t or $4t$, where t is square-free. Thus, $gcd(d,p^2) = p$. Therefore, $p \in P^2$, i.e., $P^2 = p\mathcal{O}_K$. Further, P is necessarily a prime ideal as at most two prime ideals of $\mathcal{O}_K$ can divide $p\mathcal{O}_K$.

(ii) Let $(\frac{d}{p}) = +1$. Then there exists $a \in \mathbb{Z}$ such that $a^2 \equiv d \pmod{p}$, i.e., $(a^2 - d) \equiv 0 \pmod{p}$. Clearly, $p \nmid a$, otherwise $p|d$ and it would give $(\frac{d}{p}) = 0$. Let P be an ideal generated by $P = p\mathcal{O}_K + (a+\sqrt{d})\mathcal{O}_K$ and $P' = p\mathcal{O}_K + (a-\sqrt{d})\mathcal{O}_K$.

So $PP' = p^2\mathcal{O}_K + p(a+\sqrt{d})\mathcal{O}_K + p(a-\sqrt{d})\mathcal{O}_K + (a^2-d)\mathcal{O}_K \subset p\mathcal{O}_K$. We first show $p \in PP'$.

Note that $2ap \in PP'$ and $p^2 \in PP'$, hence $gcd(2ap, p^2) = p \in PP'$. Therefore, $PP' = p\mathcal{O}_K$. Since $p\mathcal{O}_K$ can have at most two prime factors, we get P, P' are prime ideals in $\mathcal{O}_K$.

Next we show that $P \neq P'$. It is enough to show that $P + P' = \mathcal{O}_K$.

Note that $P + P' = \langle p, a+\sqrt{d}, a-\sqrt{d}\rangle$. To prove the above-mentioned statement, we have to show 1 as a $\mathbb{Z}$-linear combination of $\{p, a+\sqrt{d}, a-\sqrt{d}\}$. For this, $(a+\sqrt{d}) + (a-\sqrt{d}) = 2a \in P + P'$ and $p \in P + P'$. Hence, $gcd(2a, p) = 1 \in P + P'$. Therefore, $P + P' = \mathcal{O}_K$ and thus, $P \neq P'$.

Conversely, let $p\mathcal{O}_K = PP'$, $P \neq P'$, P prime. Then $N(P) = N(P') = p$. Also, there exists $\alpha \in P$ and $\alpha \notin p\mathcal{O}_K$. Then $\alpha = x + y(\frac{d+\sqrt{d}}{2})$, $x, y \in \mathbb{Z}$ and p divides at most one among x and y.

By Dedekind's theorem, $\alpha\mathcal{O}_K = PQ$, with $Q \subset \mathcal{O}_K$ an ideal. So, $N(\alpha\mathcal{O}_K) = N(P)N(Q)$, i.e., $p = N(P)|N(\alpha\mathcal{O}_K)$.

Now, $N(\alpha\mathcal{O}_K) = |N_K(\alpha)| = |\alpha\alpha'| = |(2x+yd)^2 - y^2d|$. Hence, $(2x+yd)^2 \equiv$

$y^2 d \pmod p$.

If $p|y$, then $p|(2x+yd)$, i.e., $p|x$. Therefore, $p|gcd(x,y)$, i.e., $\alpha \in p\mathcal{O}_K$. This is a contradiction.

Therefore, y is an invertible element of $\mathbb{Z}/p\mathbb{Z}$ and $\left(\frac{2x+yd}{y}\right)^2 \equiv d \pmod p$.

Therefore, $(\frac{d}{p}) = +1$.

(iii) The validity of (iii) is an immediate consequence of (i) and (ii). □

Definition 3.7 (Kronecker symbol)**.**

$$\left(\frac{d}{2}\right) := \begin{cases} 0 & \textit{if } d \equiv 0 \bmod 4, \\ +1 & \textit{if } d \equiv 1 \bmod 8, \\ -1 & \textit{if } d \equiv 5 \bmod 8. \end{cases}$$

Proposition 3.3. *(i) $2\mathcal{O}_K = P^2$, P prime if and only if $(\frac{d}{2}) = 0$,*

(ii) $2\mathcal{O}_K = PP'$, $P \neq P'$, P, P' prime, if and only if $(\frac{d}{2}) = +1$,

(iii) $2\mathcal{O}_K = P$, P prime, if and only if, $(\frac{d}{2}) = -1$,

where $(\frac{d}{2})$ is the Kronecker's symbol for quadratic reciprocity.

Proof. (i) Let $(\frac{d}{2}) = 0$, hence $d \equiv 0 \pmod 4$ i.e. $d = 4t$ with $t = 2,3 \pmod 4$. Accordingly we have either $d \equiv 0 \pmod 8$ or $d \equiv 4 \pmod 8$.

(a) When $d \equiv 0 \pmod 8$, let $P = \langle 2, \frac{\sqrt{d}}{2}\rangle$. So, $P^2 = 4\mathcal{O}_K + \sqrt{d}\mathcal{O}_K + \frac{d}{4}\mathcal{O}_K$. So, $P^2 \subset 2\mathcal{O}_K$.

Now to show, $2 \in P^2$, we find integer solutions for $4a + b\sqrt{d} + c\frac{d}{4} = 2$.

We know, $d = 4t$, so $4a + 2b\sqrt{t} + ct = 2$. So, $4a + ct = 2$ and $2b = 0$. So, $b = 0$. Now $t \equiv 2 \pmod 4$, so $gcd(4,t) = 2$. Hence we can use Bezout's identity to get integer solutions and hence $2\mathcal{O}_K \subset P^2$.

(b) When $d \equiv 4 \pmod 8$, then let $P = \langle 2, 1 + \frac{\sqrt{d}}{2}\rangle$. Then $P^2 = 4\mathcal{O}_K + 2(1 + \frac{\sqrt{d}}{2})\mathcal{O}_K + (1 + \frac{\sqrt{d}}{2})^2\mathcal{O}_K = 4\mathcal{O}_K + 2(1+\sqrt{t})\mathcal{O}_K + (1+\sqrt{t})^2\mathcal{O}_K$. Therefore, $P^2 \subset 2\mathcal{O}_K$.

Now to show, $2 \in P^2$, we find integer solution for $2 = 4a + 2b(1+\sqrt{t}) + c(1 + 2\sqrt{t} + t)$. Comparing the coefficients we have to find $a, b, c \in \mathbb{Z}$ such that $2 = 4a + 2b + c + ct$ and $0 = 2b + 2c$. So, $b = -c$. So, $4a + c(t-1) = 2$.

We know that $t \equiv 3 \pmod 4$. So $(t-1) \equiv 2 \pmod 4$, i.e. $gcd(4, t-1) = 2$. We can then use Bezout's identity to get integer solutions. Hence, $2 \in P^2$ and therefore, $2\mathcal{O}_K = P^2$.

Conversely let $2\mathcal{O}_K = P^2$, P prime. We need to show that $(\frac{d}{2}) = 0$, i.e., $d \equiv 0 \pmod 4$. If $d \equiv 0 \pmod 4$, then nothing to prove. So, let $d \equiv 1 \pmod 4$. So, $d = t$ and $\mathcal{O}_K = \mathbb{Z} + \mathbb{Z}(\frac{1+\sqrt{t}}{2}) = \mathbb{Z} + \mathbb{Z}(\frac{1+\sqrt{t}}{2})$. Since $P \neq P^2$, there exists $\pi = x + y(\frac{1+\sqrt{d}}{2}) \in P$ such that $\pi \notin P^2$. Hence, x, y are both not even.

Without loss of generality, we can assume that x and y are either 0 or 1. Also, for any $\alpha \in \mathcal{O}_K$, $2\alpha \in 2\mathcal{O}_K$. So, $\pi, \pi + 2\alpha \in P$ but not in P^2.

If $y = 0$, then $x \neq 0$ since otherwise $\pi = 0 \in P^2$. Also, $x \neq 1$ as then $\pi = 1 \notin P$. So, $y = 1$ and x can be 0 or 1. Now, $\pi^2 = (x + \frac{1+\sqrt{d}}{2})^2 = a + b(\frac{1+\sqrt{d}}{2})$, where $a, b \in 2\mathbb{Z}$.

So, $x^2 + 2x(\frac{1+\sqrt{d}}{2}) + \frac{1+d+2\sqrt{d}}{4} = a + \frac{b}{2} + \frac{b}{2}\sqrt{d}$. Upon comparing the coefficients, we get $\frac{b}{2} = x + \frac{1}{2}$, implying b is odd. This is a contradiction.

Therefore, $d \equiv 0 \pmod 4$, i.e., $(\frac{d}{2}) = 0$.

(ii) Let $(\frac{d}{2}) = +1$, then $d \equiv 1 \pmod 8$. So, $d = m$ and $\mathcal{O}_K = \mathbb{Z} + \mathbb{Z}(\frac{1+\sqrt{d}}{2})$.

Define $P = 2\mathcal{O}_K + (\frac{1+\sqrt{d}}{2})\mathcal{O}_K$. So, $PP' = 4\mathcal{O}_K + 2(\frac{1+\sqrt{d}}{2})\mathcal{O}_K + 2(\frac{1-\sqrt{d}}{2})\mathcal{O}_K + (\frac{1-d}{4})\mathcal{O}_K$. So, $PP' \subset 2\mathcal{O}_K$. Now, $2 = (1+\sqrt{d}) + (1-\sqrt{d})$. Thus, $2\mathcal{O}_K \subset PP'$. Therefore, $2\mathcal{O}_K = PP'$.

Now, $P \neq P'$ since if $P = P'$, then $2\mathcal{O}_K = P^2$ and then $(\frac{d}{2}) = 0$. This is a contradiction.

Conversely let $2\mathcal{O}_K = PP'$, $P \neq P'$, P prime. Then, $N(P) = 2$. Also, there exists $\pi = x + y(\frac{d+\sqrt{d}}{2}) \in P$ and $\pi \notin PP' = 2\mathcal{O}_K$. Thus, $x, y \in \mathbb{Z}$ are not both even.

Now, $\pi\mathcal{O}_K = PQ$, where $Q \subset \mathcal{O}_K$. Thus, $2 = N(P) | N(\pi\mathcal{O}_K)(= |N_K(\pi)|)$ and $|N_K(\pi)| = |\pi\pi'| = |\left(\frac{2x+yd}{2}\right)^2 - \frac{y^2d}{4}|$. Hence, $\left(\frac{2x+yd}{2}\right)^2 \equiv \frac{y^2d}{4} \pmod 2$, i.e., $(2x+yd)^2 \equiv y^2d \pmod 8$.

Note that $2 \nmid d$, because if $2|d$, then d is even and $d \equiv 0 \pmod 4$. So, $(\frac{d}{2}) = 0$ and $2\mathcal{O}_K = P^2$ and $P = P'$, which is a contradiction.

If y is even, then $y = 2y_1$, where $y_1 \notin 2\mathbb{Z}$ or $y = 2y_2$, where $y_2 \in 2\mathbb{Z}$.

Case(a) $y = 2y_1$, $2 \nmid y_1$, $y_1 \in \mathbb{Z}$. Then $(2x + 2y_1d)^2 \equiv 4{y_1}^2d \pmod 8$. So, $(x + y_1d)^2 \equiv {y_1}^2d \pmod 2$ and $2 \not| y_1$ and $2 \not| d$. Thus, $2 \not| y_1d$. So, y_1d is odd. Hence, $2 \not| (x + y_1 d)^2$ and thus $x + y_1 d$ is odd. Thus, x is even. This is a contradiction as $\pi \notin 2\mathcal{O}_K$.

Case(b) If $4|y$, then we claim that $4|(2x + yd)$. Now, $4|y$ implies $16|y^2 d$. So at least, $8|(2x + yd)^2$ and thus $16|(2x + yd)^2$. Thus, $4|(2x + yd)$. Again, $2|x$. This is a contradiction. Therefore, y has to be odd.

We can find, $y_2 \in \mathbb{Z}$ such that $y_1 y_2 \equiv 1 \pmod 8$. Then $d \equiv (2x + yd)^2 {y_2}^2 \pmod 8$. Now $2 \not| d$ implies $2|(2x + yd)^2 {y_2}^2$, implying $(2x + yd)^2 {y_2}^2$ is odd, and square of an integer is either $0 \pmod 4$ or $1 \pmod 4$. The case of $0 \pmod 4$ is not possible. So, $(2x + yd)^2 {y_2}^2 \equiv 1 \pmod 4$, i.e., $d \equiv 1 \pmod 8$. Thus, $(\frac{d}{2}) = +1$.

(iii) As before, the validity of (iii) is an immediate consequence of (i) and (ii). □

Chapter 4

Minkowski Theory and Finiteness of the class group

4.1 Lattices

Definition 4.1. *Let V be an n-dimensional $\mathbb{R}$- vector space. A **lattice** in V is a subgroup of the form $\Gamma = \mathbb{Z}v_1 + \mathbb{Z}v_2 + \cdots + \mathbb{Z}v_m$, with linearly independent vectors $v_1, v_2, \ldots, v_m$ of V. The m-tuple $(v_1, v_2, \ldots, v_m)$ is called a **basis**, and the set*

$$\Phi = \{x_1v_1 + \cdots + x_mv_m | x_i \in \mathbb{R}, 0 \leq x_i < 1\}$$

*is called the **fundamental mesh** of the lattice.*

The lattice is called **complete** or a $\mathbb{Z}$-structure of V if $m = n$, which implies that the set of all translates $\Phi + \gamma$, where $\gamma \in \Gamma$, of the fundamental mesh covers the entire space V.

A lattice is a finitely-generated subgroup of V. But not every finitely-generated subgroup is a lattice.

Example 4.1. $\Gamma = \mathbb{Z} + \mathbb{Z}[\sqrt{2}] \subset \mathbb{R}$ *is not a lattice.*

We know $\sqrt{2} - 1 \in \mathbb{Z}[\sqrt{2}]$, which implies $a_n = (\sqrt{2} - 1)^n \in \mathbb{Z}[\sqrt{2}]$, for every $n \in \mathbb{N}$.

Now, $\lim_{n\to\infty} a_n = 0 \in \mathbb{Z}[\sqrt{2}]$ is a limit point of the lattice. Hence, Γ is not discrete.

But each lattice $\Gamma = \mathbb{Z}v_1 + \mathbb{Z}v_2 + \cdots + \mathbb{Z}v_m$ is a discrete subgroup of V, i.e., any $\gamma \in \Gamma$ is an isolated point, i.e., there exists a neighbourhood which contains no other point of Γ.

The above definition makes use of a choice of linearly independent vectors. We will now give a characterisation of lattices which is independent of such a choice.

Proposition 4.1. *(Characterisation of lattices) A subgroup $\Gamma \subset V$ is a lattice if and only if it is discrete.*

Proof. If Γ is a lattice, then it is discrete by definition.

Conversely, let Γ be a discrete subgroup of V.

Claim : Γ is closed.

Proof : Let U be an open neighbourhood of 0. Then there exists $U' \subset U$, a neighbourhood of 0 such that the difference of every element of U' lies in U.

Now every U contains an open neighbourhood of 0 of the form $\prod\limits_{i=1}^{n}(-\epsilon_i, \epsilon_i)$. Then we can choose U' accordingly. Also, V is a Hausdorff space. Now, if there exists $x \notin \Gamma$ but $x \in \bar{\Gamma}$. Then x is a limit point of Γ, i.e., there exists $y_1 \in \Gamma$ such that $y_1 \in x + U'$. Also, there exists V', an open neighbourhood of $x \in x + U'$ such that $y_1 \notin V'$. But since x is a limit point, there exists $y_2 \in \Gamma$ such that $y_2 \in x + U'$. And $y_1 \neq y_2$.

Now $y_1, y_2 \in x+U'$, implies that there exists $x_1, x_2 \in U'$ such that $y_1 = x+x_1$ and $y_2 = x + x_2$.

$$0 \neq y_1 - y_2 = x_1 - x_2 \in U' - U' \subset U.$$

Since Γ is a subgroup of V, this implies $\gamma = y_1 - y_2 \neq 0 \in \Gamma$ and also belongs to U. Thus, 0 is not an isolated point, implying Γ is closed. Now we need to show that Γ is a lattice.

Let V_0 be a linear subspace of V, which is spanned by the set Γ, and m be its dimension. Then we may choose a basis $u_1, u_2, \ldots, u_m$ of V_0 which is contained in Γ and form the complete lattice $\Gamma_0 = \mathbb{Z}u_1 + \mathbb{Z}u_2 + \cdots + \mathbb{Z}u_m \subset \Gamma$ of V_0.

Claim : $[\Gamma : \Gamma_0]$ is finite.

Proof : Let $\gamma_i \in \Gamma$ vary over a system of representatives of Γ/Γ_0. Since Γ_0 is complete in V_0, the translates $\Phi_0 + \gamma$ of the fundamental mesh

$$\Phi_0 = \{x_1u_1 + \cdots + x_mu_m \; |x_i \in \mathbb{R}, 0 \leq x_i < 1\},$$

where $\gamma \in \Gamma_0$, covers the entire V_0. Therefore, $\gamma_i = \mu_i + \gamma_{0i}$, where $\mu_i \in \Phi_0$ and $\gamma_{0i} \in \Gamma_0 \subset V_0$.

As the $\mu_i = \gamma_i - \gamma_{0i} \in \Gamma$ lie discretely in the bounded set Φ_0, the have to be finite in number (since, closed and bounded discrete set is finite). In fact, $\Gamma \cap \bar{\Phi_0}$ is compact and discrete, hence finite. Put $q = [\Gamma : \Gamma_0]$, we have $q\Gamma \subset \Gamma_0$. Because for every $\gamma + \Gamma_0 \in \Gamma/\Gamma_0$, $q(\gamma + \Gamma_0) = 0 + \Gamma_0$. But $q(\gamma + \Gamma_0)$, implies that $q\gamma \in \Gamma_0$. Hence, $q\Gamma \subset \Gamma_0$.

This implies, $\Gamma \subset \frac{1}{q}\Gamma_0 = \mathbb{Z}(\frac{1}{q}u_1) + \cdots + \mathbb{Z}(\frac{1}{q}u_m)$. By Fundamental theorem of finitely-generated abelian groups, Γ admits a $\mathbb{Z}$-basis $v_1, v_2, \ldots, v_r$; $r \leq m$, i.e., $\Gamma = \mathbb{Z}v_1 + \cdots + \mathbb{Z}v_r$.

The vectors $v_1, \ldots, v_r$ are $\mathbb{R}$-linearly independent and span the m-dimensional vector space V_0. Therefore, $r = m$.

This shows Γ is a lattice. □

Proposition 4.2. *(Criterion for complete lattices) A lattice $\Gamma \in V$ is complete if and only if there exists a bounded subset $M \subset V$ such that the collection of all the translates $M + \gamma$, for $\gamma \in \Gamma$ covers the entire space V.*

Proof. If $\Gamma = \mathbb{Z}v_1 + \mathbb{Z}v_2 + \cdots + \mathbb{Z}v_n$ is complete, then take $M = \Phi_0$, where $\Phi_0 = \{x_1v_1 + \cdots + x_nv_n \mid 0 \leq x_i < 1\}$.

Conversely, Let M be a bounded subset of V whose translates $M + \gamma$, for $\gamma \in \Gamma$ covers V. Let V_0 be the subspace spanned by Γ. We have to show that $V = V_0$ i.e., to show that $V \subset V_0$.

Let $v \in V$. Since $V = \bigcup_{\gamma \in \Gamma} (M + \gamma)$. Then, $v = a + \gamma_0$, where $a \in M; \gamma_0 \in \Gamma$. Also, for every $l \in \mathbb{N}$, $lv = a_l + \gamma_l$, where $a_l \in M; \gamma_l \in \Gamma \subset V_0$.

Also, the sequence $(\frac{1}{l})$ is bounded, implying the sequence $(\frac{a_l}{l})$ is bounded. Hence, $(\frac{a_l}{l}) \longrightarrow 0$ as $l \longrightarrow \infty$.

$$v = \lim_{l \to \infty} \frac{1}{l} a_l + \lim_{l \to \infty} \frac{1}{l} \gamma_l = \lim_{l \to \infty} \frac{1}{l} \gamma_l \in V_0.$$

Since V_0 is closed, $v \in V_0$.

Thus, Γ is a complete lattice. □

Let V be an Euclidean vector space, i.e., an $\mathbb{R}$-vector space of finite dimension n, with a symmetric, positive definite bilinear form

$$\langle\ ,\ \rangle : V \times V \longrightarrow \mathbb{R},$$

i.e., $\langle v_1, v_2\rangle = \langle v_2, v_1\rangle$ for every $v_1, v_2 \in V$ and $\langle v, v\rangle\ > 0$ for every $v \neq 0$. Then we have on V a notion of volume - more precisely, a Haar measure.

The cube spanned by the orthonormal basis $\{e_1, e_2, \ldots, e_n\}$ has volume 1. The parallelepiped spanned by n linearly independent vectors $v_1, v_2, \ldots, v_n$,

$$\Phi = \{x_1v_1 + \cdots + x_nv_n\ |x_i \in \mathbb{R}, 0 \leq x_i < 1\}$$

has volume, $Vol(\Phi) = |det(A)|$, where $A = (a_{ik})$ is the change of basis matrix, $v_i = \sum\limits_k a_{ik}e_k$. Hence,

$$(\langle v_i, v_j\rangle) = \big(\sum_{k,l} a_{ik}a_{jl}\langle e_k, e_l\rangle\big) = \big(\sum_k a_{ik}a_{jk}\big) = AA^T,$$

and $Vol(\Phi) = |det(\langle v_i, v_j\rangle)|^{\frac{1}{2}}$. Let Γ be the lattice spanned by $v_1, v_2, \ldots, v_n$. Then Φ is a fundamental mesh of Γ and $Vol(\Gamma)$ is defined to be $Vol(\Phi)$.

This also shows that *a lattice is complete if and only if the volume of its fundamental mesh is non-zero.*

Further, this volume is independent of the choice of basis $v_1, \ldots, v_n$ of the lattice because the change of basis matrix has determinant ±1, so that the set Φ is transformed into a set of same volume.

Definition 4.2. *A subset X of V is called* ***centrally symmetric****, if given any point $x \in X$, the point $-x \in X$.*

It is called ***convex*** *if given any two points $x, y \in X$, $\{ty+(1-t)x\ |0 \leq t \leq 1\}$.*

Theorem 4.1. *(**Minkowski's Lattice Point Theorem**) Let Γ be a complete lattice in the Euclidean vector space V and X a centrally symmetric, convex subset of V. Suppose that $Vol(X) > 2^nVol(\Gamma)$. Then X contains at least $\gamma \neq 0 \in \Gamma$.*

Proof. It is enough to show that there exist two distinct lattice points $\gamma_1, \gamma_2 \in \Gamma$ such that

$$(\frac{1}{2}X + \gamma_1)\bigcap(\frac{1}{2}X + \gamma_2) \neq \phi.$$

Choose a point in the intersection,

$$\frac{1}{2}x_1 + \gamma_1 = \frac{1}{2}x_2 + \gamma_2,$$

where $x_1, x_2 \in X$. This implies,

$$\gamma = \gamma_1 - \gamma_2 = \frac{1}{2}x_2 - \frac{1}{2}x_1,$$

which is the centre of the line segment joining $x_2, -x_1$ and thus $\in X \cap \Gamma$.

Now, if the sets $\frac{1}{2}X + \gamma; \gamma \in \Gamma$ were pairwise disjoint, then the same would be true of their intersections $\Phi \cap (\frac{1}{2}X + \gamma)$ with a fundamental mesh Φ of Γ, i.e., we would have

$$Vol(\Phi) \geq \sum_{\gamma \in \Gamma} Vol\big(\Phi \cap (\frac{1}{2}X + \gamma)\big).$$

But translation of $\Phi \cap (\frac{1}{2}X + \gamma)$ by γ created the set $(\Phi - \gamma) \cap \frac{1}{2}X$ of equal volume and $\Phi - \gamma$, for $\gamma \in \Gamma$ covers the entire space V, thus also the set $\frac{1}{2}X$.

