Number Fields

Gaurish Korpal[1]
gaurish.korpal@niser.ac.in

Summer Internship Project Report

[1] 2^{nd} year Int. MSc. Student, National Institute of Science Education and Research, Jatni (Bhubaneswar, Odisha)

Certificate

Certified that the summer internship project report "Number Fields" is the bona fide work of "Gaurish Korpal", 2^{nd} Year Int. MSc. student at National Institute of Science Education and Research, Jatni (Bhubaneswar, Odisha), carried out under my supervision during June 1, 2016 to July 31, 2016.

Place: Bangalore
Date: July 31, 2016

Prof. Ramesh Sreekantan
Supervisor
Associate Professor,
Statistics and Mathematics Unit,
Indian Statistical Institute,
Bangalore 560059, Karnataka

Abstract

Algebraic number theory is essentially the study of number fields which are finite extensions of the field $\mathbb{Q}$ of rational numbers. A large portion of classical algebraic number theory involves investigating following questions about subrings of arbitrary number fields: What are the units in this ring? What are the irreducible elements? Do the elements factor uniquely? If not, what can we say about the factorization of ideals into prime ideals? How many ideal classes are there? And this report addresses some of these questions.

Acknowledgements

Foremost, I would like to express my sincere gratitude to my advisor *Prof. Ramesh Sreekantan* for his patience, motivation, enthusiasm, and immense knowledge. I am also thankful to my fellow intern *Arnab Char* (3rd year BS-MS, IISER-Kolkata) and *Math.StackExchange community* for the enlightening discussions.
Last but not the least, I would like to thank

- Steven Sivek, William Stein, John Cremona, Radoslav Kirov & Alyson Deines for Number Field Ideals function for SageMath
- Donald Knuth for TeX
- Michael Spivak for $\mathcal{AMS}$-TeX
- Sebastian Rahtz for TeX Live
- Leslie Lamport for LaTeX
- American Mathematical Society for $\mathcal{AMS}$-LaTeX
- Hàn Thế Thành for pdfTeX
    - Christian Feuersänger & Till Tantau for PGF/Ti*k*Z interpreter
    - Heiko Oberdiek for hyperref package
    - Steven B. Segletes for stackengine package
    - Michael Shell for ieeetrantools package
    - Alan Jeffrey & Frank Mittelbach for inputenc package
    - David Carlisle for graphicx package
    - Javier Bezos for enumitem package
    - Hideo Umeki for geometry package
    - Axel Sommerfeldt for subcaption package
    - Philipp Lehman & Joseph Wright for csquotes package
- Philipp Kühl & Daniel Kirsch for Detexify (a tool for searching LaTeX symbols)
- TeX.StackExchange community for helping me out with LaTeX related problems

Contents

Introduction

Let α be an algebraic number over a field F, then the polynomials over F having α as a root form a prime ideal[1] $\mathfrak{p}$ in ring[2] $F[x]$. Since $F[x]$ is a principal ideal domain (PID), $\mathfrak{p}$ is in fact a maximal ideal[3]. The ring $F[\alpha]$ is isomorphic to the factor ring $F[x]/\mathfrak{p}$. Since $\mathfrak{p}$ is maximal ideal we conclude that $F[\alpha]$ is a field whenever α is algebraic over F. Similarly, we can prove that for any finite number of algebraic numbers $\alpha_1, \ldots, \alpha_m$, $K = F[\alpha_1, \ldots, \alpha_m]$ is a field extension of F. Such finite degree field extension of the field of rational numbers $\mathbb{Q}$ is referred to as *number field*. Hence, in general, finite extension of given number field K will lead to another number field L. Since we will be studying field extensions, we should have understanding of the Galois group of L/K, whenever L is a normal extension of K[4]. For a nice overview of the algebra needed to study *number fields* refer pp. 36–39 of [3].

In my first summer project report[21] we saw the usage of property of unique factorization for ring of integers of the quadratic number field to solve Diophantine equations. But I presented the proofs for initial cases of Fermat's Last Theorem (for $n = 3, 4$) using elementary method of infinite descent (by Euler and Fermat) instead of algebraic ones. Now in chapter 1 we will discuss the method which was one of the main sources of the modern discipline of commutative algebra[19], to solve a case of Fermat's Last Theorem.