This implies,

$$Vol(\Phi) \geq \sum_{\gamma \in \Gamma} Vol\big((\Phi - \gamma) \cap \frac{1}{2}X\big) \geq Vol(\frac{1}{2}X) = \frac{1}{2^n} Vol(X).$$

This is a contradiction to the hypothesis that $Vol(X) > 2^n Vol(\Gamma)$. □

Minkowski's lattice point theorem cannot be improved, as can be seen by taking $X = (-1, 1)$ and $\Gamma = \mathbb{Z}$ in $\mathbb{R}$. If X is compact, however, then the statement of the theorem does remain true even if $Vol(X) \geq 2^n Vol(\Gamma)$.

4.2 Minkowski Theory

Let K be a number field of degree n. In the present section, consider the canonical mapping

$$j : K \longrightarrow K_{\mathbb{C}} := \prod_{\tau} \text{ defined by } a \longmapsto j(a) = (\tau(a)),$$

which results from the n distinct embeddings of K into $\mathbb{C}$.

Let $\tau_1, \ldots, \tau_r$ be the real embeddings; $\tau_{r+1}, \ldots, \tau_{r+s}$ be the distinct complex embeddings up to complex conjugation; and let $\tau_{r+s+1}, \ldots, \tau_{r+2s}$ are such that $\overline{\tau_{r+i}} = \tau_{r+s+i}$, for $1 \leq i \leq s$.

The $\mathbb{C}$-vector space $K_{\mathbb{C}}$ is equipped with the Hermitian scalar product

$$\langle \underline{x}, \underline{y} \rangle = \sum_{\tau} x_\tau \overline{y_\tau}$$

The Galois group $Gal_{\mathbb{R}}(\mathbb{C})$ is generated by the complex conjugation $F : \mathbb{C} \longrightarrow \mathbb{C}$ sending $z \longmapsto \bar{z}$ and $F^2 = Id_{\mathbb{C}}$.

Consider the map,

$$F_1 : K_{\mathbb{C}} \longrightarrow K_{\mathbb{C}},$$

i.e., $F_1 : \mathbb{C}^n \longrightarrow \mathbb{C}^n$, such that $F_1((x_i)) = (\bar{x_i})$. Also, F induces a map from $Em(K, \mathbb{C})$ to $Em(K, \mathbb{C})$, $\tau \longmapsto \bar{\tau}$, where $Em(K, \mathbb{C})$ denotes the group of embeddings of K into $\mathbb{C}$.

Define a new map

$$\tilde{F} : K_{\mathbb{C}} \longrightarrow K_{\mathbb{C}}$$

$$\begin{aligned} &\tilde{F}(z_1, \ldots, z_r, z_{r+1}, \ldots, z_{r+s}, z_{r+s+1}, \ldots, z_{r+2s}) \\ &= (\bar{z}_1, \ldots, \bar{z}_r, \overline{z_{r+s+1}}, \ldots, \overline{z_{r+2s}}, \overline{z_{r+1}}, \ldots, \overline{z_{r+s}}). \end{aligned}$$

Note that the scalar product becomes $\langle \tilde{F}\underline{x}, \tilde{F}\underline{y} \rangle = F\langle \underline{x}, \underline{y} \rangle$.

Finally, we can define the linear map

$$Tr : \mathbb{C}^n \longrightarrow \mathbb{C} \ ; \ Tr(\underline{x}) = \sum_{i=1}^{n} x_i,$$

where $\underline{x} = (x_i) \in \mathbb{C}^n$. Hence we see that the map Tr is F-equivariant, i.e. $Tr(\tilde{F}(\underline{x})) = Tr(F_1(\underline{x})) = F(Tr(\underline{x}))$. The composite $K \xrightarrow{j} K_{\mathbb{C}} \xrightarrow{Tr} \mathbb{C}$, gives the usual trace of K over $\mathbb{Q}$. Also, $Tr_{K/\mathbb{Q}}$ is F-invariant, i.e. $Tr_{K/\mathbb{Q}}(F(\alpha)) = Tr_{K/\mathbb{Q}}(\alpha)$.

We now concentrate on the $\mathbb{R}$-vector space $K_{\mathbb{R}}$, which is the $\tilde{F}$-invariant subspace of $K_{\mathbb{C}}(= \mathbb{C}^n)$, i.e.,

$$K_{\mathbb{R}} = \{\underline{z} = (z_i) \in \mathbb{C}^n \ | z_i = \overline{z_i} \text{ for } 1 \leq i \leq r \ ; z_{r+i} = \overline{z_{r+s+i}} \text{ for } 1 \leq i \leq s\}.$$

Note that $K_{\mathbb{R}}$ is an $\mathbb{R}$-module, and hence a $\mathbb{R}$-vector space.

Now, it is easy to see that $j(K) \subset K_{\mathbb{R}}$. Hence, we can define the map $j : K \longrightarrow K_{\mathbb{R}}$. So, $\tilde{F}(j(\alpha)) = j(\alpha)$, for every $\alpha \in K$.

Let us now restrict the hermitian scalar product $\langle \ , \ \rangle$ from $K_{\mathbb{C}}$ to $K_{\mathbb{R}}$.

$$\langle \ , \ \rangle : K_{\mathbb{C}} \times K_{\mathbb{C}} \longrightarrow \mathbb{C}$$

$$\langle\ ,\ \rangle\big|_{K_{\mathbb{R}}\times K_{\mathbb{R}}\to\mathbb{R}}$$

Let $\underline{x}, \underline{y} \in K_{\mathbb{R}}$.

$$\langle \underline{x}, \underline{y}\rangle = \sum_{i=1}^{n} x_i\bar{y_i} = \sum_{i=1}^{r} x_i y_i + \sum_{i=1}^{s} x_{r+i}\ \overline{y_{r+i}} + \sum_{i=1}^{s} x_{r+s+i}\ \overline{y_{r+s+i}}.$$

This inner product is a real inner product.

We call the Euclidean vector space $K_{\mathbb{R}}$ the **Minkowski space**, its scalar product $\langle\ ,\ \rangle$ the **canonical metric**, and the associated Haar measure the **canonical measure**.

Also, we have the trace map $Tr : K_{\mathbb{R}} \longrightarrow \mathbb{R}$ and its composite with $j : K \longrightarrow K_{\mathbb{R}}$ gives us the trace map $Tr_{K/\mathbb{Q}}$, i.e. $Tr \circ j = Tr_{K/\mathbb{Q}}$.

Proposition 4.3. *There is an isomorphism $f : K_{\mathbb{R}} \longrightarrow \prod_{\tau} \mathbb{R} = \mathbb{R}^{r+2s}$, such that $(z_i) \longmapsto (x_i)$, where*

$$f((z_i)) = (x_i) = \begin{cases} z_i & \text{if } 1 \le i \le r \\ Re(z_i) & \text{if } r+1 \le i \le r+s \\ Im(z_{i-s}) & \text{if } r+s+1 \le i \le r+2s \end{cases}$$

This isomorphism transforms the canonical metric $\langle\ ,\ \rangle$ into a scalar product,. Let $\underline{x}, \underline{y} \in K_{\mathbb{R}}$,then

$$(\underline{x}, \underline{y}) = \sum_{\tau} \alpha_\tau x_\tau y_\tau,$$

where $\alpha_\tau = 1$, if τ is real; and $\alpha_\tau = 2$, if τ is complex.

Proof. Let $(z_i) \in ker f$. Then $x_i = z_i = 0$ for $1 \le i \le r$, $x_{r+i} = Re(z_{r+i}) = 0$ for $1 \le i \le s$, and $x_{r+s+i} = Im(z_{r+i}) = 0$ for $1 \le i \le s$. Hence, $(z_i) = (0)$. Therefore, f is injective.

Since $K_{\mathbb{R}}$ and $\mathbb{R}^{r+2s}$ are finite-dimensional vector spaces, the map f is also surjective.

Thus, f is an isomorphism.

If $\underline{z} = (z_i) = (a_i + ib_i)$ and $\underline{z'} = (z'_i) = (c_i + id_i)$ are in $K_{\mathbb{R}}$, then

$$\langle \underline{z}, \underline{z'}\rangle = \sum_{\tau} z_i \bar{z'_i} = \sum_{i=1}^{r} a_i c_i + \sum_{i=r+1}^{r+s} (a_i + ib_i)(c_i - id_i) + \sum_{i=r+s+i}^{r+2s} (a_i + ib_i)(c_i - id_i)$$

$$= \sum_{i=1}^{r} a_i c_i + \sum_{i=r+1}^{r+s} (a_i + ib_i)(\overline{c_i + id_i}) + \sum_{i=r+i}^{r+s} (\overline{a_i + ib_i})(\overline{\overline{c_i + id_i}})$$

$$= \sum_{i=1}^{r} a_i c_i + \sum_{r+1}^{r+s} 2 \cdot Re[(a_i + ib_i)(c_i - id_i)]$$

$$= \sum_{i=1}^{r} a_i c_i + \sum_{r+1}^{r+s} 2 \cdot (a_i c_i + b_i d_i)$$

Now, for $(x_i) = f((z_i))$ and $(y_i) = f((z_i'))$, then in $\mathbb{R}^{r+2s}$ under the map f, we have

$$(\underline{x}, \underline{y}) = \sum_{\tau_1}^{\tau_{r+2s}} x_i y_i = \sum_{\tau_1}^{\tau_r} a_i c_i + \sum_{\tau_{r+1}}^{\tau_{r+s}} (a_i c_i + b_i d_i) + \sum_{\tau_{r+s+1}}^{\tau_{r+2s}} (a_i c_i + (-b_i)(-d_i))$$

$$= \sum_{i=1}^{r} a_i c_i + \sum_{r+1}^{r+s} 2 \cdot (a_i c_i + b_i d_i) = \langle \underline{z}, \underline{z'} \rangle.$$

□

The scalar product defined above transfers the canonical measure from $K_{\mathbb{R}}$ to $\mathbb{R}^{r+2s}$. It differs from the standard Lebesgue measure by

$$Vol_{canonical}(X) = 2^s \; Vol_{Lebesgue}(f(X)).$$

Now the next proposition will give us examples of lattices in the Minkowski space $K_{\mathbb{R}}$.

Proposition 4.4. *If $I \neq 0$ is an ideal of $\mathcal{O}_K$, then $\Gamma = j(I)$ is a complete lattice in $K_{\mathbb{R}}$. Its fundamental mesh has volume*

$$Vol(\Gamma) = \sqrt{|d_K|} N(I),$$

where $N(I)$ is the norm of the integral ideal I.

Proof. Let $\alpha_1, \alpha_2, \ldots, \alpha_n$ be a $\mathbb{Z}$-basis of I. So, $\Gamma = \mathbb{Z}j(\alpha_1) + \cdots + \mathbb{Z}j(\alpha_n)$.

Choose a numbering of the embeddings $\tau : K \longrightarrow \mathbb{C}$ as $\tau_1, \ldots, \tau_n$ and form a matrix $A = (\tau_l(\alpha_i))_{n \times n}$.

$$\mathscr{D}(I) = \mathscr{D}(\alpha_1, \ldots, \alpha_n) = (det A)^2 = (N(I))^2 \cdot d_K.$$

Also,

$$det(\langle j(\alpha_i), j(\alpha_k)\rangle)_{n\times n} = \big(\sum_{i=1}^{n} \tau_l(\alpha_i)\overline{\tau_l}(\alpha_k)\big) = det(A\bar{A}^T) = detA \cdot det\bar{A}$$

$$= detA \cdot \overline{detA} = |detA|^2.$$

So,

$$Vol(\Gamma) = \big|det(\langle j(\alpha_i), j(\alpha_k)\rangle)\big|^{\frac{1}{2}} = |detA| = \sqrt{|d_K|}N(I).$$

□

Using this proposition and Minkowski's lattice point theorem, we get:

Theorem 4.2. *Let $I \neq 0$ be an integral ideal of K and let $c_{\tau_i} = c_i > 0$ for $\tau_i \in Hom(K, \mathbb{C})$ be real numbers such that $c_{\tau_i} = c_{\overline{\tau_i}}$ and*

$$\prod_{\tau} c_i > A \cdot N(I),$$

where $A = \left(\frac{2}{\pi}\right)^s \sqrt{|d_K|}$. Then there exists $a \in I$ and $a \neq 0$ such that

$$|\tau_i(a)| < c_i, \text{ for every } \tau_i \in Hom(K,\, \mathbb{C}).$$

Proof. The set $X = \{(z_i) \in K_{\mathbb{R}}\big|\ |z_i| < c_i\}$ is centrally symmetric and convex. Its volume $Vol(X)$ can be computed via

$$f : K_{\mathbb{R}} \to \prod_{\tau} \mathbb{R}$$
$$(z_i) \mapsto (x_i),$$

where

$$f((z_i)) = (x_i) = \begin{cases} z_i & \text{if } 1 \leq i \leq r \\ Re(z_i) & \text{if } r+1 \leq i \leq r+s \\ Im(z_{i-s}) & \text{if } r+s+1 \leq i \leq r+2s. \end{cases}$$

Hence,

$$f(X) = \{(x_i) \in \prod_{\tau} \mathbb{R}\big|\ |x_i| < c_i \text{ for } 1 \leq i \leq r;\ x_i^2 + x_{i+s}^2 < c_i^2 \text{ for } r+1 \leq i \leq r+s\}$$

The canonical volume of X comes out to be 2^s times the Lebesgue volume of the image.

$$Vol_{can}(X) = 2^s \; Vol_{Leb}(f(X)) = 2^s \prod_{i=1}^{r}(2 \; c_i) \prod_{i=r+1}^{i=r+2s}(\pi c_i^2) = 2^{r+s}\pi^s \prod_i c_i.$$

Now, using the previous proposition,

$$Vol_{can}(X) > 2^{r+s}\pi^s \big(\frac{2}{\pi}\big)^s \sqrt{|d_K|}N(I) = 2^n Vol(\Gamma).$$

Thus the hypothesis of Minkowski's lattice point theorem is satisfied. So, there exists a point $j(a) \in X$, $a \neq 0 \in I$. In other words,

$$|\tau_i(a)| < c_i, \text{ for every } \tau_i \in \text{Hom(K, } \mathbb{C}).$$

□

There is a multiplicative version of Minkowski theory. It is based on the homomorphism

$$j : K^* \longrightarrow K^*_{\mathbb{C}} = \prod_\tau \mathbb{C}^*$$

The multiplicative group $K^*_{\mathbb{C}}$ admits the homomorphism,

$$N : K^*_{\mathbb{C}} \longrightarrow \mathbb{C}^*$$

given by the product of coordinates. The composite

$$K^* \xrightarrow{j} K^*_{\mathbb{C}} \xrightarrow{N} \mathbb{C}^*$$

is the usual norm of K over $\mathbb{Q}$. $N_{K/\mathbb{Q}}(a) = N(j(a))$.

In order to produce a lattice from the multiplicative theory, we use the logarithm to pass from multiplicative to additive groups.

$$\begin{aligned} l : \mathbb{C}^* &\longrightarrow \mathbb{R} \\ z &\longmapsto log|z| \end{aligned}$$

The image of $K^*_{\mathbb{R}}$ under the map l lies in the set $\Big[\prod_\tau \mathbb{R}\Big]^+ = \{(x_i) \in \prod_\tau \mathbb{R} \; | x_1, x_2, \ldots, x_r \in \mathbb{R}; x_{r+i} = \overline{x_{r+s+i}} \; , 1 \leq i \leq s\}$.

It induces a surjective homomorphism

$$\begin{aligned} \tilde{l} : K_{\mathbb{C}}^{+} &\longrightarrow \prod_{\tau} \mathbb{R} \\ (z_\tau) &\longmapsto (log|z_\tau|), \end{aligned}$$

and we can obtain the commutative diagram

$$\begin{tikzcd} K^* \arrow[r, "j"] \arrow[d, "N_{K/\mathbb{Q}}"'] & K_{\mathbb{C}}^* \arrow[r, "\tilde{l}"] \arrow[d, "N"] & \prod_{\tau} \mathbb{R} \arrow[d, "Tr"'] \\ \mathbb{Q}^* \arrow[r, "i"] & \mathbb{C}^* \arrow[r, "l"] & \mathbb{R} \end{tikzcd}$$

The involution $F \in Gal_{\mathbb{R}}(\mathbb{C})$ acts on all groups trivially on K^*, the map $\tilde{F}$ on $K_{\mathbb{C}}*$ as before, and on points $x \in \prod_{\tau} \mathbb{R}$ by $\tau_i(\tilde{F}(x)) = \bar{\tau}_i(x)$.

We have,

$$\begin{aligned} \tilde{F} \circ j &= j, \\ \tilde{F} \circ \tilde{l} &= \tilde{l} \circ \tilde{F}, \\ N \circ \tilde{F} &= F \circ N, \\ Tr \circ \tilde{F} &= Tr. \end{aligned}$$

We now pass to the fixed modules under $Gal_{\mathbb{R}}(\mathbb{C})$ and obtain the following diagram:

$$\begin{tikzcd} K^* \arrow[r, "j"] \arrow[d, "N_{K/\mathbb{Q}}"'] & K_{\mathbb{R}}^* \arrow[r, "\tilde{l}"] \arrow[d, "N"] & \left[\prod_{\tau} \mathbb{R}\right]^+ \arrow[d, "Tr"'] \\ \mathbb{Q}^* \arrow[r, "i"] & \mathbb{R}^* \arrow[r, "l"] & \mathbb{R} \end{tikzcd}$$

The $\mathbb{R}$-vector space $\left[\prod_{\tau} \mathbb{R}\right]^+$ is explicitly given as follows.

Separate as before the embeddings $\tau : K \longrightarrow \mathbb{C}$ into real ones $\tau_1, \dots, \tau_r$ and pairs of complex conjugate ones $\tau_{r+1}, \overline{\tau_{r+1}}, \dots, \tau_{r+s}, \overline{\tau_{r+s}}$. We obtain a decomposition analogous to the one for $\left[\prod_{\tau} \mathbb{C}\right]^+$.

$$\left[\prod_{\tau} \mathbb{R}\right]^+ = \prod_{i=1}^{r} \mathbb{R} \times \prod_{i=r+1}^{r+s} [\mathbb{R} \times \mathbb{R}]^+.$$

The factor $[\mathbb{R}\times\mathbb{R}]^+$ now consists of points (x,x) and we identify with $\mathbb{R}$ by the map $(x,x)\longmapsto 2x$. In this way we obtain an isomorphism

$$[\prod_\tau \mathbb{R}]^+ \cong \mathbb{R}^{r+s},$$

which transforms the map $Tr : \big[\prod_\tau \mathbb{R}\big]^+ \longrightarrow \mathbb{R}$ into the usual map

$$Tr : \mathbb{R}^{r+s} \longrightarrow \mathbb{R},$$

given by the sum of coordinates.

Identifying $\big[\prod_\tau \mathbb{R}\big]^+$ with $\mathbb{R}^{r+s}$, the homomorphism

$$\tilde{\tilde{l}} : K^*_\mathbb{R} \longrightarrow \mathbb{R}^{r+s}$$

is given by

$$\tilde{\tilde{l}}(x_i) = (log|x_1|,\ldots,log|x_r|,log|x_{r+1}|^2,\ldots,log|x_{r+s}|^2),$$

where $(x_i)\in K^*_\mathbb{R}\subset \prod_\tau \mathbb{C}^*$.

4.3 Class group

Let K be a number field of degree n. The non-zero fractional ideals in K form a multiplicative group which we denote by $\triangle$. The ring $\mathcal{O}_K$ of algebraic integers is the identity element of $\triangle$.

A fractional ideal in K is said to be *principal* if it is of the form $\alpha\mathcal{O}_K$ with $\alpha\in K$. The principal fractional ideals $I\neq 0$ forms a subgroup Π of $\triangle$. The quotient group $\mathcal{H}_K = \triangle/\Pi$ is called the *group of ideal classes* in K or the **class group of K**.

The order of $\mathcal{H}_K$, denoted by h_K is called the **class number** of K. If $h_K = 1$, then $\mathcal{O}_K$ is a principal ideal domain.

Two fractional ideals $I, J\neq 0$ in K are therefore in the same ideal class if and only if $I = (\alpha)J$ for some $\alpha\in K$. In that case they are said to be **equivalent**.

4.3.1 Finiteness of class group

The aim of this subsection is to prove that the class number of a number field K is finite. But we need a lemma first.

Lemma 4.1. *In every integral ideal $I \neq 0$, there exists $a \in I$, $a \neq 0$ such that*

$$|N_{K/\mathbb{Q}}(a)| \leq \big(\frac{2}{\pi}\big)^s \sqrt{|d_K|} N(I).$$

Proof. Given $\epsilon > 0$, we choose positive real numbers c_i for $\tau_i \in Hom(K, \mathbb{C})$ such that for the complex conjugate homomorphisms τ_i and $\overline{\tau_i}$, $c_i = c_{s+i}$ for $r+1 \leq i \leq r+s$ and

$$\prod_{i=1}^{n} c_i = \big(\frac{2}{\pi}\big)^s \sqrt{|d_K|} N(I) + \epsilon.$$

Then by Theorem 4.2, there exists $a \neq 0 \in I$, satisfying $|\tau_i(a)| < c_i$.

Thus, $|N_{K/\mathbb{Q}}(a)| = \big(\frac{2}{\pi}\big)^s \sqrt{|d_K|} N(I) + \epsilon$. This is true for all $\epsilon > 0$.

Hence,

$$|N_{K/\mathbb{Q}}(a)| \leq \big(\frac{2}{\pi}\big)^s \sqrt{|d_K|} N(I).$$

□

As a first application of Minkowski theory, we are going to show that the ideal class group $\mathcal{H}_K$ of an algebraic number field is finite.

Theorem 4.3. *The ideal class group $\mathcal{H}_K = \triangle/\Pi$ is finite.*

Proof. If $P \neq 0$ is a prime ideal of $\mathcal{O}_K$ and $P \cap \mathbb{Z} = p\mathbb{Z}$. Then $\mathcal{O}_K/P$ is a finite field extension of $\mathbb{Z}/p\mathbb{Z}$ of degree say $f \geq 1$, we have $N(P) = p^f$.

Given a p, there exist only finitely many prime ideals P such that $P \cap \mathbb{Z} = p\mathbb{Z}$ (because this means $P | \langle p \rangle$ and by Dedekind's theorem, it has only finitely many prime ideals in its decomposition and each of them is maximal).

Hence there are only finitely many prime ideals with bounded norm. Since every integral ideal admits a representation $I = P_1^{v_1} \ldots P_r^{v_r}$, where $v_i > 0$ and $N(I) = N(P_1)^{v_1} \ldots N(P_r)^{v_r}$, and altogether only a finite number of ideals I of $\mathcal{O}_K$ with $N(I) \leq M$, for a given M.

It therefore suffices to show that each ideal class $[I]$ of $\mathcal{H}_K$ contains an integral ideal I_1 such that

$$N(I_1) \leq M = \big(\frac{2}{\pi}\big)^s \sqrt{|d_K|}.$$

For this, choose an arbitrary representation I of the class, and a $\gamma \in \mathcal{O}_K$, $\gamma \neq 0$ such that $J = \gamma I^{-1} \subset \mathcal{O}_K$.