A *number field* K can be viewed as a subfield of $\mathbb{C}$ which is a finite dimensional vector space over $\mathbb{Q}$. Moreover, we can write every number field $K = \mathbb{Q}[\alpha]$ for some chosen α with the degree of the algebraic number α being equal to the dimension of K over $\mathbb{Q}$. Hence a number field always has power basis over $\mathbb{Q}$. On the contrary, the ring of integers of every number field need not be of form $\mathbb{Z}[\alpha]$, which we shall discuss in chapter 2.

We know that the rings of algebraic integers do not always have unique factorization property. But since every ring of algebraic integers happens to be a Dedekind domain, every proper ideal admits a unique factorization as a product of prime ideals. We shall exploit this fact in chapter 3.

In chapter 4 we shall try to address the question: "How much ideals in a Dedekind domain behave like elements?". One part of the answer is given by the ideal class group (section 1.2) since its size is a measure for the deviation of a ring of integers from being a unique factorization domain (UFD)[5]. The other part of the answer is provided by the multiplicative group of units of the Dedekind domain, since passage from principal ideals to their generators requires the use of units. Also in my recent winter project report[22] we saw that Roth's theorem can be applied to a large variety of Diophantine equations to show that they have only finitely many solutions. In certain special cases, however, it is possible to make more precise statements about the number and nature of possible solution[5]. Hence, towards the end of this chapter we shall concern ourselves with the equation $x^3 + dy^3 = 1$ and calculate its exact number of solutions using group of units.

[1] By a prime ideal we will always mean a non-zero prime ideal

[2] By a ring we will always mean a commutative ring with unity (multiplicative identity).

[3] In a PID, every non-zero prime ideal is maximal.

[4] Number fields are of characteristic zero. In characteristic zero and finite fields every extension is separable. Hence, if a number field is normal then it is Galois.

[5] A Dedekind domain is a UFD iff it is a PID. A ring of integers is a PID iff it has a trivial ideal class group.

Chapter 1

First Case of Fermat's Last Theorem

Fermat's Last Theorem (FLT) states that no n^{th} power can be the sum of two other n^{th} powers, where $n > 2$. It is easy to show that if the theorem is true when n equals some integer r, then it is true when n equals any multiple of r. Since every integer greater than 2 is divisible by 4 or an odd prime, it is sufficient to prove the theorem for $n = 4$ and every odd prime.

In 1770, Leonhard Euler formulated an ingenious algebraic proof (apart from his elementary proof in 1760) for $n = 3$, but it had a serious flaw. Euler assumed that $\mathbb{Z}[\sqrt{-3}]$ was characterized by unique factorization, which is wrong. The flaw was easily corrected since the quadratic ring of integers $\mathbb{Z}[\frac{-1+\sqrt{-3}}{2}]$ is characterized by unique factorization. For application of this algebraic method to solve some more specific exponent cases refer [16].

In 1823, Marie-Sophie Germain proved FLT (using elementary methods) for all prime exponents $2 < p < 100$ by giving a prime q for which following theorem applies.

Theorem (Germain, 1823[1])**.** *Let p, q be distinct odd primes, and assume the following two conditions:*

1. $p \not\equiv a^p \pmod q$ *for any* $a \in \mathbb{Z}$

2. $x^p + y^p + z^p \equiv 0 \pmod q$ *has no set of integral solution, each not divisible by* q

Then FLT holds for p such that $p \nmid xyz$.

For example, if $p = 7$, $q = 29$, then both the conditions of the Germain's theorem are satisfied[12] and hence FLT is proved for $p = 7$. For proof of this theorem refer to Paulo Ribenboim's book[2].

1.1 The Two Cases

As a corollary of the above theorem by Germain, we get:

Corollary 1 (Germain, 1823)**.** *For a prime p if $2p + 1$ is also prime and $p \nmid xyz$, then there is no integer solution of $x^p + y^p = z^p$.*

[1] Since women were not allowed in French Academy of Sciences, Adrien-Marie Legendre communicated the results and credited Germain for them.