By the previous lemma, there exists $\alpha \in J$, $\alpha \neq 0$ such that

$$|N_{K/\mathbb{Q}}(\alpha)| \leq M \cdot N(J).$$

This implies

$$|N_{K/\mathbb{Q}}(\alpha)| \; N(J)^{-1} = N(\langle\alpha\rangle) \cdot N(J^{-1}) = N(\langle\alpha\rangle \cdot J^{-1}) = N(\alpha J^{-1}) \leq M.$$

The ideal $I_1 = \alpha J^{-1} = \alpha\gamma^{-1} I \in [I]$. □

4.4 Minkowski bound

Consider the set $X_t = \{(x_i) \in K_{\mathbb{R}} | \sum\limits_i |x_i| < t\}$. This set is convex and centrally symmetric. We know the map $f : K_{\mathbb{R}} \longrightarrow \prod\limits_\tau \mathbb{R} = \mathbb{R}^{r+2s}$. Now consider a map

$$g : \mathbb{R}^{r+2s} \longrightarrow \mathbb{R}^r \times \mathbb{C}^s$$

such that,

$$(x_1, x_2, \ldots, x_r, y_1, \ldots, y_s, y_{s+1}, \ldots, y_{2s}) \longmapsto (x_1, \ldots, x_r, y_1 + iy_{s+1}, \ldots, y_s + iy_{2s}).$$

This map g is an isometric isomorphism.

Now look at the image of X_t under function composition $g \circ f$, call it B_t. Then

$$B_t = \left\{ (y_1, \ldots, y_r, z_1, \ldots, z_s) \in \mathbb{R}^r \times \mathbb{C}^s \mid \sum_{i=1}^r |y_i| + 2 \sum_{j=1}^s |z_j| \leq t \right\}$$

for $t \geq 0$. Since g is an isometric isomorphism, we can see that

$$Vol(B_t) = Vol(g \circ f(X_t)) = Vol(f(X_t)).$$

Hence, to show that the canonical volume of the set X_t, we will use n-dimensional integration on the set B_t. We will show that the $Vol_{Leb}(B_t) = 2^r(\frac{\pi}{2})^s \frac{t^n}{n!}$. Then $Vol_{Can}(X_t) = 2^s Vol_{Leb}(B_t)$, i.e the canonical volume of the set X_t is $\frac{2^r \pi^s t^n}{n!}$.

Proposition 4.5. *The* $Vol_{Leb}(B_t) = V(r,s,t) = 2^r \left(\frac{\pi}{2}\right)^s \frac{t^n}{n!}$.

Proof. The proof is by double induction on r and s.

If $r = 1$ and $s = 0$. Hence $n = 1$. We are calculating the length of $[-t, t]$, which is $2t$ as predicted.

If $r = 0$ and $s = 1$, then $n = 2$. We are calculating the area of

$$\{z_1 \in \mathbb{C} \mid 2|z_1| \leq t\},$$

which is a disc of radius $t/2$ and hence the resulting volume is $\frac{\pi t^2}{4}$.

Now assume that the formula holds for r, s and all t. Then $V(r+1, s, t)$ is the volume of the set described by

$$|y| + \sum_{i=1}^{r} |y_i| + 2\sum_{j=1}^{s} \leq t,$$

i.e.,

$$\sum_{i=1}^{r} |y_i| + 2\sum_{j=1}^{s} \leq t - |y|.$$

Now if $|y| > t$, then B_t is empty.

For smaller values of $|y|$, suppose we change $|y|$ to $|y| + dy$. This creates a box in $(n+1)$-space with dy as one of its dimensions. The volume of the box is $V(r, s, t - |y|)dy$.

Thus, $V(r+1, s, t) = \int\limits_{-t}^{t} V(r, s, t - |y|)dy = 2\int\limits_{0}^{t} 2^r \left(\frac{\pi}{2}\right)^s \left(\frac{(t-y)^n}{n!}\right) dy$

$$= \frac{2^{r+1}}{n!} \left(\frac{\pi}{2}\right)^s \int\limits_{0}^{t} (t-y)^n dy = 2^{r+1} \left(\frac{\pi}{2}\right)^s \frac{t^{n+1}}{(n+1)!}$$

as desired. Now $V(r, s+1, t)$ is the volume of the set described by

$$\sum_{i=1}^{r} |y_i| + 2\sum_{j=1}^{s} |z_j| + 2|z| \leq t.$$

As above,

$$V(r, s+1, t) = \int\limits_{|z| \leq t/2} V(r, s, t - 2|z|)d\mu(z),$$

where μ is the Lebesgue measure on $\mathbb{C}$. In polar coordinates, the integral becomes

$$= \int_{\theta=0}^{2\pi} \int_{l=0}^{t/2} 2^r \left(\frac{\pi}{2}\right)^s \frac{(t-2l)^n}{n!} l \cdot dl \cdot d\theta = \int_{\theta=0}^{2\pi} 2^r \left(\frac{\pi}{2}\right)^s \frac{1}{n!} d\theta \int_{l=0}^{t/2} (t-2l)^n l \; dl.$$

Write $(t-2l)^n l \; dl = -l\frac{d(t-2l)^{n+1}}{2(n+1)}$ and consider $\int\limits_{l=0}^{t/2} \frac{-l}{2(n+1)} d(t-2l)^{n+1}$.

Now integrating by parts, we get

$$\int_{l=0}^{t/2} \frac{-l}{2(n+1)} d(t-2l)^{n+1} = (-l)\frac{(t-2l)^{n+1}}{(-2)(n+1)} + \int_{0}^{t/2} \frac{(t-2l)^{n+1}}{2(n+1)} dl = 0 + \frac{t^{n+2}}{4(n+1)(n+2)}.$$

Thus, $V(r, s+1, t) = 2^r \left(\frac{\pi}{2}\right)^{s+1} \frac{t^{n+2}}{(n+2)!}$. This completes the induction. □

Theorem 4.4 (Minkowski bound)**.** *If $I \neq 0$ is an integral ideal of $\mathcal{O}_K$, then there exists $a \neq 0 \in I$ such that*

$$|N_{K/\mathbb{Q}}(a)| \leq M \cdot N(I),$$

*where $M = \frac{n!}{n^n}(\frac{4}{\pi})^s\sqrt{|d_K|}$ is called the **Minkowski bound**.*

Proof. The set B_t is convex, symmetric about the origin and compact. Also

$$Vol_{Leb}(B_t) = 2^r \left(\frac{\pi}{2}\right)^s \frac{t^n}{n!} \tag{4.1}$$

We choose a $t \geq 0$ such that

$$Vol_{Leb}(B_t) = 2^{-s} Vol_{Can}(B_t) = 2^{-s} Vol_{Can}(f(X_t)) = 2^{n-s} Vol(j(I))$$
$$= 2^{n-s}\sqrt{|d_K|}N(I) \tag{4.2}$$

Now, equating equations (4.1) and (4.2),

$$t^n = 2^{n-r}\pi^{-s}(n!)\sqrt{|d_K|}N(I)$$

By Minkowski's lattice point theorem, there exists a non-zero element $a \in I$ such that $j(a) \in B_t$. Also,

$$|N_{K/\mathbb{Q}}(a)| = \prod_{i=1}^{n} |\tau_i(a)|.$$

Let $\tau_i(a) = a_i$. Now using the AM-GM inequality $(a_1 a_2 \cdots a_n)^{1/n} \leq \frac{a_1+a_2+\cdots+a_n}{n}$ for positive real numbers we get,

$$|N_{K/\mathbb{Q}}(a)| = \prod_{i=1}^{n} a_i \leq \left(\frac{1}{n} \sum_{i=1}^{r} |a_i| + \frac{2}{n} \sum_{i=r+1}^{r+s} |a_i| \right)^n .$$

Since $j(a) \in B_t$, we have $|N_{K/\mathbb{Q}}(a)| \leq \frac{t^n}{n^n}$. By choice of t,

$$|N_{K/\mathbb{Q}}(a)| \leq \frac{1}{n^n} 2^{n-r} \pi^{-s} (n!) \sqrt{|d_K|} N(I) = \left(\frac{4}{\pi} \right)^s \frac{n!}{n^n} \sqrt{|d_K|} N(I).$$

□

Corollary 4.1. *In every ideal class of a number field K of degree n, there exists an integral ideal I such that*

$$N(I) \leq (\frac{4}{\pi})^s \frac{n!}{n^n} \sqrt{|d_K|}.$$

Proof. Choose J' as a fractional ideal in the given ideal class. Then, without loss of generality, $J = (J')^{-1}$ is an integral ideal.

Choose a non-zero $\alpha \in J$ such that α satisfies the norm inequality. Let $I = \alpha J'$, is our candidate.

I is an integral ideal because $\alpha \in J$ and $JJ' = \mathcal{O}_K$. So $IJ = \langle \alpha \rangle$. So,

$$N(I)N(J) = |N_{K/\mathbb{Q}}(\alpha)| \leq \left(\frac{4}{\pi} \right)^s \left(\frac{n!}{n^n} \right) \sqrt{d_K} N(J),$$

i.e.,

$$N(I) \leq \left(\frac{4}{\pi} \right)^s \left(\frac{n!}{n^n} \right) \sqrt{d_K}.$$

□

Corollary 4.2. *Let K be a number field of degree n and let d_K be its discriminant. Then*

$$|d_K| \geq \left(\frac{n^n}{n!} \right)^2 \left(\frac{\pi}{4} \right)^{2s} > \frac{1}{e^2 n} \left(\frac{\pi e^2}{4} \right)^n .$$

Proof. If I is an integral ideal and $a \in I$, non-zero, then

$$N(\langle a \rangle) \geq N(I),$$

this implies,

$$M = \left(\frac{4}{\pi}\right)^s \frac{n!}{n^n} \sqrt{|d_K|} \geq 1,$$

i.e.

$$|d_K| \geq \left(\frac{n^n}{n!}\right)^2 \left(\frac{\pi}{4}\right)^{2s}.$$

The second inequality in he statement is obtained by Stirling's approximation, viz., $n! \sim \sqrt{2\pi n}(\frac{n}{e})^n$.

Hence,

$$|d_K| \geq \left(\frac{n^n}{n!}\right)^2 \left(\frac{\pi}{4}\right)^{2s} > \frac{1}{e^2 n} \left(\frac{\pi e^2}{4}\right)^n.$$

□

Note that $\frac{\pi e^2}{4} \approx 5.8 > 1$. Now, using ratio test for $(a_n) = \frac{1}{e^2 n}(\frac{\pi e^2}{4})^n$,

$$\lim_{n\to\infty} |\frac{a_{n+1}}{a_n}| = \lim_{n\to\infty} |\frac{n}{n+1}\frac{\pi e^2}{4}| = \frac{\pi e^2}{4} \lim_{n\to\infty} \frac{1}{1+\frac{1}{n}} = \frac{\pi e^2}{4} > 1.$$

Therefore, $(a_n) \to \infty$ as $n \to \infty$. By comparison test, $|d_K| \to \infty$ as $n \to \infty$. This shows that the absolute value of the discriminant $|d_K|$ tends to ∞ with the degree n of the number field.

Chapter 5

Dirichlet's unit theorem

5.1 Group of units

Let K be a number field of degree n and let $\mathcal{O}_K$ be its ring of integers.

Definition 5.1. *A non-zero element $\alpha \in \mathcal{O}_K$ is called a **unit** of $\mathcal{O}_K$ if $\alpha^{-1} \in \mathcal{O}_K$.*

So, the units of K form a subgroup U of K^*.

If $\alpha \in \mathcal{O}_K$ is an unit, then there exists $\beta \in \mathcal{O}_K$ such that $\alpha\beta = 1$. So, $N_K(\alpha\beta) = N_K(\alpha)N_K(\beta) = 1$. Hence, $N_K(\alpha) = \pm 1$ (since, $N_K(\alpha), N_K(\beta) \in \mathbb{Z}$).

Conversely, if $\alpha \in \mathcal{O}_K$ and $N_K(\alpha) = \pm 1$, then α is a unit. Since $\alpha^{(1)} \cdot \alpha^{(2)} \cdots \alpha^{(n)} = \pm 1$, where $\alpha^{(i)} = \sigma_i(\alpha)$ and for $1 \leq i \leq n$, σ_i's are the distinct embeddings of K into $\mathbb{C}$.

Example 5.1. *Let $K = \mathbb{Q}[\sqrt{5}]$, then $\mathcal{O}_K = \mathbb{Z}[\frac{1+\sqrt{5}}{2}]$. Then $\{1, \frac{1+\sqrt{5}}{2}\}$ is an integral base. Let $\alpha = \frac{1}{2} + \frac{\sqrt{5}}{2}$.*

$$1 \longmapsto (\frac{1}{2} + \frac{\sqrt{5}}{2}) \text{ and } \sqrt{5} \longmapsto (\frac{\sqrt{5}}{2} + \frac{5}{2}).$$

Hence, $A_\alpha = \begin{pmatrix} \frac{1}{2} & \frac{5}{2} \\ \frac{1}{2} & \frac{1}{2} \end{pmatrix}$. Then $det(A_\alpha) = N_K(\alpha) = \frac{1}{4} - \frac{5}{4} = -1$. Hence α is an unit in K.

Lemma 5.1. *Let $c \geq 0$ be a real number. The number of algebraic integers $\alpha \in \mathcal{O}_K$ such that $|\alpha^{(i)}| \leq c$ and for all $1 \leq i \leq n$, is finite.*

Proof. Let $w_1, w_2, \dots, w_n$ be an integral base of $\mathcal{O}_K$, then any $\alpha \in \mathcal{O}_K$ can be written as $\alpha = x_1 w_1 + \cdots + x_n w_n,\ x_i \in \mathbb{Z}$.

Also, $\alpha^{(i)} = x_1 w^{(i)} + \cdots + x_n w^{(i)}$. So, $A = \Omega X$, where

$$A = \begin{pmatrix} \alpha^{(1)} \\ \vdots \\ \alpha^{(n)} \end{pmatrix}_{n\times 1},\ X = \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix}_{n\times 1} \quad \text{and } \Omega = (w_j^{(k)}).$$

Since Ω has an inverse Ω^{-1} in $\mathcal{M}_n(\mathbb{C})$. Thus, $X = \Omega^{-1}A$. By assumption, $|\alpha^{(i)}| \leq c$. Hence, $|x_i| \leq Mc$, where M depends only on Ω^{-1}, thus only on K. Since the number of integers satisfying $|x_i| \leq Mc$ is finite, the lemma follows. □

Definition 5.2. *A complex number α is called a* ***root of unity*** *if $\alpha^m = 1$ for some $m \neq 0 \in \mathbb{Z}$.*

If ρ is a root of unity in K then $\rho^m = 1$ for some $m \neq 0 \in \mathbb{Z}$. So, $|\rho^{(i)}| = 1$, for $1 \leq i \leq n$.

Also, every root of unity in K is a unit, but not conversely.

Example 5.2. *Let $K = \mathbb{Q}[\sqrt{2}]$, $1 + \sqrt{2}$ is a unit, but not a root of unity.*

Corollary 5.1. *In the previous lemma, let $c = 1$. Then the number of roots of unity in K is finite.*

Lemma 5.2. *The roots of unity in K form a finite cyclic subgroup.*

Proof. Let Z_K be the group of roots of unity in K, let $\zeta_t = e^{\frac{2\pi i p_t}{q_t}}$, for $t = 1, 2, \dots, w$ be the elements of Z_K.

Let $q_0 = q_1 q_2 \dots q_w$ and let A be the subgroup of $\mathbb{Z}$ consisting of integers p for which $e^{\frac{2\pi i p}{q_0}} \in Z_K$. Then, $A = p_0\mathbb{Z}$ for some $p_0 > 0 \in \mathbb{Z}$, and

$$\langle e^{\frac{2\pi i p_0}{q_0}} \rangle \subset Z_K.$$

Now, any element in Z_K is $\zeta_1 = e^{\frac{2\pi i p_1}{q_1}} = e^{\frac{2\pi i k p_0}{q_0}}$, for some $k \in \mathbb{Z}$. Hence, $\zeta_1 \in \langle e^{\frac{2\pi i p}{q_0}} \rangle$. Thus, $Z_K \subset \langle e^{\frac{2\pi i p_0}{q_0}} \rangle$. □

5.2 Dirichlet's unit theorem

Let $\mathcal{O}_K^*$ denote the group of units in $\mathcal{O}_K$ and $\mu(K)$ denote the group of roots of unity in K. It is clear that $\mu(K) \subset \mathcal{O}_K$.

The size of the group $\mathcal{O}_K^*$ is determined by the number r of real embeddings of K and the number s of pairs of complex conjugate embeddings. In order to describe the group, we use the diagram which was set up in Chapter 4, during the discussion on multiplicative Minkowski theory:

$$\begin{tikzcd}
K^* \arrow[r, "j"] \arrow[d, "N_{K/\mathbb{Q}}"'] & K_{\mathbb{R}}^* \arrow[r, "\tilde{l}"] \arrow[d, "N"] & {[\prod_\tau \mathbb{R}]^+} \arrow[d, "Tr"'] \\
\mathbb{Q}^* \arrow[r, "i"] & \mathbb{R}^* \arrow[r, "log|\ |"] & \mathbb{R}
\end{tikzcd}$$

In the above commutative diagram we consider the subgroups:

$$\mathcal{O}_K^* = \{\epsilon \in \mathcal{O}_K | N_{K/\mathbb{Q}}(\epsilon) = \pm 1\},$$

the group of units,

$$S = \{y \in K_{\mathbb{R}}^* | N(y) = \pm 1\},$$

the "norm-one surface", and

$$H = \{x \in \Big[\prod_\tau \mathbb{R}\Big]^+ | Tr(x) = 0\},$$

the "trace-zero hyperplane".

We obtain the homomorphisms

$$\mathcal{O}_K^* \xrightarrow{j} S \xrightarrow{\tilde{l}} H$$

and the composite $\lambda := \tilde{l} \circ j : \mathcal{O}_K^* \longrightarrow H$. The image will be denoted by $\Gamma = \lambda(\mathcal{O}_K^*) \subset H$.

Proposition 5.1. *The sequence*

$$1 \longrightarrow \mu(K) \longrightarrow \mathcal{O}_K^* \xrightarrow{\lambda} \Gamma \longrightarrow 0$$

is exact.

Proof. We have to show the $\mu(K)$ is the kernel of λ.

For $\zeta \in \mu(K)$ and $\tau : K \longrightarrow \mathbb{C}$ any embedding we find $log|\tau(\zeta)| = log1 = 0$. So, $\mu(K) \subset ker(\lambda)$.

Conversely, let $\epsilon \in \mathcal{O}_K^*$ be an element in the kernel. So, $\lambda(\epsilon) = \tilde{l}(j(\epsilon)) = 0$. This means that $|\tau(\epsilon)| = 1$ for each embedding $\tau : K \longrightarrow \mathbb{C}$. Hence, $j(\epsilon) = (\tau(\epsilon))$ lies in the bounded domain of the $\mathbb{R}$-vector space $K_{\mathbb{R}}$.

While, $j(\epsilon)$ is a point of the lattice $j(\mathcal{O}_K)$ of $K_{\mathbb{R}}$. Therefore, the kernel of λ can contain only finite number of elements, and thus, being a finite group, contains only the roots of unity in K^*. □

We now state the main theorem of this section. Once we have proven this theorem, Dirichlet's unit theorem can be easily deduced.

Theorem 5.1. *The set $\Gamma = \lambda(\mathcal{O}_K^*)$, as defined above, is a complete lattice in H.*

As of now, all we know is the $\Gamma \subset H$. Recall from earlier that a complete lattice is a free $\mathbb{Z}$-module. So here, since H is a $(r+s-1)$-dimensional space, then our ultimate goal is to prove that Γ is a free $\mathbb{Z}$-module with $r+s-1$ generators. To prove this theorem, we will need several lemmas.

Lemma 5.3. *Let a be a non-zero rational integer. Up to multiplication by units, there are only finitely many elements $\alpha \in \mathcal{O}_K$ such that $N_{K/\mathbb{Q}}(\alpha) = a$.*

Proof. Let $\alpha_1, \alpha_2 \in \mathcal{O}_K$ such that $N_{K/\mathbb{Q}}(\alpha_1) = N_{K/\mathbb{Q}}(\alpha_2) = a$ and $\alpha_1 = \alpha_2 + a\gamma$, where $\gamma \in \mathcal{O}_K$. Then $\frac{\alpha_1}{\alpha_2} = 1 + \frac{a}{\alpha_2}\gamma \in \mathcal{O}_K$.

But the same is true for $\frac{\alpha_2}{\alpha_1}$. so, $\frac{\alpha_1}{\alpha_2}$ must be a unit. So we have proven that if α_1, α_2 have norm a and if $\alpha_1 \equiv \alpha_2 \pmod{a\mathcal{O}_K}$, then $\frac{\alpha_1}{\alpha_2}$ is a unit.

Since there are only finitely many elements in the factor ring $\mathcal{O}_K/a\mathcal{O}_K$, therefore, up to multiplication by units, there are at most $|\mathcal{O}_K/a\mathcal{O}_K|$ elements of norm $\pm a$. □

Recall that Γ' is a lattice in $\mathbb{R}^m$ if and only if it is a discrete subgroup of $\mathbb{R}^m$. Since, $\Gamma \subset H \subset \mathbb{R}^{r+s} \cong [\prod_\tau \mathbb{R}]^+ \subset \prod_\tau \mathbb{R}$, to show that Γ is a discrete subset, it is enough to prove the following:

Lemma 5.4. *For any $c > 0$, the set $\{(x_i) \in \prod_\tau \mathbb{R} |\ |x_i| \leq c\}$ contains only finitely many elements of Γ.*

Proof. If $\alpha \in \mathcal{O}_K^*$, then $\tilde{l}(j(\alpha))$ is in the set if and only if $e^{-c} \leq |\tau(\alpha)| \leq e^c$ for every $\tau \in Hom(K, \mathbb{C})$. This puts a bound on the coefficients of the minimal polynomial of α, (since the coefficients are just sums and products of the conjugates $\tau(\alpha)$ of α.

Hence there are only finitely many such polynomials, which means there can only be finitely many such α. Hence this set has only finitely many elements. □

We deduce from this lemma that Γ is a discrete subgroup and thus Γ is a lattice. It remains to be shown that Γ is a complete lattice of H.

Recall that if $\Gamma \subset \mathbb{R}^m$ is a lattice, and $M \subset \mathbb{R}^m$ is a bounded set such that $M + \Gamma = \mathbb{R}^m$, then Γ is a complete lattice.

Proof of Theorem 5.1. We would like to construct such a set M for Γ. First, let $S := \{y \in K_{\mathbb{R}}^* | \ |N(y)| = 1\}$. Recall the map $j : K^* \longrightarrow K_{\mathbb{R}}^* \subset K_{\mathbb{R}}$. We will construct a subspace T of S such that T is bounded in $K_{\mathbb{R}}$ and $S = \bigcup\limits_{\epsilon \in \mathcal{O}_K^*} T \cdot j(\epsilon)$. Then $M = \tilde{l}(T)$ will be a set that satisfies the above mentioned condition for Γ.

It is easy to see that $\tilde{l}(S) = H$. Then we have

$$H = \tilde{l}(S) = \bigcup_{\epsilon \in \mathcal{O}_K^*} \tilde{l}(T)\tilde{l}(j(\epsilon)) = \bigcup_{\gamma \in \Gamma} \tilde{l}(T)\gamma = \bigcup_{\gamma \in \Gamma} M\ \gamma,$$

and setting $M = \tilde{l}(T)$ hence we get $H = M + \Gamma$. Also since $T \subset S$, T is bounded and hence M is bounded. Therefore, once we have constructed such a set T, then we can define M as above. So we now construct T.

Recall from Minkowski theory, Theorem 4.2 which states, Let $I \neq 0$ be an integral ideal of K and let $c_{\tau_i} = c_i > 0$ for $\tau_i \in Hom(K, \mathbb{C})$ be real numbers such that $c_{\tau_i} = c_{\overline{\tau_i}}$ and

$$\prod_{\tau} c_i > A \cdot N(I),$$

where $A = \left(\frac{2}{\pi}\right)^s \sqrt{|d_K|}$. Then there exists $a \in I$ and $a \neq 0$ such that

$$|\tau_i(a)| < c_i, \text{ for every } \tau_i \in \text{Hom(K, } \mathbb{C}).$$

. We apply this to case $I = \mathcal{O}_K$. Let c_i be as above, and let $C := \prod\limits_{\tau} c_i > (\frac{2}{\pi})^s \sqrt{|d_K|}$. Now define a set

$$X := \{(z_i) \in K_{\mathbb{R}} | |z_i| < c_i\}.$$

Then by Theorem 4.2, there exists a non-zero $\alpha \in \mathcal{O}_K$ such that $j(\alpha) \in X$. (Recall from earlier, in Minkowski theory, that j is a map whose image in $K_{\mathbb{R}}$ is defined by an ordered n-tuple, each coordinate of which is the image of the original point under some embedding of the number field K.)