[2] *13 Lectures on Fermat's Last Theorem.* New York: Springer-Verlag, 1979. pp. 55. http://dx.doi.org/10.1007/978-1-4684-9342-9 (or) *Fermat's Last Theorem for Amateurs.* New York: Springer-Verlag, 1999. pp. 109. http://dx.doi.org/10.1007/b97437

So, if she could prove that there are infinitely many such primes p, now called *Sophie Germain primes*, then she would have been able to prove FLT for infinite number of prime exponents. But, we still don't know that whether there are finite or infinite number of Sophie Germain primes. Based on this result, the statement of FLT is generally subdivided into two cases, with Germain's condition being the first case:

1. For the prime exponent p when there do not exist integers x, y, z such that $p \not| xyz$ and $x^p + y^p = z^p$.

2. For the prime exponent p when there do not exist integers x, y, z all different from zero, such that $p|xyz$, $\gcd(x, y, z) = 1$ and $x^p + y^p = z^p$.

1.2 Kummer's Theory

A naive approach to solve (at least) first case of FLT would be to generalize Euler's approach. Firstly we factorize right hand side of general equation

$$x^p + y^p = (x + y)(x + \zeta y) \cdots (x + \zeta^{p-1} y) = z^p$$

where $\zeta = e^{\frac{2\pi i}{p}}$ is the p^{th} root of unity. Then we assume that the unique factorization property holds for

$$\mathbb{Z}[\zeta] = \left\{ \sum_{i=0}^{p-2} a_i \zeta^i : a_i \in \mathbb{Z} \quad \text{for} \quad 0 \leq i \leq p-2 \right\}$$

But even when this kind of argument is successfully executed (see pp. 4, [1]), we will be able to prove FLT only for finitely many prime exponents, since now it is known that only for $p = 3, 5, 7, 11, 13, 17$ and 19, $\mathbb{Z}[\zeta]$ has unique factorization property[3].

Ernst Kummer had been working on theory of *cyclotomic integers*, the ring of integers $\mathbb{Z}[\zeta_n]$ where ζ_n is complex n^{th} root of unity, for long time. It was known that the unique factorization property doesn't always exist in $\mathbb{Z}[\zeta_n]$, for example if $n = 23$. To restore this unique factorization property, Kummer introduced *ideal prime factors* into the arithmetic of cyclotomic integers, somewhat analogous to introduction of $i = \sqrt{-1}$ into the arithmetic of ordinary integers by Carl Friedrich Gauss. Influenced by Carl Jacobi's work on cyclotomic functions[7], Kummer's theory of ideal factorization came into existence and is considered to be one of the major achievements of 19^{th} century mathematics[12][15]. But today, Kummer's ideal prime numbers and certain classes of numbers that are related to them (to which he devoted twenty of his best years) are called *ideals*. His aim was to find the solution of the problem of the higher reciprocity laws posed by Gauss. Since FLT is closely related to the problem of higher reciprocity laws[4], Kummer was able to prove the FLT for every odd prime integer n between 1 to 100 except 37, 59 and 67 using his concept of *ideal factorization*.

Definition 1 (Ideal Class)**.** Given two ideals $\mathfrak{a}$ and $\mathfrak{b}$ of a ring of integers, $\mathfrak{a} \sim \mathfrak{b}$ if and only if $\alpha\mathfrak{a} = \beta\mathfrak{b}$ for some α, β in the ring of integers in the number field. This equivalence relation $\sim$ on the set of ideals leads to equivalence classes, called ideal classes.

Definition 2 (Class Number)**.** The class number h of a ring of integers in a number field is the order of the group formed by ideal classes.

[3] Masley, J. H. and Montgomery, H. L. "Cyclotomic fields with unique factorization." *Journal für die reine und angewandte Mathematik (Crelle's Journal)* 1976, no. 286-287 (Jan 1976): 248–256. http://dx.doi.org/10.1515/crll.1976.286-287.248

[4] Although Gauss himself always denied that he was interested in FLT per se, but expressed the hope that from his results concerning higher reciprocity laws he would be able to deduce FLT easily.

Definition 3 (Regular Primes)**.** A prime integer p is called regular if and only if it doesn't divide the class number h of the ring $\mathbb{Z}[\zeta_n]$.

1.3 The Proof

Since $\mathbb{Z}[\zeta]$ is the ring of integers in the number field $\mathbb{Q}[\zeta]$ (proved in Theorem 7) and the ring of integers is a Dedekind domain (introduced in chapter 3), we conclude that $\mathbb{Z}[\zeta]$ has unique factorization property in ideals.