Now let us take $y = (y_i) \in S$. Then we define Xy to be a similar set:

$$Xy := \{(z_i) \in K_{\mathbb{R}} | \; |z_i| < c_i \cdot |y_i| \text{ for all } \tau_i \in Hom(K, \mathbb{C})\}.$$

Notice that since $y \in S$, then the product of over all $\tau \in Hom(K, \mathbb{C})$ of $c_i \cdot |y_i| = C$. Again by Theorem 4.2, there exists a non-zero $\alpha \in \mathcal{O}_K$ such that $j(\alpha) \in Xy$, so $j(\alpha) = xy$ for some $x \in X$. So upon rearranging terms, $y^{-1} = x(j(\alpha))^{-1}$.

We now know that any element of S can be written as $xj(\alpha)^{-1}$, i.e., the product of an element from a bounded set and some element of $K_{\mathbb{R}}$. In order to prove $S = \bigcup\limits_{\epsilon \in \mathcal{O}_K^*} T \cdot \gamma\epsilon$, we need to show that we can replace $(j(\alpha))^{-1}$ by an element of norm 1.

By a previous lemma, if we know that there are $\alpha_1, \cdots, \alpha_n \in \mathcal{O}_K$ such that for every $\alpha \in \mathcal{O}_K$ having $|N_{K/\mathbb{Q}}(\alpha)| < C$, then we have a representation $\epsilon\alpha = \alpha_i$ for some unit ϵ in K. Applying this, we have:

$$y^{-1} = x(j(\alpha))^{-1} = x(j(\alpha^{-1})) = xj(\epsilon\alpha_i^{-1}) = xj(\epsilon)j(\alpha_i^{-1}),$$

and since $y^{-1} \in S$, $j(\epsilon) \in S$, then $x(j(\alpha))^{-1} \in S$. It follows then that

$$S = \bigcup_{\epsilon \in \mathcal{O}_K^*} \Big(\bigcup_{i=1}^{n} (S \cap Xj(\alpha_i^{-1})) \Big) j(\epsilon).$$

Now let $T := \bigcup\limits_{i=1}^{n} (S \cap Xj(\alpha_i^{-1}))$. T is bounded in $K_{\mathbb{R}}$, since S is bounded and the boundedness of $Xj(\alpha_i^{-1})$ follows from the boundedness of X.

Therefore, Γ is a complete lattice. □

Now we can state and prove Dirichlet's unit theorem.

Theorem 5.2. ***(Dirichlet's Unit Theorem)*** *The group of units $\mathcal{O}_K^*$ of $\mathcal{O}_K$ is the direct product of the finite cyclic group $\mu(K)$ and a free abelian group of rank $r + s - 1$.*

Proof. Since $\Gamma = \lambda(\mathcal{O}_K^*)$, the map $\lambda : \mathcal{O}_K^* \longrightarrow \Gamma \cong \mathbb{Z}^{r+s-1}$ is a surjective group homomorphism and with $ker\lambda = \mu(K)$.

Let $\gamma_1, \dots, \gamma_{r+s-1}$ be a free system of generators of Γ. Let $\epsilon_1, \dots, \epsilon_{r+s-1}$ be such that $\lambda(\epsilon_i) = \gamma_i$. Then

$$\mu(K) \cap \epsilon_1^{\mathbb{Z}} \cdot \epsilon_2^{\mathbb{Z}} \cdots \epsilon_{r+s-1}^{\mathbb{Z}} = 1,$$

i.e.,

$$\mu(K) \cdot \epsilon_1^{\mathbb{Z}} \cdot \epsilon_2^{\mathbb{Z}} \cdots \epsilon_{r+s-1}^{\mathbb{Z}} = \mathcal{O}_K^*,$$

where $\epsilon_i^{\mathbb{Z}}$ denotes any integer power of ϵ_i.

Hence there exist elements $\epsilon_1 \cdots \epsilon_{r+s-1} \in \mathcal{O}_K^*$ such that every $\epsilon \in \mathcal{O}_K^*$ can be written uniquely in the form

$$\epsilon = \zeta \cdot \epsilon_1^{m_1} \cdot \epsilon_2^{m_2} \cdots \epsilon_{r+s-1}^{m_{r+s-1}},$$

where $\zeta \in \mu(K)$ and $m_1, \dots, m_{r+s-1} \in \mathbb{Z}$. □

The units $\epsilon_1, \dots, \epsilon_{r+s-1}$ are called *fundamental units.*

5.3 Regulator

Identifying $[\prod_\tau \mathbb{R}]^+ = \mathbb{R}^{r+s}$, H becomes a subspace of the euclidean space $\mathbb{R}^{r+s}$ and thus itself a euclidean space.

We may therefore try computing the volume of the fundamental mesh $Vol(\lambda(\mathcal{O}_K^*))$ of the unit lattice $\Gamma = \lambda(\mathcal{O}_K^*)) \subset H$.

Let $\epsilon_1, \epsilon_2, \dots, \epsilon_t$, where $t = r + s - 1$, be a system of fundamental units and Φ the fundamental mesh of the unit lattice $\lambda(\mathcal{O}_K^*))$, spanned by the vectors $\lambda(\epsilon_1), \dots, \lambda(\epsilon_t) \in H$.

Now let us take a vector in $\mathbb{R}^{r+s}$ orthogonal to H. We will choose

$$\lambda_0 := \frac{1}{\sqrt{r+s}}(1, 1, \dots, 1) \in \mathbb{R}^{r+s}.$$

Then $\lambda_0, \lambda(\epsilon_1), \dots, \lambda(\epsilon_t)$ is a basis of a complete lattice in $\mathbb{R}^{r+s}$. The fundamental mesh of this lattice has volume:

$$d := \left| \det \begin{pmatrix} \frac{1}{\sqrt{r+s}} & \lambda_1(\epsilon_1) & \cdots & \lambda_1(\epsilon_t) \\ \vdots & \vdots & \ddots & \vdots \\ \frac{1}{\sqrt{r+s}} & \lambda_{t+1}(\epsilon_1) & \cdots & \lambda_{t+1}(\epsilon_t) \end{pmatrix} \right|$$

If Φ is the fundamental mesh of Γ in H, then $Vol(\Phi) = d$. We can compute d by adding all rows to any chosen row. For instance, if we do this for the first row, we get

$$d := \left| \det \begin{pmatrix} \sqrt{r+s} & 0 & \cdots & 0 \\ 0 & \lambda_2(\epsilon_1) & \cdots & \lambda_2(\epsilon_t) \\ \vdots & \vdots & \ddots & \vdots \\ 0 & \lambda_{t+1}(\epsilon_1) & \cdots & \lambda_{t+1}(\epsilon_t) \end{pmatrix} \right|.$$

Therefore, letting the bottom right $t \times t$ matrix to be A, we have $d = \sqrt{r+s}|\det(A)|$.

Definition 5.3. *The* ***regulator of K****, denoted by R_K, is defined to be the absolute value of the determinant of any $t \times t$, where $t = r + s - 1$, minor of the matrix*

$$\begin{pmatrix} \lambda_1(\epsilon_1) & \cdots & \lambda_1(\epsilon_t) \\ \vdots & \ddots & \vdots \\ \lambda_{t+1}(\epsilon_1) & \cdots & \lambda_{t+1}(\epsilon_t) \end{pmatrix}.$$

From our above analysis, we see that the regulator is well-defined, i.e., it is invariant under the choice of minor, which follows since d is independent of the choice of the fundamental system of units and also choice of deletion. The explicit form of this matrix is:

$$\begin{pmatrix} log|\tau_1(\epsilon_1)| & \cdots & log|\tau_1(\epsilon_t)| \\ \vdots & \ddots & \vdots \\ log|\tau_r(\epsilon_1)| & \cdots & log|\tau_r(\epsilon_t)| \\ log|\tau_{r+1}(\epsilon_1)|^2 & \cdots & log|\tau_{r+1}(\epsilon_t)|^2 \\ \vdots & \ddots & \vdots \\ log|\tau_{r+s}(\epsilon_1)|^2 & \cdots & log|\tau_{r+s}(\epsilon_t)|^2 \end{pmatrix},$$

where $\tau_1, \dots, \tau_r$ are the real embeddings of K and $\tau_{r+1}, \dots, \tau_{r+s}$ are the distinct complex embeddings, up to conjugation, of K.

5.4 Units in a quadratic field

Let K be a quadratic field of discriminant d. In the notation of $n = r + 2s$, if $d > 0$, then $r = 2$ and $s = 0$; if $d < 0$, then $r = 0$ and $s = 1$.

In the case of real quadratic field K, the only roots of unity in K are real roots of unity, viz., ± 1.

So, by Dirichlet's unit theorem, every unit ϵ in K can be written in the form $\pm\epsilon_1^n$, $n \in \mathbb{Z}$, for a fixed unit ϵ_1 in K, as $r+s-1 = 2-1 = 1$ in this case.

Also, $\epsilon_1 \neq \pm 1$ (otherwise, we will not get the other units in K). If ϵ_1 has this property, so do $\epsilon_1^{-1}, -\epsilon_1, -\epsilon_1^{-1}$. But among $\epsilon_1, \epsilon_1^{-1}, -\epsilon_1, -\epsilon_1^{-1}$, exactly one of them is greater than 1. We denote it by η and call it the *fundamental unit* of K.

It is uniquely determined and every unit ϵ in K is of the form $\pm\eta^n$ for $n \in \mathbb{Z}$.

5.4.1 Pell's equation

Any unit $\epsilon \in K = \mathbb{Q}(\sqrt{d})$ of discriminant $d > 0$ gives rise to a solution of the Diophantine equation

$$x^2 - dy^2 = \pm 4; \ x, y \in \mathbb{Z}.$$

Since $N_K(\epsilon) = N_K(\frac{x+y\sqrt{d}}{2}) = \frac{x^2-dy^2}{4}$ and $N_K(\epsilon) = \pm 1$.

Conversely, if for $d > 0$ in $\mathbb{Z}$, there exist $x, y \in \mathbb{Z}$ satisfying $x^2 - dy^2 = \pm 4$, then $\frac{x \pm y\sqrt{d}}{2}$ is a unit in $K = \mathbb{Q}(\sqrt{d})$.

In case d is the discriminant of a real quadratic field, we'll have a non-trivial solution to the Diophantine equation. This equation $x^2 - dy^2 = \pm 4$ is called the **Pell's equation**.

If $d < 0$, K is an imaginary quadratic field and $t = r+s-1 = 0$. Thus by Dirichlet's unit theorem, every unit in K is a root of unity.

We know, the roots of unity form a finite cyclic group. Thus, the units in K form a finite cyclic group of order w.

Proposition 5.2. *When K is a complex quadratic field with discriminant d, such that if*

(i) $d < -4$, then $w = 2$,

(ii) $d = -4$, then $w = 4$, and

(iii) $d = -3$, then $w = 6$.

We don't look at $d = -2 \equiv 2 \pmod 4$ or $d = -1 \equiv 3 \pmod 4$ because $d \equiv 0 \pmod 4$ or $d \equiv 1 \pmod 4$.

Proof. Let $K = \mathbb{Q}(\sqrt{d})$ and let $\alpha \in K$ be a unit. Also, $\alpha = p + q(\frac{d+\sqrt{d}}{2})$ where $p, q \in \mathbb{Z}$. Then,

$$N_K(\alpha) = (p + q\frac{d}{2})^2 + \frac{q^2}{4}|d| = 1. \tag{5.1}$$

So, $(p + \frac{qd}{2})^2 \leq 1$ and $q^2 \leq \frac{4}{|d|}$.

Case(i) If $d < -4$, then $q = 0$. So, $\alpha = p = \pm 1$ are the only units in K. Therefore, $w = 2$ for $d < -4$.

Case(ii) If $d = -4$, then $q = 1, -1$ or 0.

If $q = 0$, then $p = \pm 1$. If $q = 1$, then $p = 2$. If $q = -1$, then $p = -2$.

Hence in $\mathbb{Q}(\sqrt{-4}) = \mathbb{Q}(i)$, the only units are ± 1 and $\pm\sqrt{-1}$. Therefore, $w = 4$.

Case(iii) $K = \mathbb{Q}(\sqrt{-3})$. Here also $q = 0, 1$ or -1.

Substituting everything in equation (5.1) we get the feasible values of p in $\mathbb{Z}$, and thus eventually the units in the field K. The only units here are: $\{\pm 1, \pm(\frac{1}{2} + \frac{\sqrt{-3}}{2}), \pm(\frac{1}{2} - \frac{\sqrt{-3}}{2})\}$. Hence $w = 6$. □

Chapter 6

Ramification theory

Let K be a number field, $A = \mathcal{O}_K$ the ring of integers of K, L an extension of finite degree of K, and $B = \mathcal{O}_L$ the integral closure of A in L (i.e., the ring of integers of L).

The ideal $P\mathcal{O}_L = PB$ generated in B by a non-zero prime ideal P of A, is not in general prime. It splits into a product of prime ideals, as stated by Dedekind's theorem, i.e., $PB = \prod\limits_i P_i^{e_i}$.

6.1 Preliminaries from rings and modules theory

Let us now recall a few results from Ring and module theory.

Definition 6.1. *Let A be an integral domain and let S be a multiplicatively closed subset of $A - \{0\}$ and $1 \in S$.*

Ring of fractions of A with respect to S or ***localisation of** A **at** S*, denoted by $S^{-1}A$ is defined as $\{\frac{a}{s} | a \in A, s \in S\}$.*

$S^{-1}A$ is a commutative ring which contains A. If $S = A \setminus \{0\}$, then $S^{-1}A = K$. If $S = \{1\}$, or if it contains only units in A, then $S^{-1}A = A$.

Proposition 6.1. *Let A be an integral domain and let S be a multiplicatively closed subset of A. Let $A' = S^{-1}A$.*

(1) For any ideal I' of A', it is true that $(I' \cap A)A' = I'$. So, the mapping $I' \longmapsto I' \cap A$ is an increasing injection of the set of ideals of A' into the set of ideals of A.

(2) The mapping $P' \longmapsto P' \cap A$is an isomorphism of the partially-ordered set (poset) of prime ideals of A' on the poset of prime ideals P of A, which satisfy $P \cap S = \phi$. The inverse mapping is $P \longmapsto PA'$.

Corollary 6.1. *If A is a Noetherian integral domain, then every ring of fractions $S^{-1}A$ is Noetherian.*

Proposition 6.2. *Let R be an integral domain, A a subring of R, S a multiplicatively closed subset of $A - (0)$, and let B be the integral closure of A in R. Then the integral closure of $S^{-1}A$ in $S^{-1}R$ is $S^{-1}B$.*

Corollary 6.2. *If A is an integrally closed ring, then $S^{-1}A$ is integrally closed.*

Proposition 6.3. *If A is a Dedekind ring, then every $S^{-1}A$ is a Dedekind ring.*

Proof. We know $S^{-1}A$ is Noetherian and integrally closed. Since when going from the set of prime ideals of A to prime ideals of $S^{-1}A$, we leave out the prime ideals P whose $P \cap S \neq \phi$ (by Proposition 1 (2)). Thus, every non-zero prime ideal of $S^{-1}A$ is maximal. □

Proposition 6.4. *Let A be a Dedekind ring. Let P be a non-zero prime ideal of A. Let $S = A - P$. Then $S^{-1}A$ is a principal ideal ring. More precisely, there exist a prime $p \in S^{-1}A = A_P$ such that the non-zero ideals of $S^{-1}A$ are of the form (p^n), $n \geq 0$.*

Proof. Since P is the only non-zero prime ideal of A disjoint from S, the only non-zero prime ideal of $S^{-1}A$ is $Q = S^{-1}P$.

Since, $S^{-1}A$ is a Dedekind ring, its only non-zero ideals are of the form Q^n, $n \geq 0$, due to the Dedekind's theorem. (Let $I \neq (0)$ be an ideal in A_P. $I =$ product of prime ideals in $A_P = Q^n$ for some $n \geq 0$.

Let $p \in Q - Q^2$. The ideal $(p) \subset Q$ but $(p) \not\subset Q^2$. So, $(p) =$ product of Q's $= Q^n$ if an only if $n = 1$. So, $(p) = Q$ and $(p^n) = Q^n$ for every $n \geq 0$.

Thus $S^{-1}A$ is a principal ideal ring and all its ideals are of the form (p^n), $n \geq 0$. □

Proposition 6.5. *Let A be an integral domain, S a multiplicatively closed subset of $A - (0)$ and let $\mathscr{M}$ be a maximal ideal of A, where $\mathscr{M} \cap S = \phi$. Then $S^{-1}A/\mathscr{M}S^{-1}A \cong A/\mathscr{M}$.*

6.2 Splitting of prime ideals in an extension

Theorem 6.1. *Let A be a Dedekind ring, K its field of fractions, L is an extension of finite degree over K and A' the integral closure of A in L. Let characteristic of $K = 0$. Then A' is a Dedekind ring and an A-module of finite-type.*

Proof. A' is integrally closed by construction. It is Noetherian and an A-module of finite-type. It remains to show that every prime ideal $P' \neq (0)$ of A' is maximal.

Let $x \in P' - \{0\}$ and consider an equation of integral dependence of x over A, the degree of which is minimum, $x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0 = 0$, $a_i \in A$.

Then $a_o \neq 0$. Also, $a_0 \in A'x \cap A \subset P' \cap A$. Thus, $P' \cap A \neq (0)$. Since $P' \cap A$ is a maximal ideal of A, and $A/(P' \cap A)$ is a field.

But $A/(P' \cap A)$ may be identified with a subring of A'/P' is integral over $A/(P' \cap A)$, (since A' is an integral over A).

Thus A'/P' is a field, so P' is maximal. □

Corollary 6.3. *Along with the hypothesis of the previous theorem, if we assume that A is principal, then A' is a free A-module of rank n.*

Let P be a non-zero prime ideal of A. Then BP is an ideal of B and its has an expression of the form:

$$BP = \prod_{i=1}^{q} P_i^{e_i},$$

where P_i's are distinct prime ideals of B and e_i's ≥ 0, by Dedekind's theorem.

Proposition 6.6. *The P_i's are precisely those prime ideals $\mathscr{D}$ of B such that $\mathscr{D} \cap A = P$.*

Proof. For a prime ideal $\mathscr{D}$ of B, we have $\mathscr{D} \cap A = P$ if and only if $BP \subset \mathscr{D}$.

Because, $P \subset \mathscr{D}$ implies $BP \subset \mathscr{D}$.

Further, if $BP \subset \mathscr{D}$, then $PB \cap A \subset \mathscr{D} \cap A$. Thus, $P \subset BP \cap A \subset \mathscr{D} \cap A$. But $\mathscr{D} \cap A$ is a prime ideal of A, which is a Dedekind ring. Therefore $\mathscr{D} \cap A = P$.

Clearly, $BP = P_1^{e_1} P_2^{e_2} \ldots P_m^{e_m}$. So, $BP \subset P_i$ for every $i = 1, 2, \ldots, m$. Thus, from our equivalence, $P_i \cap A = P$. □

Both A/P and B/P_i for $1 \leq i \leq m$ are fields. Since B is an A-module of finite-type, B/P_i is a finite-dimensional vector space over A/P.

The **residual degree** of P_i over A, denoted by f_i, is defined to be the dimension of B/P_i over A/P as a vector space.

The exponent e_i in $BP = P_1^{e_1} \dots P_m^{e_m}$ is called the **ramification index** of P_i over A.

Also, $BP \cap A = P$, because, $P \subset BP \cap A$. Also, $BP \cap A = (P_1^{e_1} \dots P_m^{e_m}) \cap A$. So, for each $1 \leq i \leq m$, $P_i \cap A = P$. Thus, $BP \cap A \subset P$.

So, B/BP is a finite-dimensional vector space over A/P.

Theorem 6.2. *With the preceding notions,* $\sum\limits_{i=1}^{m} e_i f_i = [B/BP : A/P] = n$*, where* n *denotes the degree of the extension* L *over* K.

The above expression is also known as the *fundamental identity* about splitting of prime ideals.

Proof. For the first equality, note that $B/BP = B/\prod\limits_{i=1}^{m} P_i^{e_i} \cong \prod B/P_i^{e_i}$ (by Chinese remainder theorem). So it suffices to show that $[B/P_i^{e_i} : A/P] = e_i f_i$.

From the definition of f_i, we know that B/P_i is a field of degree f_i over A/P.

Consider the sequence of ideals,

$$B \supset P_1 \supset P_1^2 \supset \dots P_1^{e_1} \supset P_1^{e_1} P_2 \supset \dots P_1^{e_1} P_2^{e_2} \supset \dots \supset P_1^{e_1} \dots P_m^{e_m} = BP$$

For each r_i, $P_i^{r_i}/P_i^{r_i+1}$ is a B/P_i-module. Since there is no ideal between $P_i^{r_i}$ and $P_i^{r_i+1}$, it must have dimension 1 as a B/P_i-vector space. Hence, dimension f_i as a A/P-vector space.

Therefore each quotient in the chain

$$B \supset P_i \supset P_i^2 \supset \dots \supset P_i^{e_i}$$

has dimension f_i over A/P, and so the dimension of $B/P_i^{e_i}$ is $e_i f_i$.

The proof of the second equality is easy when B is a free A-module. For example, if A is a principal ideal domain, then by Corollary 7.3, if $\{x_1, x_2, \dots, x_n\}$ is a base of B as an A-module. Reduction modulo BP gives a base for B/BP over A/P.

Now, let S be a multiplicative subset of A disjoint from P and such that $S^{-1}A$ is principal (e.g., $S = A - P$).

Write $B' = S^{-1}B$ and $A' = S^{-1}A$. Then B' is the integral closure of A' in L, and $PB' = \prod(P_iB')^{e_i}$.

Since, $P_i \cap A = P$, $P_i \cap S = \phi$ and P_iB' is a non-zero prime ideal of B'. So, from the first part of the proof,

$$[B'/PB' : A'/PA'] = \sum_{i=1}^{m} e_i[B'/P_iB' : A'/PA'].$$

But, $[A'/PA' : A/P]$ and $[B/P_iB' : B/P_i]$.

Therefore, $\sum e_if_i = [B'/PB' : A'/PA']$, but A' is principal, and so, $[B'/PB' : A'/PA'] = n$. This completes the proof. □

Example 6.1. (**Cyclotomic fields**)

Let p be a prime number and let $\zeta = \zeta_{p^r}$ be a primitive $p^r - th$ root of unity in $\mathbb{C}$. In this case, all the complex $p^r - th$ roots of unity are of the form ζ^j, $j = 1, 2, \ldots, p^r$.

The primitive roots of unity are those for which j is not a multiple of p. The number of primitive roots is $\varphi(p^r) = p^r - p^{r-1}$, where φ is the Euler's phi function. These are the roots of the cyclotomic polynomial

$$F(X) = \frac{X^{p^r} - 1}{X^{p^{r-1}}} = X^{p^{r-1}(p-1)} + X^{p^{r-1}(p-2)} + \cdots + X^{p^{r-1}} + 1.$$

Let $e = p^{r-1}(p-1)$ and let $\zeta_1, \ldots, \zeta_e$ be all the primitive $p^r - th$ roots of unity. Since the constant term of $F(X+1)$ is p,

$$\pm p = \prod_{j=1}^{e}(\zeta_j - 1).$$

Let $\mathcal{O}_K$ be the ring of integers of $K = \mathbb{Q}[\zeta]$. Clearly, $\zeta_j \in \mathcal{O}_K$ and $\zeta_j - 1 \in \mathcal{O}_K(\zeta_k - 1)$ for all j and k, since $\zeta_j = \zeta_k^q$ of ζ_k and $\zeta_k^q - 1 = (\zeta_k - 1)(\zeta_k^{q-1} + \cdots + \zeta_k + 1)$. Thus all ideals $\mathcal{O}_K(\zeta_k - 1)$ are same.

So, $p\mathcal{O}_K = \mathcal{O}_K(\zeta_1 - 1)^e$. Write $p\mathcal{O}_K = \prod\limits_{i=1}^{m} \mathcal{P}_i^{e_i}$, where $\mathcal{P}_i$'s are prime ideals of $\mathcal{O}_K$. The e_i's must be multiples of e.

But $e \geq [\mathbb{Q}[\zeta] : \mathbb{Q}]$, so $e \geq \sum\limits_{i=1}^{m} e_if_i$. Thus,

$$m = 1, e = e_1, f_1 = 1 \text{ and } [\mathbb{Q}[\zeta] : \mathbb{Q}] = e.$$

In summary:

(i) $[\mathbb{Q}[\zeta]:\mathbb{Q}] = e = p^{r-1}(p-1)$.

(ii) $\mathcal{O}_K(\zeta_1 - 1)$ is a prime ideal of $\mathcal{O}_K$ of residual degree 1,

(iii) $p\mathcal{O}_K = \mathcal{O}_K(\zeta_1 - 1)^e$.

6.3 The discriminant and ramification

Let $PB = \prod_{i=1}^{m} P_i^{e_i}$. A prime ideal P of A is said to *ramify* in B (or in L) if any one of the ramification indices e_i is ≥ 1.

In this section, we will characterise those prime ideals of A which ramify in B. In particular, we want to show that only finitely many prime ideals of A ramify in B. First we need some lemmas.

Lemma 6.1. *Let A be a ring, let $B_1, \dots, B_q$ be rings containing A, which are free A-modules of finite-type. Let $B = \prod_{i=1}^{q} B_i$ be the product ring. Then the discriminant is :*

$$\mathscr{D}_{B/A} = \prod_{i=1}^{q} \mathscr{D}_{B_i/A}.$$

Proof. We will prove the lemma for $q = 2$ and the rest will follow by induction.

So, for $q = 2$, i.e., $B = B_1 \times B_2$.

Let $\{x_1, \dots, x_m\}$, $\{y_1, \dots, y_m\}$ be bases for B_1, B_2 as A-modules.

B_1 is identified with $B_1 \times (0)$ and B_2 is identified with $(0) \times B_2$. We may consider $\{(x_1, 0), \dots, (x_m, 0), (0, y_1), \dots, (0, y_m)\}$ as a base for $B = B_1 \times B_2$ over A.

By definition of product ring structure, $x_i y_j = 0$, so, $Tr(x_i y_j) = 0$.

Therefore,

$$D((x_1,0),\dots,(x_m,0),(0,y_1),\dots,(0,y_m)) = det \begin{pmatrix} Tr(x_i x_j) & 0 \\ 0 & Tr(y_i y_j). \end{pmatrix}$$

So,

$$D((x_1,0),\dots,(x_m,0),(0,y_1),\dots,(0,y_m)) = det(Tr(x_i x_j) \cdot Tr(y_i y_j))$$

$$= det(Tr(x_ix_j)) \cdot det(Tr(y_iy_j)) = D(x_1, \ldots, x_m) \cdot D(y_1, \ldots, y_m).$$

□

Lemma 6.2. *Let A, B be rings, $A \subset B$ and I be an ideal of A. Assume that B is a free A-module with base $\{x_1, \ldots, x_n\}$. For $x \in B$, $\bar{x}$ be the residue class of x in B $(\mathrm{mod}\ IB)$. Then $\{\bar{x_1}, \ldots, \bar{x_n}\}$ is a base of B/IB over A/I and*

$$D(\bar{x_1}, \ldots, \bar{x_n}) = \overline{D(x_1, \ldots, x_n)}.$$

Proof. Let $x \in B$. If the matrix of multiplication by x with respect to the base $\{x_1, \ldots, x_n\}$ is (a_{ij}), where $a_{ij} \in A$ for every i, j, then the matrix of multiplication by $\bar{x}$ with respect to the base $\{\bar{x_1}, \ldots, \bar{x_n}\}$ is $(\overline{a_{ij}})$.

Thus, $Tr(\bar{x}) = \overline{Tr(x)}$.

Let $x = x_ix_j$, we get $Tr(\overline{x_i}\overline{x_j}) = Tr(\overline{x_ix_j}) = \overline{Tr(x_ix_j)}$. So,

$$\begin{aligned} D(\{\bar{x_1}, \ldots, \bar{x_n}\}) &= det(Tr(\overline{x_i}\overline{x_j}) = det(\overline{Tr(x_ix_j)}) \\ &= \overline{det(Tr(x_ix_j))} = \overline{D(x_1, \ldots, x_n)}. \end{aligned}$$

□

Lemma 6.3. *Let K be a field which is finite or characteristic of K is 0. Let L be a finite dimensional (commutative) K-algebra. L is reduced, i.e., has no non-zero nilpotent elements if and only if $\mathscr{D}_{L/K} \neq (0)$.*

Proof. Suppose L is not reduced. Let $x \in L$ be a non-zero nilpotent element. Let $\{x_1, \ldots, x_n\}$ be a base for L over K, such that $x = x_1$.

Then $x_1 \cdot x_j$ is nilpotent for every j and multiplication by x_1x_j is a nilpotent endomorphism of the vector space L over K. Thus, all the characteristic values of this endomorphism are zero. So, $Tr(x_1x_j) = 0$.

The matrix $(Tr(x_ix_j))$ has a row comprised entirely of zeroes. Hence, $D(x_1, \ldots, x_n) = 0$, i.e., $\mathscr{D}_{L/K} = 0$.

Next suppose that L is reduced. Then the ideal (0) of L is expressible as a finite intersection of prime ideals, i.e., there exist prime ideals $P_1, \ldots, P_q$ in $\mathcal{O}_L$ such that $(0) = \bigcap\limits_{i=1}^{q} P_i$.

Since, L/P_i is an integral domain and a finite dimensional algebra over K, it is a field. Hence, P_i is a maximal ideal of L and $P_i + P_j = L$ for $i \neq j$. Therefore,

$L \cong \prod_{i=1}^{q} L/P_i$ (by Chinese Remainder Theorem and since $P_1 \cap \cdots \cap P_q = P_1 \ldots P_q = (0)$).

By Lemma 7.1, $\mathscr{D}_{L/K} = \prod_{i=1}^{q} \mathscr{D}_{L/P_i/K}$. But $\mathscr{D}_{L/P_i/K} \neq (0)$ since K is a finite field or a field of characteristic zero.

Therefore, $\mathscr{D}_{L/K} \neq (0)$. □

Definition 6.2. *Let K and L be number fields with $K \subset L$. Let A and B be the rings of integers of K and L, i.e., $\mathcal{O}_K = A$ and $\mathcal{O}_L = B$. The discriminant of B over A ($\mathscr{D}_{B/A}$) is the ideal of A generated by the discriminants of bases of L over K, which are contained in B.*

Remark 6.1. *If $\{x_1, \ldots, x_n\}$ is a base of L over K contained in B then $Tr_{L/K}(x_i x_j) \in A$. So, $D(x_1, \ldots, x_n) \in A$. Thus, $\mathscr{D}_{B/A}$ is an integral ideal of A. It is non-zero as $D(x_1, \ldots, x_n) = (det(a_{ij})^2 \neq 0$, where (a_{ij}) is the matrix of multiplication of $D(x_1, \ldots, x_n)$ with respect to the given base.*

Remark 6.2. *When B is a free A-module (example, when A is principal), we have already defined the discriminant $\mathscr{D}_{B/A}$ as the ideal generated by $D(e_1, \ldots, e_n)$, where $\{e_1, \ldots, e_n\}$ is an A-module base for B.*

Our old definition coincides. Given any base $\{x_1, \ldots, x_n\}$ of L over K contained in B, $x_i = \sum_{j=1}^{n} a_{ij} e_j$, with $a_{ij} \in A$.

Therefore, $D(x_1, \ldots, x_n) = (det(a_{ij}))^2 D(e_1, \ldots, e_n)$.

Theorem 6.3. *Let the notations be as in the definition. In order that a prime ideal P of A ramify in B, it is necessary and sufficient that it contain the discriminant $\mathscr{D}_{B/A}$. Hence there are only finitely many prime ideals of A which ramify in B.*

Proof. Let $PB = P_1^{e_1} \ldots P_g^{e_g}$, where $P_1, \ldots, P_g$ are distinct prime ideals in B and $e_1, \ldots, e_g$ are their ramification indices.

Suppose P is a ramified prime. Then $e_i > 1$ for some i and thus the ring $B/P_i^{e_i}$ contains a non-zero nilpotent element (which may be taken to be any element of $P_i^{e_i - 1} - P_i^{e_i}$), and hence so does B/PB. So, B/PB is not reduced and thus $\mathscr{D}_{(B/PB)/(A/P)} = (0)$ (by the previous lemma).

Now put $S = A - P$, $A' = S^{-1}A$, $B' = S^{-1}B$, and $P' = S^{-1}P$. Then A' is a principal ideal ring, B' is a free A'-module, $A/P \cong A'/P'$, and $B/PB \cong$

$B'/P'B'$. Therefore, writing $\{e_1, \ldots, e_n\}$ for an A'-module base of B', we know that $\mathscr{D}_{(B/PB)/(A/P)} = (0)$ if and only if $D(e_1, \ldots, e_n) \in P'$ (because of Lemma 7.2).

If $D(e_1, \ldots, e_n) \in P'$ and if $\{x_1, \ldots, x_n\}$ is a base for L over K contained in B, then $x_i = \sum a'_{ij}e_j$, with $a'_{ij} \in A'$ (because $B \subset B'$). So,

$$D(x_1, \ldots, x_n) = det(a'_{ij})^2 D(e_1, \ldots, e_n) \in P'.$$

Since $P' \cap A = P$, we can say that $D(x_1, \ldots, x_n) \in P$ and $\mathscr{D}_{B/A} \subset P$.

Conversely, if $\mathscr{D}_{B/A} \subset P$ then $D(e_1, \ldots, e_n) \in P'$ (since we can write $e_i = y_i s^{-1}$, with $y_i \in B$ and $s \in S$, for $1 \leq i \leq n$. Thus,

$$D(e_1, \ldots, e_n) = \frac{1}{s^{2n}} D(y_1, \ldots, y_n) \in A'\mathscr{D}_{B/A} \subset A'P = P'.)$$

The second assertion follows from the fact that $\mathscr{D}_{B/A}$ is a non-zero integral ideal of A and thus Dedekind's theorem applies.

□

Corollary 6.4. *Let K be a number field. A rational prime p ramifies if and only if p divides d_K. In particular, only finitely many primes of $\mathbb{Z}$ ramify in K.*

6.4 Galois extensions of number fields

We will recall a few results from Galois theory to facilitate the rest of the chapter.

Given a field L and a set G of automorphisms of L, the set $x \in L$ such that $\sigma(x) = x$, for every $\sigma \in G$ is a subfield of L, called the *fixed field* of G.

For an extension L of a field K, the set of K-automorphisms of L is a group under composition of mappings.

Theorem 6.4. *Let L be an extension of finite degree n of a field K, where K is finite or of characteristic zero. Then the following are equivalent:*

(A) K is fixed field of the group G of K-automorphisms of L.

(B) For every $x \in L$ the minimal polynomial of x over K has all its roots in L.

(C) L is generated by the roots of a polynomial with coefficients in K.

Under the above conditions, the group G of K-automorphisms of L is of order n.

Definition 6.3. *If the above conditions are satisfied, L is called a* ***Galois extension*** *of K and G is called the* ***Galois group*** *of L over K.*

If G is abelian (respectively, cyclic), L is called an abelian (respectively, cyclic) extension of K.

Corollary 6.5. *Let K be a finite field or of characteristic zero. Let $dim_K(L) = n$. If H is a group of automorphisms of L such that K is the fixed field of H and $|H| = n$, then L is a Galois extension of K and $Gal(L/K) = H$.*

Theorem 6.5. *(**Fundamental theorem of Galois theory**) Let K be a field which is finite or of characteristic zero. Let L be a Galois extension of K and $G = Gal(L/K)$. To any subgroup G' of G, let $k(G')$ be the fixed field of G'. To any subfield K' of L containing K, let $g(K')$ be the subgroup of G consisting of all K'-automorphisms of L.*

(A) The mappings g and k are bijections and are inverses of one another. They are both decreasing with respect to the inclusion relations on G, i.e., they reverse inclusions. The field L is a Galois extension of any intermediate field K' (i.e., $K \subset K' \subset L$).

(B) In order that an intermediate field K' be a Galois extension of K, it is necessary and sufficient that $g(K')$ be a normal subgroup of G. In this case, $Gal(K'/K) \cong G/g(K')$.

Example 6.2. (**Quadratic extensions**) Let $dim_K(L) = 2$. $L = K[x]$ for some $x \in L$ which is a root of $X^2 - d$, where d is the discriminant and is square-free. The other root of this polynomial is $-x$. There exists a non-trivial K-automorphism such that $\sigma(x) = -x$, i.e., $\sigma(a+bx) = a-bx$, where $a, b \in K$.

Clearly, $\sigma^2 = 1$ and K is the fixed field of σ. Thus L is a Galois extension of K with cyclic Galois group $\{1, \sigma\}$.

Example 6.3. (**Cyclotomic extensions**) Let K be a field of characteristic zero. Let ζ_n be a primitive $n-th$ root of unity in an extension of K, and let $L = K(\zeta_n)$. The field L is called a *cyclotomic extension* of K.

The minimal polynomial of ζ_n over K divides $X^n - 1$. So, its roots are $n-th$ roots of unity and consequently power of ζ_n. Thus L is a Galois extension of K by the previous theorem.

Let $G = Gal(L/K)$. Any $\sigma \in G$ is determined by its effect on ζ_n. More precisely, $\sigma(\zeta_n)$ is a power $\zeta_n^{j(\sigma)}$ of ζ_n, where $j(\sigma)$ is uniquely determined modulo n.

For $\sigma, \tau \in G$, $\sigma(\tau(\zeta_n)) = \sigma(\zeta_n^{j(\tau)}) = \zeta_n^{j(\tau)j(\sigma)}$. So, $j(\sigma\tau) \equiv j(\sigma)j(\tau) \pmod{n}$.

In other words, $\sigma \longmapsto j(\sigma)$ defines a homomorphism of $G \longrightarrow (\mathbb{Z}/n\mathbb{Z})^*$. Since $j(\sigma)$ determines σ, this homomorphism is injective, and G is abelian.

Thus any cyclotomic extension is abelian. If n is a prime p, this extension is even cyclic and G is isomorphic to a subgroup of $(\mathbb{Z}/p\mathbb{Z})^* = \mathbb{F}_p^*$.

Example 6.4. (**Finite fields**) Let $\mathbb{F}_q$ be a finite field ($q = p^s$, with p prime). Any extension of finite degree of $\mathbb{F}_q$ is of the form $\mathbb{F}_{q^n}$. Its degree is n.

The mapping $x \longmapsto x^q$ is an automorphism of $\mathbb{F}_{q^n}$ with $\mathbb{F}_q$ as its fixed field. For any $x \in \mathbb{F}_{q^n}$, we have $\sigma^j(x) = x^{q^j}$ and $\sigma^n = 1$ (since $x \in \mathbb{F}_{q^n}$ satisfies the relation $x^{q^n} = x$).

On the other hand, for $1 \leq j \leq n-1$, $\sigma^j \neq 1$ since if $j < n$, there exists $x \in \mathbb{F}_{q^n}$ such that $x^{q^j} \neq x$. (Suppose for $j < n$ and $\sigma^j(x) = x^{q^j} = x$, for every $x \in \mathbb{F}_{q^n}$. Hence, every $x \in \mathbb{F}_{q^n}$ satisfies $P(X) = X^{q^j} - 1$, thus the number of solutions of $P(X) \geq q^n$. Also since $\mathbb{F}_{q^n}$ is a field, so the number of solutions of $P(X) \leq q^n$. This is a contradiction.)

Thus $\{1, \sigma, \ldots, \sigma^{n-1}\}$ is a cyclic group of order n.

According to the Corollary 6.5, $\mathbb{F}_{q^n}$ is a cyclic extension of degree n of $\mathbb{F}_q$. Its Galois group has a canonical generator, the mapping $x \longmapsto x^q$. This mapping is called the **Frobenius automorphism**.

Now assume L is Galois over K, with $G = Gal(L/K)$. Let P be a prime ideal of $\mathcal{O}_K$. If $\mathcal{P}$ is lying above P in $\mathcal{O}_L$, i.e. $\mathcal{P} \mid P\mathcal{O}_L$ and $\sigma \in G$, then $\sigma(\mathcal{P})$ is a prime ideal above P. Indeed, $\sigma(\mathcal{P}) \cap \mathcal{O}_K \subset K$, thus $\sigma(\mathcal{P}) \cap \mathcal{O}_K = \mathcal{P} \cap \mathcal{O}_K$ since K is fixed by σ.

Theorem 6.6. *With the hypothesis as above, let*

$$P\mathcal{O}_L = \prod_{i=1}^{g} \mathcal{P}_i^{e_i}$$

be the factorisation of $P\mathcal{O}_L$ in $\mathcal{O}_L$. Then G acts transitively on the set $\{\mathcal{P}_1, \ldots, \mathcal{P}_g\}$. Furthermore, we have that

$$\begin{aligned} e_1 = \cdots = e_g &= e, \\ f_1 = \cdots = f_g &= f, \text{ and} \\ [L:K] &= efg. \end{aligned}$$

Proof. To show G acts transitively, let $\mathcal{P}$ be one of the $\mathcal{P}_i$. We need to prove that there exists $\sigma \in G$ such that $\sigma(\mathcal{P}_j) = \mathcal{P}$, for $\mathcal{P}_j$ any other of the $\mathcal{P}_i$'s.

We have seen previously that there exists $\beta \in \mathcal{P}$ such that $\beta\mathcal{O}_L\mathcal{P}^{-1}$is an integral ideal coprime to $P\mathcal{O}_L$. The ideal

$$I = \prod_{\sigma \in G} \sigma(\beta\mathcal{O}_L\mathcal{P}^{-1})$$

is an integral ideal of $\mathcal{O}_L$ (since $\beta\mathcal{O}_L\mathcal{P}^{-1}$ is), which is again coprime to $P\mathcal{O}_L$ (since $\sigma(\beta\mathcal{O}_L\mathcal{P}^{-1})$ and $\sigma(P\mathcal{O}_L)$ are coprime and $\sigma(P\mathcal{O}_L) = \sigma(P)\sigma(\mathcal{O}_L) = P\mathcal{O}_L$).

Thus I can be rewritten as

$$I = \frac{\prod_{\sigma \in G} \sigma(\beta)\mathcal{O}_L}{\prod_{\sigma \in G} \sigma(\mathcal{P})} = \frac{N_{L/K}(\beta)\mathcal{O}_L}{\prod_{\sigma \in G} \sigma(\mathcal{P})},$$

and we have that

$$I \prod_{\sigma \in G} \sigma(\mathcal{P}) = N_{L/K}(\beta)\mathcal{O}_L.$$

Since $N_{L/K}(\beta) = \prod_{\sigma \in G} \sigma(\beta)$, $\beta \in \mathcal{P}$ and one of the σ is identity, so we have that $N_{L/K}(\beta) \in \mathcal{P}$.

Furthermore, $N_{L/K}(\beta) \in \mathcal{O}_K$ since $\beta \in \mathcal{O}_L$, and we get that $N_{L/K}(\beta) \in \mathcal{P} \cap \mathcal{O}_K = P$.

Hence, P divides the right hand side of the above equation, and thus the lest hand side. Since I is coprime to P we get that P divides $\prod_{\sigma \in G} \sigma(\mathcal{P})$.

In other words, using the factorisation of P, we have that

$$\prod_{\sigma \in G} \sigma(\mathcal{P}) \text{ is divisible by } P\mathcal{O}_L = \prod_{i=1}^{g} \mathcal{P}_i^{e_i}$$

and each of the $\mathcal{P}_i$ has to be among $\{\sigma(\mathcal{P})\}_{\sigma \in G}$.

To show that all the ramification indices are equal, note that from the first part we know that there exists $\sigma \in G$ such that $\sigma(\mathcal{P}_i) = \mathcal{P}_k$, $i \neq k$. Now we have that

$$\sigma(P\mathcal{O}_L) = \prod_{i=1}^{g} \sigma(\mathcal{P}_i)^{e_1} = P\mathcal{O}_L = \prod_{i=1}^{g} \mathcal{P}_i^{e_i},$$

where the second equality holds since $P \in \mathcal{O}_K$ and L over K is Galois. By comparing the two factorisations of P and its conjugates, we get that $e_i = e_k$.

That all the inertial degrees are equal follows from the fact that σ induces the following field isomorphism

$$\mathcal{O}_L/\mathcal{P}_i \cong \mathcal{O}_L/\sigma(\mathcal{P}_i).$$

Finally we have that

$$|G| = n = [L : K] = efg.$$

□

6.4.1 Decomposition and inertia groups

In this section, A is a Dedekind domain, K is the field of fractions of A and characteristic of $K = 0$. Let K' be a Galois extension of degree n of K, and let A' be the integral closure of A in K'.

Let $x \in A'$ and let $\sigma \in G$. Applying σ to an equation of integral dependence of x over A shows that $\sigma(x) \in A'$.

Also, A' is stable under G, i.e., $\sigma(A') = A'$ for all $\sigma \in G$ (since, $\sigma(A') \subset A'$ and also, $\sigma^{-1}(A') \subset A'$, so, $A' = \sigma\sigma^{-1}(A') \subset \sigma(A')$).

On the other hand, if P is a maximal ideal of A and P' a maximal ideal of A' such that $P' \cap A = P($ i.e., P' appears in the factorisation of PA' into a product of prime ideals in A'). Then, $\sigma(P') \cap A = P$. So, $\sigma(P')$ also appears in the expression for PA', with the same exponent as P'.

We shall call P' and $\sigma(P')$ are **conjugate** prime ideals of A'. We are going to show that all the prime ideals in the prime factorisation of PA' in A' are conjugate.

Proposition 6.7. *From Theorem 7.6, we can say that the maximal ideals P_i' of A' which appear in the expression for PA' as a product of prime ideals in A' are all conjugate. They have the same residual degree f and the same ramification index e. Thus, $PA' = (\prod_{i=1}^{g} P_i')^e$ and $n = efg$.*

Proof. Suppose if, P' be one of the P_i's and assume that another of the P_i's, which we shall denote by Q', is not a conjugate to P'.

Since Q' and $\sigma(P')$ for $\sigma \in G$ are maximal and distinct, $\sigma(P') \not\subset Q'$. Now we need the following lemma.

Lemma 6.4. *Let R be a ring, $P_1, \dots, P_q$ a finite set of prime ideals of R, and let I be an ideal of R such that $I \not\subset P_i$ for any index i. Then there exists $b \in I$ such that $b \in P_i$ for any i.*

Proof. Without loss of generality, suppose $P_j \not\subset P_i$ for $i \neq j$. Let $x_{ij} \in P_j - P_i$ for $i \neq j$, $1 \leq i, j \leq q$. Since $I \not\subset P_i$, there exists $a_i \in I - P_i$. Put $b_i = a_i \prod\limits_{i \neq j} x_{ij}$. Then $b_i \in I$, $b_i \in P_j$ for $i \neq j$ and $b_i \notin P_i$ (since P_i is prime).