Theorem 1 (Kummer, 1847)**.** *Let p be a regular prime, then there do not exist rational integers x, y, z such that $x^p + y^p = z^p$ if $p \nmid xyz$.*

Proof. Suppose $x^p + y^p = z^p$, with x, y and z relatively prime integers (without loss of generality) and with p not dividing xyz. We have ideal factorization

$$\langle x + y\rangle\langle x + y\zeta\rangle \cdots \langle x + y\zeta^{p-1}\rangle = \langle z\rangle^p$$

in which all factors are interpreted as principal ideals and $\zeta = e^{\frac{2\pi i}{p}}$.

Claim 1 p can't be equal to 3

If our assumption is true for $p = 3$, then there exist x, y, z such that $x^3 + y^3 = z^3$ and $3 \nmid xyz$. Then these x, y, z must also satisfy $x^3 + y^3 - z^3 \equiv 0 \pmod 9$ (see pp. 3 of [21]). We chose to reduce modulo 9 because if $a^3 \equiv b \pmod 9$ then $b = 0, \pm 1$. Using this fact in all 27 possible cases, we conclude that $x^3 + y^3 - z^3 \equiv \pmod 9$ iff $3|xyz$ since at least one of x, y, z must be a multiple of 9. Contradicting our assumption that $3 \nmid xyz$ and hence proving our claim.

Claim 2 $x \not\equiv y \pmod p$

If $x \equiv y \equiv -z \pmod p$, then $-2z^p \equiv z^p \pmod p$ which is a contradiction since $p > 3$ by Claim 1. Hence, we get $x \not\equiv y \pmod p$.

Claim 3 Ideals $\langle x + \zeta^i y\rangle$ are relatively prime

On the contrary, assume that they have a common prime ideal $\mathfrak{p}$ dividing two of them. By eliminating x, we see that $\mathfrak{p}$ divides $\langle 1 - \zeta\rangle$ or $\langle y\rangle$, whereas eliminating y, we see that $\mathfrak{p}$ divides $\langle 1 - \zeta\rangle$ or $\langle x\rangle$. Let $\lambda = 1 - \zeta$, then $\mathfrak{p} = \langle\lambda\rangle$. Thus

$$\begin{aligned} x + y \equiv x + \zeta^i y \equiv 0 \pmod{\lambda} \\ \Rightarrow z^p \equiv x + y \equiv 0 \pmod{\lambda} \end{aligned}$$

leading to the contradiction that p divides z since by setting $t = 1$ in $1 + t + \ldots + t^{p-1} = \prod_{j=1}^{p-1}(t - \zeta^j)$ we get

$$p = (1 - \zeta)(1 - \zeta^2) \cdots (1 - \zeta^{p-1}) = \lambda(1 - \zeta^2) \cdots (1 - \zeta^{p-1})$$

in which all factors are interpreted as algebraic numbers.

Claim 4 $x + \zeta^i y = \epsilon_i \alpha_i^p$, for some unit ϵ_i and some element α_i of $\mathbb{Z}[\zeta]$

By unique factorization of ideals and Claim 3, each factor is a p^{th} power of some ideal $\mathfrak{a}$. Hence

$$\langle x + \zeta^i y\rangle = \mathfrak{a}^p$$

Now since ideal classes form a finite abelian group (discussed in chapter 4), if p is regular (i.e. doesn't divide order of the group formed by ideal classes) then clearly this group contains no element of order p. It follows that if an ideal $\mathfrak{a}^p$ is principal then so is $\mathfrak{a}$ (pp. 5, [1]). Therefore, $\mathfrak{a} = \langle \alpha_i \rangle$ for some $\alpha_i \in \mathbb{Z}[\zeta]$ and

$$x + \zeta^i y = \epsilon_i \alpha_i^p$$

where ϵ_i is some unit element of $\mathbb{Z}[\zeta]$.

Claim 5 Any unit[5] ε of $\mathbb{Z}[\zeta]$ is a power of ζ times a real unit.

Let $f \in \mathbb{Q}[x]$ be a monic polynomial. Suppose all the roots of f have absolute value 1. Then the sum of the roots taking them r at a time is bounded by $\binom{n}{r}$ by the triangle inequality. Thus the coefficient of x^r is bounded by this $\binom{n}{r}$, hence for any fixed n there are only finitely many algebraic integers α such that all conjugates have absolute value 1 because there are only finitely many polynomials in $\mathbb{Z}[x]$ with given bounded coefficients.