Thus, $b = b_1 + \cdots + b_q \in I - \bigcup\limits_{i=1}^{q} P_i$. □

Returning to the previous discussion, from the lemma we see that there exists $x \in Q'$ such that $x \notin \sigma(P')$ for all $\sigma \in G$.

Consider the norm of x, $N(x) = \prod\limits_{\tau \in G} \tau(x)$. Since $\tau(x) \in A'$ for every $\tau \in G$, we see that $N(x) \in Q'$, in fact $N(x) \in Q' \cap A = P$. Also, $x \notin \tau^{-1}(P')$. Hence, $\tau(x) \notin P'$ for any $\tau \in G$. Since P' is prime, $N(x) \notin P'$ and this contradicts $N(x) \in P$. □

Now let P' be a maximal ideal of A' such that $P' \cap A = P$.Those $\sigma \in G$ for which $\sigma(P') = P'$ form a subgroup D of G, called the **decomposition group** of P', denoted by $D(P')$.

If g denotes the number of conjugates of P', then $|G/D| = g = |G||D|^{-1}$, where $G/D = \{\sigma \in G | \sigma(P') \neq P'\} = \{\sigma \in G | \sigma_1(x) = \sigma_2(x)$ for every $x \in P', then [\sigma_1] = [\sigma_2]\}$. So, $card(D) = \frac{n}{g} = ef$.

For $\sigma \in D$, the relations $\sigma(A') = A'$ and $\sigma(P') = P'$ imply σ induces an automorphism $\overline{\sigma} : A'/P' \longrightarrow A'/P'$, where $x \pmod{P'} \longmapsto \sigma(x) \pmod{P'}$. This map is well-defined because $x \equiv y \pmod{P'}$ implies $\sigma(x) \equiv \sigma(y) \pmod{P'}$. So, $\overline{\sigma}$ is an A/P-automorphism.

Consider the mapping $D(P') \longrightarrow Aut_{A/P}(A'/P')$ such that $\sigma \longmapsto \overline{\sigma}$. This map is a group homomorphism.

Consider the kernel (I) of this map, $\overline{\sigma}(\bar{x}) = Id_{A'/P'}(\bar{x}) = \bar{x}$, for every $x \in A'/P'$. So, $\sigma(x) \pmod{P'} = x \pmod{P'}$ and thus, $\sigma(x) - x \in P'$, for every $x \in A'$. Hence, $I = \{\sigma \in D | \sigma(x) - x \in P'$ for every $x \in A'\}$.

Therefore, I is a normal subgroup of D, called the **inertia subgroup** of P'.

Proposition 6.8. *With the same notations as above, assume that A/P is finite or of characteristic zero. Then A'/P' is a Galois group of degree f of*

A/P, and the mapping $\sigma \longmapsto \overline{\sigma}$ is a surjective homomorphism of D on the Galois group of A'/P' over A/P. Moreover, $card(I) = e$.

Proof. Let K_D be the fixed field of D. Let $A_D = A' \cap K_D$ and $P_D = P' \cap A_D$ be the prime ideal.

According to the previous proposition and the definition of D, P' is the only prime factor of $A'P_D$.

Put $A'P_D = (P')^{e'}$ and write f' for the residual degree of $[A'/P' : A_D/P_D]$. According to the fundamental identity of the splitting of prime ideals, we have $e'f' = [K' : K_D] = card(D) = ef$.

Since $A/P \subset A_D/P_D \subset A'/P'$. So, $f' \leq f$. Also since $PA_D \subset P_D$, we get $e' \leq e$.

Therefore, $e = e'$ and $f = f'$ and thus $A/P \cong A_D/P_D$.

Now let $\bar{x}$ be a primitive element for A'/P' over A/P and let $x \in A'$ be a representative of $\bar{x}$. Let $X^r + a_{r-1}X^{r-1} + \cdots + a_o = P(X)$ be the minimal polynomial for x over K_D.

We know that $a_i \in A_D$. The roots of $P(X)$ are all of the form $\sigma(x)$ with $\sigma \in D$.

The reduced polynomial $\bar{P}(X) = X^r + \bar{a}_{r-1}X^{r-1} + \cdots + \bar{a}_0$ has its coefficients in A/P and the roots of $\bar{P}(X)$ are all of the form $\bar{\sigma}(\bar{x})$ with $\sigma \in D$.

Consequently, A'/P' contains all conjugates of $\bar{x}$ over A/P and A'/P' is a Galois extension of A/P.

Also, since every conjugate of $\bar{x}$ over A/P is of the form $\bar{\sigma}(\bar{x})$, every A/P-automorphism of A'/P' is of the form $\bar{\sigma}$ for some $\sigma \in D$. Thus the Galois group of A'/P' over A/P may be identified with D/I.

Since the order of $[A'/P' : A/P] = f$, so, $card(I) = e$. □

Corollary 6.6. *In order that P not ramify in A' it is necessary and sufficient that the inertia group I of P' (of any P' over P) be trivial.*

Remark 6.3. Write $D_{P'}$, $I_{P'}$ for the decomposition and inertia groups of the maximal ideal $P' \subset A'$. For a conjugate ideal $\sigma(P')$, for $\sigma \in G$

$$D_{\sigma(P')} = \sigma D_{P'} \sigma^{-1} \text{ and } I_{\sigma(P')} = \sigma I_{P'} \sigma{-}1.$$

To prove the above statement, note that for $\tau \in D_{P'}$, we have

$$\sigma\tau\sigma^{-1}(\sigma(P')) = \sigma\tau(P') = \sigma(P').$$

So, $\sigma D_{P'}\sigma^{-1} \subset D_{\sigma(P')}$. For the reverse inclusion, let $\tau \in D_{\sigma(P')}$. So,

$$\tau(\sigma(P')) = \sigma(P'), i.e., \sigma^{-1}\tau\sigma(P') = \sigma^{-1}\sigma(P') = P'.$$

So, $\sigma^{-1}\tau\sigma \in D_{P'}$. Thus, $\tau \in \sigma D_{P'}\sigma^{-1}$.

Similarly, for $\tau \in I_{P'}$ and $x \in A'$,

$$\sigma\tau\sigma^{-1}(x) - x = \sigma\tau(\sigma^{-1}(x)) - \sigma\sigma^{-1}(x) = \sigma(\tau(\sigma^{-1}(x) - \sigma^{-1}(x)) \in \sigma(P').$$

So $\sigma I_{P'}\sigma^{-1} \subset I_{\sigma(P')}$. The reverse inclusion follows from a similar argument.

So when K' is an abelian extension of K, the groups $D_{\sigma(P')}$ for $\sigma \in G$ are all equal, and so are $I_{\sigma(P')}$. They only depend on the ideal P of the ring A.

6.5 The Frobenius automorphism

Let K, K' be number fields such that K' is a Galois extension of K with Galois group G. Let $A = \mathcal{O}_K$ and $A' = \mathcal{O}_{K'}$. Let P be a maximal ideal of A which does not ramify in A', and let P' be a prime factor of PA'.

The inertia group (I) of P' consists only of the identity of G alone and its decomposition group D is canonically isomorphic to the Galois group of A'/P' over A/P.

But the Galois group of A'/P' over A/P is cyclic with a canonical generator $\bar{\sigma} : \bar{x} \longmapsto \bar{x}^q$, where $q = card(A/P)$.

Thus, D itself is cyclic with a canonical generator σ defined by the relation $\sigma(x) \equiv x^q \pmod{P'}$ for any $x \in A'$. This generator is called the **Frobenius automorphism** of P'. We denote it by $(P', K'/K)$.

For $\tau \in G$, we have (as in the remark),

$$(\tau(P'), K'/K) = \tau(P', K'/K)\tau^{-1}.$$

In particular, if K' is an abelian extension, $(P', K'/K)$ depends only on the ideal P of A. In this case we write, $(\frac{K'/K}{P})$.

Proposition 6.9. *With the preceding hypothesis and notations, let F be an intermediate field ($K \subset F \subset K'$) and write f for the residual degree of $P' \cap F$ over K. Then :*

(a) $(P', K'/F) = (P', K'/K)^f$,

(b) If F is Galois over K, the restriction of $(P', K'/K)$ to F equals $(P' \cap F, F/K)$.

Proof. (a) Put $\sigma = (P', K'/K)$. By definition, $\sigma(P') = P'$ and $\sigma(x) \equiv x^q \pmod{P'}$ for every $x \in A'$, where $q = card(A/P)$.

Thus $\sigma^f(P') \equiv x^{q^f} \pmod{P'}$ for every $x \in A'$. By definition of f, q^f is the cardinality of the residual field $(A' \cap F)/(P' \cap F)$. Also, the decomposition group of P' over F is obviously a subgroup of the decomposition D of P' over K. It is of order

$$[A'/P' : (A' \cap F)/(P' \cap F)] = \frac{1}{f}[A'/P' : A/P] = \frac{1}{f}card(D).$$

Since D is cyclic and generated by σ, the only subgroup of D of order $\frac{card(D)}{f}$ is generated by σ^f. This completes the proof of (a).

(b) Suppose F is Galois over K and write σ' for the restriction of σ to F.

Since $\sigma(P') = P'$, it follows that $\sigma(P' \cap F) = P' \cap F$ and σ' belongs to the decomposition group of $P' \cap F$ over K. Also, it is clear that $\sigma'(x) \equiv x^q \pmod{P' \cap F}$, for every $x \in A' \cap F$, with $q = card(A/P)$. □

6.5.1 Application to cyclotomic fields

We are going to utilise the theory we just developed to present another proof of irreducibility of the cyclotomic polynomial.

Theorem 6.7. *Let ζ be a primitive complex $n - th$ root of unity. Then:*

(a) No prime number which does not divide n ramifies in $\mathbb{Q}[\zeta]$.

(b) $\mathbb{Q}[\zeta]$ is an abelian extension of $\mathbb{Q}$ of degree $\varphi(n)$ and with Galois group isomorphic to $(\mathbb{Z}/n\mathbb{Z})^*$.

Proof. (a) Let $F(X)$ be the minimal polynomial of ζ over $\mathbb{Q}$ and let $deg(F(X)) = d$, i.e. $d = dim_{\mathbb{Q}}(\mathbb{Q}[\zeta])$. The polynomial $F(X)|X^n - 1$. Let $X^n - 1 = F(X)G(X)$. So, $nX^{n-1} = F'(X)G(X) + F(X)G'(X)$.

Put $X = \zeta$ in the above equation. We get, $n\zeta^{n-1} = F'(\zeta)G(\zeta)$. Since ζ is a unit of $\mathbb{Q}[\zeta]$, it is of norm ± 1.

Upon taking norms, $N(n\zeta^{n-1}) = N(F'(\zeta)G(\zeta))$, i.e., $n^d(\pm 1) = N(F'(\zeta))N(G(\zeta))$. We also know that the discriminant $D(1, \zeta, \ldots, \zeta^{d-1}) = \pm N(F'(\zeta))$. Hence, $N(F'(\zeta))|n^d$, i.e., $D(1, \zeta, \ldots, \zeta^{d-1})|n^d$.

From theorem, in order that a prime ideal P of A ramify in B, it is necessary and sufficient that it contain the discriminant $\mathscr{D}_{B/A}$. There are only finitely many prime ideals of A which ramify in B.

Therefore, no prime number which does not divide n, ramifies in $\mathbb{Q}[\zeta]$. This proves (a).

(b) Recall that $\mathbb{Q}[\zeta]$ is an abelian extension of $\mathbb{Q}$ and that there is an injective homomorphism j of the Galois group G of $\mathbb{Q}[\zeta]$ over $\mathbb{Q}$ into $(\mathbb{Z}/n\mathbb{Z})^*$.

More precisely, the element $\sigma \in G$ raises all the $n-th$ roots of unity to the power $j(\sigma)$. Let p be a prime number which does not divide n.

By (a), the Frobenius automorphism $\frac{\mathbb{Q}[\zeta]/\mathbb{Q}}{p}$ is defined, denote it by σ_p.

Writing A for the ring of integers of $\mathbb{Q}[\zeta]$ and P for an arbitrary prime factor of pA', we obtain, from the definition of Frobenius automorphism the relation $\sigma_p(x) \equiv x^p \pmod{P}$ for every $x \in A$. In particular, let $j = j(\sigma_p)$, we get $\zeta^j \equiv \zeta^p \pmod{P}$.

Let $P(X) = X^n - 1 = \prod_{0 \leq r \leq n-1} (X - \zeta^r)$. Then recall that

$$\prod_{0 \leq r \leq n-1; r \not\equiv p \pmod{n}} (\zeta^p - \zeta^r) = P'(\zeta^p) = n\zeta^{p(n-1)}.$$

So n is relatively prime to p, since $P \cap \mathbb{Z} = p\mathbb{Z}$ and since ζ is a unit in the ring of integers of $\mathbb{Q}[\zeta]$, we may conclude from the relation $P'(\zeta^p) = n\zeta^{p(n-1)}$ that, $\prod_{\substack{0 \leq r \leq n-1 \\ r \not\equiv p \pmod{n}}} (\zeta^p - \zeta^r) \notin P$.

The relation $\zeta^{\equiv}\zeta^p \pmod{P}$ thus implies that j represents the residue class of p modulo n. Hence $j(G)$ contains the residue class modulo n of all prime numbers p which do not divide n.

This means, $j(G) = (\mathbb{Z}/n\mathbb{Z})^*$. This proves (b). □

6.5.2 Proof of Quadratic reciprocity laws

Let q be an odd prime. Let K be the cyclotomic field generated by a primitive $q-th$ root of unity in $\mathbb{C}$. The $Gal_{\mathbb{Q}}(K) = G \cong \mathbb{F}_q^*$. It is cyclic and of even order $q-1$.

There is a unique subgroup H of index 2, which corresponds to the subgroup of squares $(\mathbb{F}_q^*)^2 \subset \mathbb{F}_q^*$. Thus, K contains a unique quadratic field $\mathbb{F}$.

No prime number $p \neq q$ ramifies in $\mathbb{F}$ for, if it did, it would ramify in K. This would contradict the theorem in the previous section.

Set

$$\mathbb{F} = \mathbb{Q}(\sqrt{q}) \text{ if } q \equiv 1 \pmod 4$$
$$\mathbb{F} = \mathbb{Q}(\sqrt{-q}) \text{ if } q \equiv 3 \pmod 4.$$

Note that when $q \equiv 3 \pmod 4$, then $-q \equiv 1 \pmod 4$. Put $q^* = (-1)^{\frac{q-1}{2}} q$. So, $\mathbb{F} = \mathbb{Q}[\sqrt{q^*}]$.

Let p be a prime number and $p \neq q$. Write σ_p for the Frobenius automorphism $(\frac{K/\mathbb{Q}}{p})$. The restriction to $\mathbb{F}$ is $(\frac{\mathbb{F}/\mathbb{Q}}{p})$. It is the identity if $\sigma_p \in H$, i.e., if the exponent $j(\sigma_p) =$ residue class of $p \pmod q$ is a square in $\mathbb{F}_q^*$. Otherwise, it is the nontrivial automorphism of $\mathbb{F}$.

In other words, identifying the Galois group G/H of $\mathbb{F}$ over $\mathbb{Q}$ with $\{+1, -1\}$. We have,

$$\left(\frac{\mathbb{F}/\mathbb{Q}}{p}\right) = \left(\frac{p}{q}\right), \tag{6.1}$$

by the definition of Legendre symbol.

On the other hand, theory regarding splitting of primes below in an extension $\mathbb{F}$ tells that:

1. If p splits in $\mathbb{F}$, then $\left(\frac{\mathbb{F}/\mathbb{Q}}{p}\right) = Id$ automorphism.

2. If p remains a prime in $\mathbb{F}$, then $\left(\frac{\mathbb{F}/\mathbb{Q}}{p}\right)$ is the non-trivial automorphism.

If p is odd,

$$\left(\frac{\mathbb{F}/\mathbb{Q}}{p}\right) = \left(\frac{q^*}{p}\right). \tag{6.2}$$

Comparing the equations (6.1) and (6.2), we get

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

But,

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

Thus,

$$\left(\frac{p}{q}\right) = (-1)^{\frac{(p-1)(q-1)}{4}} \left(\frac{q}{p}\right).$$

For the case $p = 2$,

$$\begin{aligned}&2 \text{ splits in } \mathbb{F} \text{ if } q^* \equiv 1 \pmod 8,\\ &2 \text{ remains a prime in } \mathbb{F} \text{ if } q^* \equiv 5 \pmod 8.\end{aligned}$$

However, $(-1)^{\frac{q^2-1}{8}} = (-1)^{\frac{(q^*)^2-1}{8}} = +1$ if $q^* \equiv 1 \pmod 8$ and $= -1$ if $q^* \equiv 5 \pmod 8$. Thus,

$$\left(\frac{\mathbb{F}/\mathbb{Q}}{2}\right) = (-1)^{\frac{q^2-1}{8}}. \tag{6.3}$$

So, from the equations (6.1) and (6.3), we get

$$\left(\frac{2}{q}\right) = (-1)^{\frac{q^2-1}{8}}.$$

Chapter 7

Dirichlet's class number formula

We begin this chapter, by recalling a few facts about the Riemann zeta function.

Definition 7.1. *The* ***Riemann zeta function****, denoted by $\zeta(s)$ is defined for all $\Re(s) > 1$ by the convergent series*

$$\zeta(s) := \sum_{n \geq 1} \frac{1}{n^s}.$$

Theorem 7.1. ***(Euler product)*** *The above series converges absolutely for all $\Re(s) > 1$ and there $\zeta(s)$ can be written as an infinite product*

$$\zeta(s) = \prod_{p \in \mathbb{N}} \left(1 - \frac{1}{p^s}\right)^{-1},$$

where the product is taken over all prime numbers $p \in \mathbb{N}$.

Theorem 7.2. *The Riemann zeta function has a meromorphic extension to the whole complex plane with a simple pole at $s = 1$ and no other poles. The residue of $\zeta-$ function at $s = 1$ is 1, i.e.,*

$$\lim_{s \to 1^+} (s-1)\zeta(s) = 1.$$

7.1 Dedekind zeta function

Let K be an algebraic number field of degree n. The group $\mathcal{H}_K$ of ideal classes of K is a finite group of order $h = h_K$. In this chapter, we will try to obtain a formula for h when K is a quadratic field.

Let $C_0 = 1, C_1, \dots, C_{h-1}$ denote the different ideal classes. For each class C, we define the zeta function of C, denoted by $\zeta_K(s, C)$ as

$$\zeta_K(s, C) \coloneqq \sum_{I(\neq 0) \in C} \frac{1}{N(I)^s}.$$

The summation is over all non-zero integral ideals I of C. For simplicity here we take $s > 1$, but the sum exists for an $s \in \mathbb{C}$ such that $\Re(s) > 1$.

The zeta function of the filed K, called the **Dedekind zeta function** and denoted by $\zeta_K(s)$, is defined by

$$\zeta_K(s) \coloneqq \sum_{C \in \mathcal{H}_K} \zeta_K(s, C) = \sum_{I \neq 0} \frac{1}{N(I)^s}.$$

The summation is now over all non-zero integral ideals of K.

Proposition 7.1. *The Dedekind zeta function $\zeta_K(s)$ converges absolutely for $s > 1$.*

Proof. Let $x > 0$ be a real number. We want to first show that

$$\sum_{N(I) \leq x} \frac{1}{N(I)^s} \leq \prod_{N(P) \leq x} \left(1 - \frac{1}{N(P)^s}\right)^{-1}, \tag{7.1}$$

the product being over all prime ideals P with $N(P) \leq x$.

Now,

$$\left(1 - \frac{1}{N(P)^s}\right)^{-1} = 1 + \frac{1}{N(P)^s} + \frac{1}{N(P)^{2s}} + \dots \tag{7.2}$$

By Dedekind's theorem, any integral ideal I can be written uniquely as a product of prime ideals. Further if $N(I) \leq x$ then every prime divisor P of I satisfies $N(P) \leq x$.

So, (7.1) follows from multiplying the series in (7.2) for all $N(P) \leq x$.

Also,

$$\prod_{N(P) \leq x} \left(1 - \frac{1}{N(P)^s}\right)^{-1} - \sum_{N(I) \leq x} \frac{1}{N(I)^s} = \sum_{N(I) > x} \frac{1}{N(I)^s}, \tag{7.3}$$

where the last summation is over the integral ideals I of norm $> x$, all of whose prime divisors are of norm $\leq x$.

Any prime ideal P contains a unique prime number $p \in \mathbb{Z}$. We have $N(P) = p^f$ for a certain integer $f \geq 1$ so that $p^f \leq x$ if $N(P) \leq x$.

Also there are at most n distinct prime ideals $P_1, \dots, P_g$, with $g \leq n$ containing a given p. In fact, they are uniquely determined by the equation

$$p\mathcal{O}_K = P_1^{e_1} \dots P_g^{e_g},$$

and

$$p^n = N(p\mathcal{O}_K) = \prod_{i=1}^{g} N(P_i)^{e_i} = \prod_{i=1}^{g} p^{f_i e_i} \geq p^g.$$

Hence (7.1) gives

$$\sum_{N(I) \leq x} \frac{1}{N(I)^s} \leq \prod_{p \leq x} \left(1 - \frac{1}{p^s}\right)^{-n},$$

(we can create the various norms of $N(I)^{-s}$ by choosing the required part from each product).

Since the product $\prod(1 - \frac{1}{p^s})^{-1}$ is absolutely convergent for $s > 1$, the series $\sum \frac{1}{N(I)^s}$ converges for $s > 1$. This completes the proof of the proposition. □

Remark 7.1. *If we now let $x \to \infty$ in equation (7.3) we obtain the Euler product for $\zeta_K(s)$, viz., $\zeta_K(s) = \prod\limits_{P}(1 - \frac{1}{N(P)^s})^{-1}$. This equality in fact holds for $s \in \mathbb{C}$ and $Re(s) > 1$.*

Remark 7.2. *The Euler product is in fact a more general phenomenon of the under lying multiplicative structure. If $\{a_m\}$ is a sequence of complex numbers with $a_1 = 1$ $a_{mk} = a_m a_k$ for all integers $m, k \geq 1$, and if $\sum\limits_{m=1}^{\infty} |a_m| < \infty$, then*

$$\sum_{m=1}^{\infty} a_m = \prod_{p} (1 - a_p)^{-1}.$$

In particular, for $Re(s) > 1$, we have

$$\zeta(s) = \sum_{m=1}^{\infty} \frac{1}{m^s} = \prod_{p} \left(1 - \frac{1}{p^s}\right)^{-1}.$$

We now recall the **Wiener - Ikehara Theorem**. Consider the following general statement.

Theorem 7.3. *Let $A(x)$ be a non-negative, monotonic non-decreasing function of x, defined for $0 \leq x < \infty$. Suppose that*

$$\int_0^\infty A(x)e^{-xs}dx$$

converges for $Re(s) > 1$ to the function $f(s)$ and that , for some non-negative integer c,

$$f(s) - \frac{c}{s-1}$$

has an extension as a continuous function for $Re(s) \leq 1$. Then the limit as $x \to \infty$ of $e^{-1}A(x)$ is equal to c.

An important application of the theorem is to **Dirichlet series** of the form

$$\sum_{n \geq 1} \frac{a_n}{n^s},$$

where a_n is non-negative. If the series converges to an analytic function in $Re(s) \geq b$, with a simple pole of residue c at $s = b$, then

$$\sum_{n \leq x} a_n \sim \frac{c}{b} x^b.$$

Applying this Dirichlet series version to the logarithmic derivative of the Riemann zeta function, where the coefficients in the Dirichlet series are values of the *von Mangoldt function*, it is possible to deduce the *Prime number theorem* from the fact that the Riemann zeta function has no zeroes on the line $\Re(s) = 1$.

7.2 Class number formula for quadratic number fields

In this section, K stands for a quadratic number field, unless otherwise stated.

Definition 7.2. *Let K be a quadratic number field with discriminant d. Then the* ***Dirichlet*** L***-function*** $L_d(s)$ *defined for all $s > 1$ is given by*

$$L_d(s) = \sum_{n \geq 1} \left(\frac{d}{n}\right) \frac{1}{n^s}.$$

So Remark 7.1 applied to $a_m = \left(\frac{d}{m}\right)\frac{1}{m^s}$ gives us

$$L_d(s) = \sum_{m\geq 1}\left(\frac{d}{m}\right)\frac{1}{m^s} = \prod_p \left(1 - \left(\frac{d}{p}\right)\frac{1}{p^s}\right)^{-1}.$$

We will now state the *Dirichlet class number formula* for quadratic fields and then prove the propositions required to arrive at the result.

Theorem 7.4. ***(Dirichlet)*** *Let K be a quadratic field of discriminant d. Let h be the class number of K. Then we have*

$$h = \begin{cases} \frac{\sqrt{d}}{2log\eta}L_d(1) & \text{if } d > 0 \\ \frac{w\sqrt{d}}{2\pi}L_d(1) & \text{if } d < 0. \end{cases}$$

Here w counts the number of roots of unity in case of the imaginary quadratic fields and $\eta > 1$ is the fundamental unit in case of real quadratic fields.

Before proving this, we need to relate $\zeta_K(s)$ with the Riemann zeta function.

Proposition 7.2. *For $s > 1$, we have*

$$\zeta_K(s) = \zeta(s)L_d(s),$$

and hence holds for all complex number $\neq 1$.

Proof. We start with the Dirichlet L-function. We know that for all $n \in \mathbb{N}$, the symbol $(\frac{d}{n})$ for quadratic reciprocity is $-1, 0$, or 1 and so $|(\frac{d}{n})| \leq 1$. Hence $L_d(s)$ converges absolutely for $s > 1$.

Now note that since the symbol $(\frac{d}{n})$ is multiplicative, for $s > 1$ we can rewrite the L-series in Euler product form so that

$$L_d(s) = \prod_{p\in\mathbb{N}}\left(1 - \left(\frac{d}{p}\right)\frac{1}{p^s}\right)^{-1} = \prod_{(\frac{d}{p})=+1}\left(1 - \frac{1}{p^s}\right)^{-1}\prod_{(\frac{d}{q})=-1}\left(1 + \frac{1}{q^s}\right)^{-1}\prod_{(\frac{d}{r})=0} 1,$$

where p, q, r are all prime numbers.

Then we can perform the same splitting of the Euler product for the Riemann zeta function to get

$$\zeta(s)L_d(s) = \prod_{(\frac{d}{p})=+1}\left(1 - \frac{1}{p^s}\right)^{-2}\prod_{(\frac{d}{q})=-1}\left(1 + \frac{1}{q^s}\right)^{-1}\left(1 - \frac{1}{q^s}\right)^{-1}\prod_{(\frac{d}{r})=0}\left(1 - \frac{1}{r^s}\right)^{-1}$$

$$= \prod_{(\frac{d}{p})=+1} \left(1-\frac{1}{p^s}\right)^{-2} \prod_{(\frac{d}{q})=-1} \left(1-\frac{1}{q^{2s}}\right)^{-1} \prod_{(\frac{d}{r})=0} \left(1-\frac{1}{r^s}\right)^{-1}.$$

But we know that, if $(\frac{d}{p}) = +1$, then p split and there exist distinct prime ideals $P_1, P_2 \subset \mathcal{O}_K$ such that $p\mathcal{O}_K = P_1P_2$. Taking the norm gives $N(P_1P_2) = N(P_1)N(P_2) = N(p\mathcal{O}_K) = p^2$. But both ideals are prime and hence $N(P_i) \neq 1$ for $i = 1, 2$. Therefore, $N(P_1) = N(P_2) = p$.

If $(\frac{d}{q}) = -1$, then q remains a prime and $q\mathcal{O}_K = Q$ is a prime ideal, so $N(Q) = N(q\mathcal{O}_K) = q^2$.

Finally, if $(\frac{d}{r}) = 0$, then r is ramified and there exists a prime ideal $R \subset \mathcal{O}_K$ such that $r\mathcal{O}_K = R^2$. Therefore, $N(R) = r$.

Using these facts, we can write the Euler product in terms of norms of ideals:

$$\zeta(s)L_d(s) = \prod_{(\frac{d}{p})=+1} \left(1-\frac{1}{N(P_1)^s}\right)^{-1} \left(1-\frac{1}{N(P_2)^s}\right)^{-1} \prod_{(\frac{d}{q})=-1} \left(1-\frac{1}{N(Q)^s}\right)^{-1}$$
$$\prod_{(\frac{d}{r})=0} \left(1-\frac{1}{N(R)^s}\right)^{-1}.$$

But since every prime ideal in $\mathcal{O}_K$ must be one among the three cases mentioned above, every prime ideal must occur only once in the above product. Therefore, we can simplify it to

$$\zeta(s)L_d(s) = \prod_{P\subset\mathcal{O}_K} \left(1-\frac{1}{N(P)^s}\right)^{-1}.$$

But we know from Proposition 7.1 that the above product is $\zeta_K(s)$ for all $s > 1$. Therefore, $\zeta_K(s) = \zeta(s)L_d(s)$. □

Now we encounter a constant, known as the *Dirichlet structure constant* κ for a quadratic field K with discriminant d. We first need a lemma.

Lemma 7.1. *Let Ω be a bounded open set in the plane $\mathbb{R}^2$. For $X > 0$, let*

$$\Omega_X = \{\xi = (\xi_1, \xi_2) \in \mathbb{R}^2 | \left(\frac{\xi_1}{X}, \frac{\xi_2}{X}\right) \in \Omega\}.$$

Let $N_\Omega(X)$ denote the number of lattice points in Ω_X. Then, $\lim_{X\to\infty} \frac{N_\Omega(X)}{X^2} = \iint_\Omega d\xi_1 d\xi_2$ = area of Ω, provided that this integral exists in the sense of Riemann.

Proof. Divide the plane into squares S of side $\frac{1}{X}$ parallel to the coordinate axes. For any S, let $P(S)$ denote the point whose coordinates have smallest values (the lower-left vertex).

Clearly, $N_\Omega(X) = \{\text{number of squares } S \mid P(S) \in \Omega\}$. Now if N_1, N_2 denote, respectively, the number of $S \subset \Omega$ and $S \cap \Omega \neq \phi$, then by the definition of Riemann integral, $\frac{N_1}{X^2} \to \iint\limits_\Omega d\xi_1 d\xi_2$ and $\frac{N_2}{X^2} \to \iint\limits_\Omega d\xi_1 d\xi_2$.

Since $N_1 \leq N_\Omega(X) \leq N_2$, the result follows because in Riemann integration, $f \leq g$ implies $\int f \leq \int g$. □

Theorem 7.5. *Let K be a quadratic field with discriminant d and w the number of roots of unity in K. Let C be an ideal class of K and $N(X, C)$ the number of non-zero integral ideals $I \in C$ with $N(I) < X$. Then*

$$\lim_{X\to\infty} \frac{N(X,C)}{X} = \kappa,$$

exists and we have

$$\kappa = \begin{cases} \frac{2log\eta}{\sqrt{d}} & \text{if } d > 0 \\ \frac{2\pi}{w\sqrt{|d|}} & \text{if } d < 0. \end{cases}$$

Proof. Let J be an integral ideal in C^{-1}, then for any integral ideal $I \in C$, $IJ = \alpha\mathcal{O}_K$, where $\alpha \in J$ (because from a previous lemma, there exists $\omega \in \mathcal{O}_K$ such that $gcd(IJ, \omega\mathcal{O}_K) = J$. We know that $IJ = \alpha\mathcal{O}_K$ for $\alpha \in K$, thus, $gcd(\alpha\mathcal{O}_K, \omega\mathcal{O}_K) = J$, which means, $\alpha \in J$ and $\omega \in J$).

Conversely, if $\alpha \in J$, then $I = J^{-1}\alpha\mathcal{O}_K$ is an integral ideal in C.

Moreover, $|N_K(\alpha)| = N(I)N(J)$. So, $N(I) < X$ if and only if $|N_K(\alpha)| < XN(J) = Y$ (say). Consequently, $N(X, C)$ is the number of non-zero principal ideals in $\alpha\mathcal{O}_K$, $\alpha \in J$ such that $|N_K(\alpha)| < Y$.

In other words, $N(X, C) = \{\text{number of } \alpha \in J, \alpha \neq 0, \text{ which are pairwise non-associates and for which } |N_K(\alpha)| < Y\}$.

Case(i) $d > 0$: Let $\eta > 1$ be the fundamental unit. Clearly, for any $\alpha \in J$, $\alpha \neq 0$, there exists $m \in \mathbb{Z}$ such that if $\eta_1 = \alpha\eta^m$, we have

$$0 \leq \log\left|\frac{\eta_1}{|N_K(\eta_1)^{\frac{1}{2}}|}\right| < \log\eta. \tag{7.4}$$

Conversely, if η_1, η_2 are associate elements of J satisfying 8.4, then $\eta_1 = \epsilon\eta_2$, where ϵ is an unit with $1 \leq |\epsilon| < \eta$. So, $\epsilon = \pm 1$. Hence,

$$2N(X,C) = \{\text{number of } \eta_1 \in J \mid 0 < |N_K(\eta_1)| < Y, 0 \leq \log\left|\frac{\eta_1}{|N_K(\eta_1)^{\frac{1}{2}}|}\right| < \log\eta\}. \tag{7.5}$$

Case(ii) $d < 0$: In this case we have $wN(X,C) = \{\text{number of } \eta_1 \in J : 0 < |N_K(\eta_1)| < Y\}$.

In either case, let (β_1, β_2) be an integral base of J and let β_1', β_2' be the conjugates of β_1, β_2 respectively. Let Ω denote the following open set in the plane:

if $d > 0$,

$$\Omega = \{\xi = (\xi_1, \xi_2) \in \mathbb{R}^2 \mid 0 < |\xi_1\beta_1 + \xi_2\beta_2||\xi_1\beta_1' + \xi_2\beta_2'| < 1,$$
$$0 < \log\frac{|\xi_1\beta_1 + \xi_2\beta_2|}{|\xi_1\beta_1 + \xi_2\beta_2|^{\frac{1}{2}}|\xi_1\beta_1' + \xi_2\beta_2'|^{\frac{1}{2}}} < \log\eta\};$$

if $d < 0$,

$$\Omega = \{\xi = (\xi_1, \xi_2) \in \mathbb{R}^2 \mid 0 < |\xi_1\beta_1 + \xi_2\beta_2|^2 < 1\}.$$

We show Ω is bounded in both cases.

For $d > 0$, since $|\xi_1\beta_1 + \xi_2\beta_2||\xi_1\beta_1' + \xi_2\beta_2'| < 1$ and $\frac{|\xi_1\beta_1+\xi_2\beta_2|}{|\xi_1\beta_1'+\xi_2\beta_2'|} < \eta^2$, we see that both $\xi_1\beta_1 + \xi_2\beta_2$ and $\xi_1\beta_1' + \xi_2\beta_2'$ are bounded in Ω. Thus, ξ_1, ξ_2 are again bounded in Ω, since $\beta_1\beta_2' - \beta_2\beta_1' \neq 0$ (in fact, $\beta_1\beta_2' - \beta_2\beta_1' = \pm N(J)\sqrt{d}$ by $\triangle(I) = N(I)^2 d$). For $d < 0$, $|\xi_1\beta_1 + \xi_2\beta_2| = |\xi_1\beta_1' + \xi_2\beta_2'| < 1$ and again, since $\beta_1\beta_2' - \beta_2\beta_1' \neq 0$, we get that ξ_1, ξ_2 are bounded in Ω.

So now,

$$wN(X,C) = \begin{cases} \text{number of lattice points in } \Omega_{\sqrt{Y}} & \text{if } d > 0 \\ \text{number of lattice points in } \Omega_{\sqrt{Y}} + \text{number } A_Y & \text{if } d < 0 \\ \text{of lattice points } (\xi_1, \xi_2) \text{ with } |\xi_1\beta_1 + \xi_2\beta_2|^2 \leq Y \text{ and} & \\ |\xi_1\beta_1 + \xi_2\beta_2| = |\xi_1\beta_1' + \xi_2\beta_2'| \neq 0. & \end{cases}$$

Since, $A_Y = \sum\limits_{m<Y} a_m$, where (a_m) is a sequence of real numbers and $Y > 0$. Then $A_Y = O(\sqrt{Y}) = O(\sqrt{X})$. Hence

$$\lim_{X\to 0}\frac{wN(X,C)}{X} = N(J)\lim_{Y\to\infty}\frac{N_\Omega(\sqrt{Y})}{Y} = N(J)\iint\limits_{\Omega} d\xi_1 d\xi_2, \tag{7.6}$$

using Lemma 7.1. If $d > 0$, set $u_1 = \xi_1\beta_1 + \xi_2\beta_2$ and $u_2 = \xi_1\beta_1' + \xi_2\beta_2'$. Since, $|\beta_1\beta_2' - \beta_2\beta_1'| = N(J)\sqrt{d}$, we have

$$\iint\limits_{\Omega} d\xi_1 d\xi_2 = \frac{4}{N(J)\sqrt{d}} \iint\limits_{U^*} du_1 du_2,$$

where $U^* = \{(u_1, u_2)|0 < u_1u_2 < 1, 1 < \frac{u_1}{u_2} < \eta^2; u_1, u_2 > 0\}$.

Making change of variables, $v_1 = u_1u_2$ and $v_2 = \frac{u_1}{u_2}$, $\iint\limits_{\Omega} d\xi_1 d\xi_2 = \frac{4\log\eta}{N(J)\sqrt{d}}$. So that, along with (7.6), we get the theorem. If $d < 0$, set $u_1 = Re(\xi_1\beta_1 + \xi_2\beta_2)$ and $u_2 = Im(\xi_1\beta_1 + \xi_2\beta_2)$ and find that

$$\iint\limits_{\Omega} d\xi_1 d\xi_2 = \frac{2}{N(J)\sqrt{|d|}} \iint\limits_{u_1^2+u_2^2<1} du_1 du_2 = \frac{2\pi}{N(J)\sqrt{d}}.$$

This completes the proof. □

Let K be as above, a quadratic field with discriminant d and for $X > 0$, $N(X, K)$ the number of integral ideals I with $N(I) < X$. Since κ from the above theorem is independent of the ideal class C,

$$\lim_{X\to\infty} \frac{N(X, K)}{X} = h \cdot \kappa,$$

where h is the class number of K.

Hence by Wiener-Ikehara theorem, we get the following result.

Proposition 7.3. $\lim_{s\to 1^+}(s-1)\zeta_K(s) = h \cdot \kappa$, *where h is the class number of the quadratic field K and κ is the Dirichlet's structure constant, defined in the previous theorem.*

Now, using the fact that $(s - 1)\zeta(s) \to 1$ as $s \to 1^+$, and from the previous results in this chapter, we obtain Theorem 7.4, i.e.,

Let K be a quadratic field of discriminant d. Let h be the class number of K. Then we have

$$h = \begin{cases} \frac{\sqrt{d}}{2log\eta} L_d(1) & \text{if } d > 0 \\ \frac{w\sqrt{d}}{2\pi} L_d(1) & \text{if } d < 0. \end{cases}$$

Consider the equation $\zeta_K(s) = \zeta(s)L_d(s)$. Recall that $\zeta(s)$ has a simple pole at $s = 1$, with residue 1. Since $L_d(s)$ is the Dirichlet L-function of a non-trivial character, $L_d(s)$ has an analytic extension to the whole of complex plane. In addition, Theorem 7.4 implies that $L_d(1) > 0$.

Hence $\zeta_K(s)$ has a simple pole at $s = 1$ and has an meromorphic extension to the whole of complex plane with only a (simple) pole at $s = 1$.

This is also true for any number field, as shown by Hecke. We do not prove Hecke's result here.

Chapter 8

Analytic class number formula

In the previous chapter, we proved the Quadratic class number formula given by Dirichlet. In this chapter we will prove a more general result that has man other applications.

Recall that the Dedekind zeta function of a number field K is defined by

$$\zeta_K(s) := \sum_I \frac{1}{N(I)^s} = \prod_P \left(1 - \frac{1}{N(P)^s}\right)^{-1},$$

where I ranges over non-zero ideals of $\mathcal{O}_K$ and P ranges over nonzero prime ideals of $\mathcal{O}_K$, as we showed in the previous chapter the sum and product converge absolutely for $\Re(s) > 1$.

The following theorem is often attributed to Dirichlet, although he originally proved it only for quadratic fields. The formula for the limit in the theorem was proved by Dedekind, and analytic continuation was proved by Landau. In 1903, Landau proved that for every number field K, $\zeta_K(s)$ can be analytically continued to $Re(s) > 1 - \frac{1}{dim_{\mathbb{Q}}(K)}$.This was the first proof for general K that $\zeta_K(s)$ is meromorphic around $s = 1$. Hecke later showed that, like the Riemann zeta function, the Dedekind's zeta function has an analytic continuation to all of $\mathbb{C}$ and satisfies a functional equation, but we won't take the time to prove this here.

Theorem 8.1 (**Analytic class number formula**). *Let K be a number field of degree n. The Dedekind zeta function $\zeta_K(z)$ extends to a meromorphic function on $Re(z) > 1 - \frac{1}{n}$ that is holomorphic except for a simple pole at $z = 1$ with residue*

$$\lim_{z \to 1^+} (z-1)\zeta_K(z) = \frac{2^r (2\pi)^s h_K R_K}{w_K \sqrt{|d_K|}},$$

where r and s are the number of real and complex places of K, respectively, h_K is the class number of K, R_K is the regulator, w_K is the number of roots of unity in K, and d_K is the discriminant of K.

In practice the class number h_K is usually the most difficult quantity in the analytic class number formula to compute. We can approximate the limit in the LHS to any desired precision using a finite truncation of either the sum or product defining $\zeta_K(s)$. Provided we can compute the other quantities to similar precision this provides a method for computing (or at least bounding) the class number h_K.

8.1 Lipschitz parametrisability

In order to prove the analytic class number formula, we need an asymptotic estimate for the number of nonzero ideals of $\mathcal{O}_K$-ideals I with absolute norm $N(I)$ bounded by a parameter $t \in \mathbb{R}_{>0}$, that we will let go to infinity, this is necessary for us to understand the behaviour of $\zeta_K(z) = \sum\limits_{I} \frac{1}{N(I)^z}$ as $z \to 1^+$.

The idea is to count points in $\log(\mathcal{O}_K \cap K^*)$ that lie inside a suitably closed region S of $\mathbb{R}^{r+s}$ that we will scale by t. In order to bound this count as a function of t we need a condition on S that ensures that the count grows smoothly with t, this requires S to have a special shape. A sufficient condition for this is *Lipschitz parametrisability.*

Definition 8.1. *Let X and Y be metric spaces. A function $f : X \to Y$ is **Lipschitz continuous** if there exists $c > 0$ such that for all distinct $x_1, x_2 \in X$,*

$$d(f(x_1), f(x_2)) \leq c \cdot d(x_1, x_2).$$

Every Lipschitz continuous function is uniformly continuous, but the converse need not hold.

Definition 8.2. *A set B in a metric space X is **d-Lipschitz parametrisable** if it is the union of the images of a finite number of Lipschitz continuous functions $f_i : [0,1]^d \to B$.*

Now we will prove a few results to set the ground for the proof of the analytic class number formula.

Lemma 8.1. *Let $S \subset \mathbb{R}^n$ be a set whose boundary $\partial S := \bar{S} - S^0$ is $(n-1)$-Lipschitz parametrisable. Then*

$$\#(tS \cap \mathbb{Z}^n) = \mu(S)t^n + O(t^{n-1}),$$

as $t \to \infty$, where μ is the standard Lebesgue measure on $\mathbb{R}^n$.

Here and in what follows, for a finite set A, $\#A$ denotes the number of elements in A.

Proof. It suffices to prove the lemma for positive integers, since $\#(tS \cap \mathbb{Z}^n)$ and $\mu(S)t^n$ are both monotonically increasing functions of t and $\mu(S)(t+1)^n - \mu(S)t^n = O(t^{n-1})$.

We can partition $\mathbb{R}^n$ as the disjoint union of half-open cubes of the form

$$C(a_1, \ldots, a_n) = \{(x_1, \ldots, x_n) \in \mathbb{R}^n | x_i \in [a_i, a_i + 1)\},$$

with $a_1, \ldots, a_n \in \mathbb{Z}$. Let $\mathcal{C}$ be the set of all such half-open cubes C. For each $t > 0$, define

$$B_0(t) := \#\{C \in \mathcal{C} | C \subset tS\},$$
$$B_1(t) := \#\{C \in \mathcal{C} | C \cap tS \neq \phi\}.$$

It is easy to note that for every $t > 0$, we have

$$B_0(t) \leq \#(tS \cap \mathbb{Z}^n) \leq B_1(t).$$

We can bound $B_1(t) - B_0(t)$ by noting that each $C(a_1, \ldots, a_n)$ counted by this difference, contains a point $(a_1, \ldots, a_n) \in \mathbb{Z}^n$ within a distance $\sqrt{n} = O(1)$ of a point in $\partial tS = t\partial S$.

Let $f_1, \ldots, f_m$ be Lipschitz functions from $[0,1]^{n-1} \to \partial S$, whose images cover ∂S, and let $c_1, \ldots, c_m$ be constants such that $d(f_i(x_1), f_i(x_2)) \leq c_i d(x_1, x_2)$, for all $x_1, x_2 \in [0,1]^{n-1}$.

Now, for any $y \in \partial S$, we have $y = f_i(x_1, \ldots, x_{n-1})$ for some i, and if we put $r_j = [tx_j] \in \mathbb{Z}$, so that $0 \leq x_j - \frac{r_j}{t} \leq \frac{1}{t}$, then

$$d(y, f_i(\frac{r_1}{t}, \ldots, \frac{r_{n-1}}{t})) \leq c_i \cdot d((x_1, \ldots, x_{n-1}), (\frac{r_1}{t}, \ldots, \frac{r_{n-1}}{t})) < c_i \frac{\sqrt{n}}{t} \leq \frac{c}{t},$$

where $c := \sqrt{n} \max_i c_i$.

So, for every $y \in \partial S$, there lies a point within the distance of $\frac{c}{t}$, from the following set

$$\mathcal{P} = \left\{ f_i \left(\frac{r_1}{t}, \ldots, \frac{r_{n-1}}{t} \right) : 1 \leq i \leq m, 0 \leq r_1, \ldots, r_{n-1} \leq t \right\}.$$

This set $\mathcal{P}$ has cardinality $m(t+1)^{n-1} = O(t^{n-1})$. Hence we can say that every point of ∂tS is within a distance of c of one of the $O(t^{n-1})$ points in $t\mathcal{P}$.

The number of integer lattice points within a distance $\sqrt{n}$ of a point in ∂tS is therefore $O(t^{n-1})$ as well, and therefore,

$$B_1(t) - B_0(t) = O(t^{n-1}).$$

Also, note that $B_0(t) \leq \mu(tS) \leq B_1(t)$ and $\mu(tS) = t^n\mu(S)$. Hence the lemma follows. □

We recall the definition of a covolume of a lattice.

Definition 8.3. *Let Γ is a lattice in $\mathbb{R}^n$. Let $(v_1, \ldots, v_n)$ be an ordered basis of Γ. Let $v_i = (v_{i1}, \ldots, v_{in})$, for $1 \leq i \leq n$.*

The ***covolume*** *of L is the absolute value of the determinant of the matrix:*

$$\begin{pmatrix} v_{11} & v_{12} & \ldots & v_{1n} \\ v_{21} & v_{22} & \ldots & v_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ v_{n1} & v_{n2} & \ldots & v_{nn} \end{pmatrix}.$$

This definition is independent of the choice of the basis.