Then consider the powers of an algebraic integer α in ring of integers $\mathcal{O}$. They are all algebraic integers of degree at most n, and furthermore all their conjugates also have absolute value 1 since the Galois actions map powers of α to powers of its conjugates. Thus the powers of α are restricted to a finite set. This means α is a root of unity[6] in $\mathcal{O}$.

Let $\overline{\varepsilon}$ be the complex conjugate of ε. Now consider the conjugates of $\varepsilon/\overline{\varepsilon}$, that is $\varepsilon'/\overline{\varepsilon'}$ for all conjugates ε' of ε. Since complex conjugation is one of the Galois actions they are all algebraic integers with absolute value 1, thus $\varepsilon/\overline{\varepsilon}$ is a root of unity[7] in $\mathbb{Z}[\zeta]$. Hence $\varepsilon/\overline{\varepsilon} = \pm\zeta^k$ where $0 \leq k \leq p-1$.

Suppose $\varepsilon/\overline{\varepsilon} = -\zeta^k$. Then $\varepsilon^p = -\overline{\varepsilon}^p$. But $\varepsilon^p \equiv \overline{\varepsilon}^p \pmod{p}$. Thus $2\varepsilon^p \equiv 0 \pmod{p}$, so p divides ε which contradicts the fact that ε is a unit. Hence only plus sign holds and $\varepsilon = \overline{\varepsilon}\zeta^k$.

Now since $p > 3$, we can choose $r \in \mathbb{Z}$ such that $k \equiv 2r \pmod{p}$. Then we have $\zeta^{-r}\varepsilon = \zeta^r\overline{\varepsilon} = \overline{\zeta^{-r}\varepsilon}$ so $\zeta^{-r}\varepsilon$ is invariant under complex conjugation and is thus real. Hence, $\varepsilon = \overline{\varepsilon}\zeta^{2r} = (\zeta^{-r}\varepsilon)\zeta^r = u\zeta^r$ where u is a real unit of $\mathbb{Z}[\zeta]$.

From Claim 4 and Claim 5 we can conclude that

$$x + \zeta y = u\zeta^r\alpha^p$$

where $\alpha = a_0 + a_1\zeta + \ldots + a_{p-2}\zeta^{p-2}$ and $a_i \in \mathbb{Z}$. Then we observe that

$$\alpha^p \equiv a_0^p + a_1^p + \ldots + a_{p-2}^p \equiv a \pmod{p}$$

for some $a \in \mathbb{Z}$. Hence

$$x + \zeta y \equiv ua\zeta^r \pmod{p}$$

Since $\overline{\zeta} = \zeta^{-1}$, on complex conjugation we get

$$x + \zeta^{-1} y \equiv ua\zeta^{-r} \pmod{p}$$

Therefore,

$$\zeta^{-r}(x + \zeta y) \equiv \zeta^r(x + \zeta^{-1} y) \pmod{p}$$
$$\Rightarrow x + \zeta y - \zeta^{2r}x - \zeta^{2r-1}y \equiv 0 \pmod{p}$$

[5] The matter of units in the rings $\mathbb{Z}[\zeta]$ remains one of the higher mysteries. Kummer's achievement was to be able to tame this matter somewhat. We will discuss more about it in section 2.1 and section 4.2. Also see this discussion on Math.SatckExchange: `http://math.stackexchange.com/q/3185/214604`

[6] Not every algebraic integer with absolute value 1 is a root of unity, there are algebraic integers on the unit circle which aren't roots of unity[18][20]. Also see this Math.StackExchange discussion: `http://math.stackexchange.com/q/4323/214604`

[7] The roots of unity are the numbers of form $e^{2\pi i t/m}$ where t and m are coprime rational integers.

If the powers of ζ occurring here are distinct, then since they form part of a basis of $\mathbb{Z}[\zeta]$, we get p divides x and y, which is a contradiction to our initial assumption $p \nmid xyz$. Otherwise, we have to consider following three cases:

a) $1 = \zeta^{2r}$, then p divides y, contradicting $p \nmid xyz$

b) $1 = \zeta^{2r-1}$, then p divides $x - y$, contradicting Claim 2

c) $\zeta = \zeta^{2r-1}$, then p divides x, contradicting $p \nmid xyz$

Hence our initial assumption was wrong and there don't exist rational integers x, y and z satisfying the first case of FLT for regular prime exponents. □

In 1985, Étienne Fouvry[8], Leonard M. Adleman and David R. Heath-Brown[9] used a refinement of Germain's criterion together with difficult analytic estimates to prove that there are infinitely many primes p such that first case of FLT is true. Though Germain's proof of first case is based on elementary methods, Kummer's proof laid foundations of "Algebraic Number Theory" and hence is worth discussing.