Corollary 8.1. *Let Γ be a lattice in an $\mathbb{R}$-vector space $V \cong \mathbb{R}^n$ and let $S \subset V$ be a set whose boundary is $(n-1)$-Lipschitz parametrisable. Then*

$$\#(tS \cap \Gamma) = \frac{\mu(S)}{covol(\Gamma)} t^n + O(t^{n-1}).$$

Proof. The case $\Gamma \subset \mathbb{Z}^n$ is given by the lemma.

We now note that if the corollary holds for $s\Gamma$, for some $s > 0$, then it also holds for Γ, since $tS \cap s\Gamma = (\frac{t}{s})S \cap \Gamma$.

For any lattice Γ, we can choose $s > 0$ so that $s\Gamma$ is arbitrarily close to an integer lattice (we can take s to be the LCM of all denominators appearing in rational approximations of the coordinates of a basis for Γ). The corollary then follows. □

Remark 8.1. *With the definition of covolume given above, we can say that, $covol(\Gamma) = V_{Leb}(\Phi) = \mu(\Phi)$, for any fundamental mesh Φ for Γ.*

So the ratio $\frac{\mu(S)}{covol(\Gamma)} = \frac{\mu(S)}{\mu(\Phi)}$ in the above corollary.

We now apply the above corollary to $\Gamma = \mathcal{O}_K$ and want to replace $covol(\mathcal{O}_K)$ with $\sqrt{d_K}$, which requires us to use the normalised Haar measure on $K_{\mathbb{R}}$ defined in Chapter 4.

8.2 Counting algebraic integers of bounded norm

From the discussions in Chapter 5, we can write $\mathcal{O}_K^* = \mu(K) \times U$, where $U \subset \mathcal{O}_K^*$ is free of rank $r + s - 1$, and $\mu(K)$ is the group of roots of unity in K. The subgroup U is not uniquely determined, but let us fix a choice.

We want to estimate the quantity

$$\#\{I : N(I) \leq t\},$$

where I ranges over the non-zero ideals of $\mathcal{O}_K$, as $t \to \infty$.

As a first step, let us restrict our attention to non-zero principal ideals $\langle\alpha\rangle \subset \mathcal{O}_K$. We then want to estimate the cardinality of $\{\langle\alpha\rangle : N(\langle\alpha\rangle) \leq t\}$. We have $\langle\alpha\rangle = \langle\alpha'\rangle$ if and only if $\frac{\alpha}{\alpha'} \in \mathcal{O}_K^*$. So, this is equivalent to

$$\{\alpha \in K^* \cap \mathcal{O}_K | N(\alpha) \leq t\}/\mathcal{O}_K^*.$$

Let $S \subset K_{\mathbb{R}}^*$. Denote by the notation $S/\mathcal{O}_K^*$ the set of equivalence classes of S under the equivalence relation $\alpha \sim \beta$ if and only if $\alpha = u\beta$ for some $u \in \mathcal{O}_K^*$.

If we now define,

$$K_{\mathbb{R},\leq t}^* \coloneqq \{x \in K_{\mathbb{R}}^* | N_K(x) \leq t\} \subset K_{\mathbb{R}}^* \subset K_{\mathbb{R}},$$

then we want to estimate the cardinality of the finite set

$$\left(K_{\mathbb{R},\leq t}^* \cap \mathcal{O}_K\right)/\mathcal{O}_K^*,$$

where the intersection takes place in $K_{\mathbb{R}}$ and produces a subset of $K_{\mathbb{R}}^*$, that we partition into equivalence classes modulo $\mathcal{O}_K^*$. Note that the finiteness of the set $\left(K_{\mathbb{R},\leq t}^* \cap \mathcal{O}_K\right)/\mathcal{O}_K^*$ follows form the finiteness of the integral ideals of bounded norm.

Simplify the matter by replacing $\mathcal{O}_K^*$ with the free group $U \subset \mathcal{O}_K*$, we then have a $w_K - to - 1$ map

$$\left(K_{\mathbb{R},\leq t}^* \cap \mathcal{O}_K\right)/U \to \left(K_{\mathbb{R},\leq t}^* \cap \mathcal{O}_K\right)/\mathcal{O}_K^*.$$

It suffices to estimate the cardinality of $\left(K_{\mathbb{R},\leq t}^* \cap \mathcal{O}_K\right)/U$ and divide the result by w_K.

Recall that for $x = (x_i) \in K_{\mathbb{R}}^*$, the norm map $N : K_{\mathbb{R}}^* \to \mathbb{R}_{>0}^*$ is defined by the product of the coordinates, i.e.,

$$N(x) \coloneqq \prod_{i=1}^{r} |x_i| \prod_{i=r+1}^{r+s} |x_i|^2,$$

and satisfies $Tr(Log(x)) = \log(N(x))$ for all $x \in K_{\mathbb{R}}^*$. We now define a surjective homomorphism $\nu : K_{\mathbb{R}}^* \to K_{\mathbb{R},1}^*$, such that $x \mapsto xN(x)^{-1/n}$.

The image of $K_{\mathbb{R},1}^*$ under the Log map is precisely the "trace zero hyperplane" H (as in Chapter 5) in $\mathbb{R}^{r+s}$. Here, $Log(U) = Log(\mathcal{O}_K^*) = \Gamma$ is a lattice in H. Let us fix a fundamental mesh Φ for the lattice Γ in H. So,

$$S := \nu^{-1}(Log^{-1}(\Phi))$$

is a set of unique coset representatives for the quotient $K_{\mathbb{R}}^*/U$. If we now define

$$S_{\leq t} := \{x \in S | N(x) \leq t\} \subset K_{\mathbb{R}},$$

we want to estimate the cardinality of the finite set

$$S_{\leq t} \cap \mathcal{O}_K.$$

The set $\mathcal{O}_K$ is a lattice in the $\mathbb{R}$-vector space $K_{\mathbb{R}}$ of dimension n. We have $tS_{\leq 1} = S_{\leq t^n}$, so we can estimate the cardinality of $S_{\leq t} = t^{\frac{1}{n}} S_{\leq 1}$ (because of Corollary 8.1 with $S = S_{\leq 1}$ and $\Gamma = \mathcal{O}_K$ by replacing t with $t^{\frac{1}{n}}$). The only thing remaining to prove is that the boundary of $S_{\leq 1}$ is $(n-1)$-Lipschitz parametrisable.

The kernel of the Log map is $\{\pm 1\}^r \times U(1)^s$, where $U(1) = \{z \in \mathbb{C} | z\bar{z} = 1\}$ is the unit circle in $\mathbb{C}$.

We thus have a continuous isomorphism of locally compact groups

$$K_{\mathbb{R}}^* = (\mathbb{R}^*)^r \times (\mathbb{C}^*)^s \xrightarrow{\sim} \mathbb{R}^{r+s} \times \{\pm 1\}^r \times [0, 2\pi)^s, \tag{8.1}$$

$$\begin{aligned} & x = (x_1, \ldots, x_r, z_1, \cdots, z_s) \\ & \mapsto (Log(x)) \times (sgn(x_1), \cdots, sgn(x_r)) \times (\arg(z_1), \cdots, \arg(z_s)) \end{aligned}$$

where the map to $\mathbb{R}^{r+s}$ is the Log map, the map to $\{\pm 1\}^r$ is the vector of signs of the r real components, and the map to $[0, 2\pi)^s$ is the vector of angles $\arg(z)$ such that $\frac{z}{|z|} = e^{i \arg z}$ of the s complex components.

The set $S_{\leq 1}$ consists of 2^r connected components, one for each element of $\{\pm 1\}$. We now parametrise each of the components using n real parameters as follows:

- $r + s - 1$ parameters in $[0, 1)$ that encode a point in Φ as an $\mathbb{R}$-linear combination of $Log(\epsilon_1), \ldots, Log(\epsilon_{r+s-1})$, where $\epsilon_1, \ldots, \epsilon_{r+s-1}$ are a basis of U;

- s parameters in $[0, 1)$ that encode an element of $U(1)^s$;
- a parameter in $(0, 1]$ that encodes the nth-root of the norm.

These parametrisations define a continuously differentiable bijection from the set

$$C = [0, 1)^{n-1} \times (0, 1] \subset [0, 1]^n$$

to each of the 2^r disjoint components of $S_{\leq 1}$. The boundary ∂C is the boundary of the unit n-cube, which is clearly $(n-1)$-Lipschitz parametrisable. Thus, each component of $S_{\leq 1}$, and therefore $S_{\leq 1}$ itself, is $(n-1)$-Lipschitz parametrisable.

Now applying Corollary 9.1 to the lattice $\mathcal{O}_K$ and the set $S_{\leq 1}$ in the $n-$dimensional $\mathbb{R}$-vector space $K_{\mathbb{R}}$ with t replaced by $t^{\frac{1}{n}}$, since $S_{\leq t} = t^{\frac{1}{n}} S_{\leq 1}$. This gives

$$\#(S_{\leq t} \cap \mathcal{O}_K) = \frac{\mu(S_{\leq 1}}{covol(\mathcal{O}_K)} (t^{\frac{1}{n}})^n + O((t^{\frac{1}{n}})^{n-1}) = \left(\frac{\mu(S_{\leq 1}}{\sqrt{|d_K|}} \right) t + O(t^{1-\frac{1}{n}}). \tag{8.2}$$

Next we need to compute $\mu(S_{\leq 1})$ and we will use the normalised Haar measure μ on $K_{\mathbb{R}}$. We will use the isomorphism in (8.1) to make a change of coordinates and understand how this affects the Haar measure μ on $K_{\mathbb{R}} \cong \mathbb{R}^r \times \mathbb{C}^s$.

In terms of the standard Lebesgue measures dx and dA on $\mathbb{R}$ and $\mathbb{C}$, we have $\mu = (dx)^r (2dA)^s$, where the $2dA$ comes from the fact that the normalised absolute value for each complex place is the square of the Euclidean absolute value on $\mathbb{C}$.

For each factor of $K_{\mathbb{R}}^* \cong (\mathbb{R}^*)^r \times (\mathbb{C})^s \subset \mathbb{R}^r \times \mathbb{C}^s$, we define the following maps:

$$\begin{aligned} \mathbb{R}^* &\to \mathbb{R} \times \{\pm 1\} \\ x &\mapsto (\log |x|, sgn(x)) \\ \pm e^l &\leftarrow\!\shortmid (l, \pm 1) \\ dx &\mapsto e^l dl \ \mu_{\{\pm 1\}}, \end{aligned}$$

and

$$\begin{aligned} \mathbb{C}^* &\to \mathbb{C} \times [0, 2\pi) \\ z &\mapsto (2 \log |z|, \arg z) \\ e^{l/2 + i\theta} &\leftarrow\!\shortmid (l, \theta) \\ 2dA &\mapsto 2e^{l/2} d(e^{l/2}) d\theta = e^l dl \ d\theta, \end{aligned}$$

where dl is the Lebesgue measure on $\mathbb{R}$ $\mu_{\{\pm 1\}}$ is the counting measure on $\{\pm 1\}$, and $d\theta$ is the Lebesgue measure on $[0, 2\pi)$. We thus have

$$K_{\mathbb{R}}^{*} \xrightarrow{\sim} \mathbb{R}^{r+s} \times \{\pm 1\}^{r} \times [0, 2\pi)^{s}$$

$$\mu \longmapsto e^{T(.)}\ \mu_{\mathbb{R}^{r+s}}\ \mu_{\{\pm 1\}}^{r}\ \mu_{[0,2\pi)}^{s},$$

where the trace function $T(.)$ sums the coordinates of a vector in $\mathbb{R}^{r+s}$.

We now make one more change of coordinates:

$$\begin{aligned} \mathbb{R}^{r+s} &\to \mathbb{R}^{r+s-1} \times \mathbb{R} \\ x = (x_1, \ldots, x_{r+s}) &\mapsto (x_1, \ldots, x_{r+s-1}, y := T(x)) \\ e^{T(x)} \mu_{\mathbb{R}^{r+s}} &\mapsto e^{y} \mu_{\mathbb{R}^{r+s-1}} dy. \end{aligned}$$

If we let $\pi : \mathbb{R}^{r+s} \to \mathbb{R}^{r+s-1}$ denote the coordinate projection, then the measure of $\pi(\Phi)$ is $\mathbb{R}^{r+s-1}$ is, by definition, the regulator R_K.

The *Log* map gives us a bijection

$$S_{\leq 1} \xrightarrow{\sim} \Phi + (-\infty, 0] \left(\frac{1}{n}, \ldots, \frac{1}{n}, \frac{2}{n}, \ldots, \frac{2}{n} \right),$$

$$x = N(x)^{1/n} \nu(x) \longmapsto Log(\nu(x)) + \log N(x) \left(\frac{1}{n}, \ldots, \frac{1}{n}, \frac{2}{n}, \ldots, \frac{2}{n} \right).$$

The coordinate $y \in (-\infty, 0]$ is given by $y = T(\log x) = \log N(x)$. So, we can now view $S_{\leq 1}$ as an infinite union of cosets of $Log^{-1}(\Phi)$ parametrised by $e^{y} = N(x) \in (0, 1]$.

Under our change of coordinates, we have

$$K_{\mathbb{R}}^{*} \xrightarrow{\sim} \mathbb{R}^{r+s-1} \times \mathbb{R} \times \{\pm 1\}^{r} \times [0, 2\pi)^{s}$$

$$S_{\leq 1} \to \pi(\Phi) \times (-\infty, 0] \times \{\pm 1\}^{r} \times [0, 2\pi)^{s}.$$

Since $R_K = \mu_{\mathbb{R}^{r+s-1}}(\pi(\Phi))$, we have

$$\mu(S_{\leq 1}) = \int\limits_{-\infty}^{0} e^{y} R_K 2^{r} (2\pi)^{s} dy = 2^{r} (2\pi)^{s} R_K.$$

Putting this into equation 8.2, we get

$$\#(S_{\leq 1} \cap \mathcal{O}_K) = \left(\frac{2^{r} (2\pi)^{s} R_K}{\sqrt{|d_K|}} \right) t + O(t^{1-\frac{1}{n}}). \tag{8.3}$$

8.3 Proof of analytic class number formula

We now have the necessary results to prove the analytic class number formula. The main tool is the following theorem, which uses our discussion from the previous section to give a precise asymptotic estimate on the number of ideals of bounded norm.

Theorem 8.2. *Let K be a number field of degree n. As $t \to \infty$, the number of non-zero integral ideals I of norm $N(I) \leq t$ is,*

$$\left(\frac{2^r(2\pi)^s h_K R_K}{w_K\sqrt{d_K}}\right) t + O\left(t^{1-\frac{1}{n}}\right),$$

where r, s are the number of real and complex conjugates of K, respectively; h_K is the class number of K; R_K is the regulator; w_K is the number of roots of unity in K; and d_K is the discriminant of K.

Proof. In order to count the non-zero integral ideals I with norm $N(I) \leq t$, we group them by ideal class.

For the trivial class, we just need to count non-zero principal ideals $\langle\alpha\rangle$, equivalently, the number of non-zero $\alpha \in \mathcal{O}_K$ with $N(\alpha) \leq t$, modulo the unit group $\mathcal{O}_K^*$. Dividing equation 8.3 by w_K to account for $w_K - to - 1$ map

$$S_{\leq t} \cap \mathcal{O}_K \to (K_{\mathbb{R},\leq t}^* \cap \mathcal{O}_K)/\mathcal{O}_K^*,$$

we obtain

$$\#\{\langle\alpha\rangle \subset \mathcal{O}_K | N(\alpha) \leq t\} = \left(\frac{2^r(2\pi)^s R_K}{w_K\sqrt{|d_K|}}\right) t + O\left(t^{1-\frac{1}{n}}\right). \tag{8.4}$$

To complete the proof, we now show that we get the same answer for every ideal class. Fix an ideal class $[I]$, with I a non-zero integral ideal. Multiplication by I gives a bijection

$$\begin{aligned}&\{\text{ideals } J \in [I^{-1}] | N(J) \leq t\}\\ &\xrightarrow{\times I} \{\text{non-zero principal ideals } \langle\alpha\rangle \subset I | N(\alpha) \leq tN(I)\}\\ &\to \{\text{non-zero } \alpha \in I | N(\alpha) \leq tN(I)\}/\mathcal{O}_K^*.\end{aligned}$$

Let $S_{[I],\leq t}$ denote the set on the RHS. The estimate in (8.4) derived from Corollary 8.1 applies to any lattice in $K_{\mathbb{R}}$, not just $\mathcal{O}_K$. Replacing $\mathcal{O}_K$ with I in (8.4), we get

$$\#S_{[I],\leq t} = \left(\frac{2r(2\pi)^s R_K}{w_K \mathcal{D}(I)}\right) tN(I) + O\left(t^{1-\frac{1}{n}}\right)$$

$$= \left(\frac{2r(2\pi)^s R_K}{w_K \sqrt{|d_K|} N(I)} \right) tN(I) + O\left(t^{1-\frac{1}{n}}\right) = \left(\frac{2r(2\pi)^s R_K}{w_K \sqrt{|d_K|}} \right) t + O\left(t^{1-\frac{1}{n}}\right).$$

Note that the RHS does not depend upon the ideal class $[I]$. Summing over ideal classes yields,

$$\#\{\text{non-zero integral ideals } J|N(J) \leq t\}$$
$$= \sum_{[I] \in \mathcal{H}_K} \#S_{[I], \leq t} = \left(\frac{2^r (2\pi)^s h_K R_K}{w_K \sqrt{|d_K|}} \right) t + O\left(t^{1-\frac{1}{n}}\right),$$

as claimed. □

Lemma 8.2. *Let $a_1, a_2, \dots$ be a sequence of complex numbers and let σ be a real number. Suppose that*

$$a_1 + \cdots + a_t = O(t^\sigma) \text{ (as } t \to \infty\text{)}.$$

Then the Dirichlet series $\sum a_n n^{-s}$ defines a holomorphic function on $\Re(s) > \sigma$.

Proof. Let $A(x) := \sum\limits_{0<n\leq x} a_n$. Writing the Dirichlet sum as a Riemann-Stieltjes integral, for $\Re(s) > \sigma$, we have

$$\sum_{n=1}^{\infty} \frac{a_n}{n^s} = \int_{1^-}^{\infty} \frac{dA(x)}{x^s}$$

$$= \frac{A(x)}{x^s}\bigg|_{1^-}^{\infty} - \int_{1^-}^{\infty} A(x) d(x^{-s})$$

$$= (0-0) - \int_{1^-}^{\infty} A(x) \left(\frac{-s}{x^{s+1}}\right) dx$$

$$= s \int_{1^-}^{\infty} \frac{A(x)}{x^{s+1}} dx.$$

To conclude that $\lim_{x\to\infty} \frac{A(x)}{x^s} = 0$, we use $|A(x)| = O(x^\sigma)$ and that $\Re(s) > \sigma$.

The integral on the RHS converges uniformly on $\Re(s) > \sigma$ and the lemma follows. □

Remark 8.2. *The above lemma gives us an abscissa of convergence σ for the Dirichlet series $\sum \frac{a_n}{n^s}$. This analogous to the radius of convergence of a power series.*

Lemma 8.3. *Let $a_1, a_2, \ldots$ be a sequence of complex numbers that satisfies*

$$a_1 + \cdots + a_t = \rho t + O(t^\sigma) \ (\text{as } t \to \infty)$$

for some $\sigma \in [0,1)$ and $\rho \in \mathbb{C}^*$. The Dirichlet series $\sum a_n n^{-s}$ converges on $\Re(s) > 1$ and has a meromorphic continuation to $\Re(s) > \sigma$ that is holomorphic except for a simple pole at $s = 1$ with a residue ρ.

Proof. Define $b_n := a_n - \rho$. Then $b_1 + \cdots + b_t = O(t^\sigma)$ and

$$\sum a_n n^{-s} = \rho \sum n^{-s} + \sum b_n n^{-s} = \rho\zeta(s) + \sum b_n n^{-s}.$$

We know that the Riemann zeta function $\zeta(s)$ is holomorphic on $Re(s) > 1$ and has a meromorphic continuation to $Re(S) > 0$ that is holomorphic except for a simple pole at $s = 1$ with residue 1.

By the previous lemma, $\sum b_n n^{-s}$ is holomorphic on $Re(s) > \sigma$, and since $\sigma < 1$, it is holomorphic at $s = 1$. So the entire RHS has a meromorphic continuation to $Re(s) > \sigma$ that is holomorphic except for the simple pole at $s = 1$ coming from $\zeta(s)$, and the residue at $s = 1$ is $\rho \cdot 1 + 0 = \rho$. □

We can now proceed to prove the analytic class number formula.

Theorem 8.3 (Analytic class number formula). *Let K be a number field of degree n. The Dedekind zeta function $\zeta_K(z)$ extends to a meromorphic function on $Re(z) > 1 - \frac{1}{n}$ that is holomorphic except for a simple pole at $z = 1$ with residue*

$$\lim_{z \to 1^+} (z-1)\zeta_K(z) = \rho_K := \frac{2^r (2\pi)^s h_K R_K}{w_K \sqrt{|d_K|}},$$

where r and s are the number of real and complex places of K, respectively, h_K is the class number of K, R_K is the regulator, w_K is the number of roots of unity in K, and d_K is the discriminant of K.

Proof. We have

$$\zeta_K(z) = \sum_I \frac{1}{N(I)^z} = \sum_{t \geq 1} \frac{a_t}{t^z},$$

where I ranges over non-zero integral ideals, and $a_t := \#\{I | N(I) = t\}$ with $t \in \mathbb{Z}_{\geq 1}$. If we now define

$$\rho_K := \frac{2^r (2\pi)^s h_K R_K}{w_K \sqrt{|d_K|}},$$

then by Theorem 8.2 we have,

$$a_1 + \cdots + a_t = \#\{I | N(I) \leq t\} = \rho_K t + O\left(t^{1-\frac{1}{n}}\right) \text{ (as } t \to \infty).$$

Applying the previous lemma with $\sigma = 1 - \frac{1}{n}$, we see that $\zeta_K(z) = \sum a_t t^{-z}$ extends to a meromorphic function on $Re(z) > 1 - \frac{1}{n}$ that is holomorphic except for a simple pole at $z = 1$, with residue ρ_K. □

Remark 8.3. *As noted before, Hecke proved that $\zeta_K(z)$ extends to a meromorphic function on $\mathbb{C}$ with no poles other than the simple pole at $z = 1$ and it satisfies a functional equation. If we define the gamma factors*

$$\Gamma_{\mathbb{R}}(z) := \pi^{-z/2}\Gamma(\frac{z}{2}), \text{ and } \Gamma_{\mathbb{C}}(z) := (2\pi)^{-z}\Gamma(z),$$

and the completed zeta function

$$\xi_K(z) := |d_K|^{z/2}\Gamma_{\mathbb{R}}(z)^r\ \Gamma_{\mathbb{C}}(z)^s\ \zeta_K(z)$$

where r, s are the number of real and complex places of K respectively; then $\xi_K(z)$ is holomorphic except for simple poles at $z = 0, 1$ and satisfies the functional equation

$$\xi_K(z) = \xi_K(1 - z).$$

In the case $K = \mathbb{Q}$, we have $r = 1$ and $s = 0$, so

$$\xi_{\mathbb{Q}}(z) = \Gamma_{\mathbb{R}}(z)\zeta(z) = \pi^{z/2}\Gamma(\frac{z}{2})\zeta_{\mathbb{Q}}(z),$$

which is the completed zeta function for the Riemann zeta function $\zeta(z) = \zeta_{\mathbb{Q}}(z)$.

Bibliography

[1] *Mathematical Pamphlets*, School of Mathematics, Tata Institute of Fundamental Research, Mumbai, India.

[2] *Algebraic Theory of Numbers* by Pierre Samuel.

[3] *Algebraic Number Theory* by Jurgen Neukirch.

[4] Lecture Notes from the course *Number Theory I (18.785)* by Andrew Sutherland, Massachusetts Institute of Technology, USA.