[8] "Théorème de Brun-Titchmarsh; application au théorème de Fermat." *Inventiones Mathematicae* 79, no. 2 (1985), 383–407. http://dx.doi.org/10.1007/bf01388980

[9] Adleman, L. M. and Heath-Brown, D. R. "The first case of Fermat's last theorem." *Inventiones Mathematicae* 79, no. 2 (1985), 409–416. http://doi.org/10.1007/bf01388981

Chapter 2

Ring of Integers of Number Field

Let $\mathbb{A}$ denote the set of algebraic integers in $\mathbb{C}$. Given a number field K of degree n over $\mathbb{Q}$, then $\mathbb{A} \cap K = \mathcal{O}_K$ denotes the ring of integers of K. The additive group part of $\mathcal{O}_K$ is a *free abelian group* of rank n (proof involves application of Cramer's rule, see pp. 29, [1]).

Lemma 1 (Gauss Lemma)**.** *If a polynomial is irreducible in* $\mathbb{Z}[x]$ *then it is irreducible in* $\mathbb{Q}[x]$.

Proof. We will prove the lemma in two steps:

Step 1 If m and n be the greatest common divisor of the coefficients of polynomials f and g in $\mathbb{Z}[x]$ then mn is the greatest common divisor of the coefficients of fg.

Without loss of generality, consider two polynomials $f, g \in \mathbb{Z}[x]$ such that the greatest common divisor of coefficients of each of these polynomials in 1 (if not then can divide by the greatest common divisor and obtain such polynomials). Then we have to prove that 1 is in fact greatest common divisor of the coefficients of fg. On the contrary assume that $d > 1$ is the greatest common divisor of the coefficients of fg, and some rational prime p divides d, hence

$$fg \equiv 0 \pmod{p}$$

But $\mathbb{Z}_p$ is an integral domain, so

$$f \equiv 0 \pmod{p} \quad \text{or} \quad g \equiv 0 \pmod{p}$$

This implies that p divides the coefficients of at least one of the polynomials f or g, thus contradicting the fact that the greatest common divisor of coefficients of each of these polynomials is 1. Hence $d = 1$.

Step 2 If $h \in \mathbb{Z}[x]$ and h is irreducible over $\mathbb{Z}$ then h is irreducible over $\mathbb{Q}[x]$.

On the contrary, assume that $h = fg$ over $\mathbb{Q}[x]$. We can find rational integers a and b such that $af, bg \in \mathbb{Z}[x]$ and can also ensure that the greatest common divisor of each of the polynomials af and bg is 1. Now by Step 1 we conclude that 1 is the greatest common divisor of the coefficients of $abfg = abh$. But since $h \in \mathbb{Z}[x]$ we know that ab must divide the greatest common divisor of the coefficients of abh. Hence $ab|1$ implying $a = b = 1$ and contradicting the fact that h is irreducible in $\mathbb{Z}[x]$.

□

Definition 4 (Embedding in $\mathbb{C}$)**.** An injective homomorphism from K to $\mathbb{C}$. There are n embeddings of K in $\mathbb{C}$.

Definition 5 (Trace of algebraic number)**.** Let L be another number field lying over K and $\sigma_1, \ldots, \sigma_m$ denote the $m = [L : K]$ embeddings of L in $\mathbb{C}$ which fix K point-wise. Then for $\alpha \in L$, trace of L relative to K is a function defined as follows

$$T_K^L(\alpha) = \sigma_1(\alpha) + \sigma_2(\alpha) + \ldots + \sigma_m(\alpha)$$

Definition 6 (Norm of algebraic number)**.** Let L be another number field lying over K and $\sigma_1, \ldots, \sigma_m$ denote the $m = [L : K]$ embeddings of L in $\mathbb{C}$ which fix K point-wise. Then for $\alpha \in L$, norm of L relative to K is a function defined as follows

$$N_K^L(\alpha) = \sigma_1(\alpha)\sigma_2(\alpha) \cdots \sigma_m(\alpha)$$

Theorem 2. *The $T_K^L(\alpha)$ and $N_K^L(\alpha)$ are respectively the trace and determinant of the matrix A, where the matrix A denotes the linear mapping of multiplication by $\alpha \in L$ with respect to any basis $\{\alpha_1, \ldots, \alpha_m\}$ for L over K, $m = [L : K]$.*

Proof. Note that j^{th} column of A consists of the coordinates of $\alpha\alpha_j$ with respect to the α_i. We know that the trace and determinant are independent of the particular basis chosen; thus it is sufficient to calculate them for any convenient basis. Let's fix a basis $\{\beta_1, \beta_2, \ldots, \beta_r\}$ for L over $K[\alpha]$ with $r = [L : K[\alpha]] = \frac{m}{d}$ where $K[\alpha]$ has power basis $\{1, \alpha, \ldots, \alpha^{d-1}\}$ with $d = [K[\alpha] : K]$. Multiply both these basis to get a basis $\{\alpha^i\beta_j : 0 \le i \le d-1 \quad \text{and} \quad 1 \le j \le r\}$ of L over K. Then we make following claim

`Claim:` Let $t(\alpha)$ and $n(\alpha)$ be the sum and product of the d conjugates of α over K, then

$$T_K^L(\alpha) = \frac{m}{d} t(\alpha) \quad \text{and} \quad N_K^L(\alpha) = (n(\alpha))^{m/d}$$

Note that $t(\alpha) = T_K^{K[\alpha]}$ and $n(\alpha) = N_K^{K[\alpha]}$. Each embedding of $K[\alpha]$ in $\mathbb{C}$ extends to exactly $\frac{m}{d} = r$ embeddings on L in $\mathbb{C}$. That establishes the formulas and completes the proof of the theorem. □

Remark 1. From the claim proved in above theorem, we can also conclude that $T_K^L(\alpha)$ and $N_K^L(\alpha)$ are in K and if $\alpha \in \mathcal{O}_L$ then they are in $\mathcal{O}_K$.

Example 1. *Let $K = \mathbb{Q}[\sqrt[3]{k}]$, where k is a cube-free positive integer. For some $a \in \mathbb{Z}$, compute the value of $N_{\mathbb{Q}}^K(\sqrt[3]{k} + a)$.*

Solution. I will discuss 3 ways to compute the norm of given algebraic number

Method 1 Following are the three complex embeddings in this number field:

$$\begin{aligned} a + b\sqrt[3]{k} + c\sqrt[3]{k^2} &\mapsto a + b\sqrt[3]{k} + c\sqrt[3]{k^2} \\ a + b\sqrt[3]{k} + c\sqrt[3]{k^2} &\mapsto a + b\omega\sqrt[3]{k} + c\omega^2\sqrt[3]{k^2} \\ a + b\sqrt[3]{k} + c\sqrt[3]{k^2} &\mapsto a + b\omega^2\sqrt[3]{k} + c\omega\sqrt[3]{k^2} \end{aligned}$$

where a, b, c are rational numbers and $\omega = e^{\frac{2\pi i}{3}}$. Hence

$$N_{\mathbb{Q}}^K(\sqrt[3]{k} + a) = (a + \sqrt[3]{k})(a + \omega\sqrt[3]{k})(a + \omega^2\sqrt[3]{k})$$

Since $\omega + \omega^2 + 1 = 0$, thus

$$N_{\mathbb{Q}}^K(\sqrt[3]{k} + a) = a^3 + k$$

Method 2 We shall compute the minimal polynomial for $\alpha = \sqrt[3]{k} + a$ and then norm will be the negative of the constant term (the product of conjugates of α).

$$\begin{aligned} x &= \sqrt[3]{k} + a \\ \Rightarrow (x-a)^3 &= k \\ \Rightarrow x^3 - 3ax^2 + 3a^2x - (a^3 + k) &= 0 \end{aligned}$$

Hence, $N_{\mathbb{Q}}^{K}(\sqrt[3]{k} + a) = a^3 + k$

Method 3 As per the theorem above, the norm of $\alpha \in \mathbb{Q}[\sqrt[3]{k}]$ is the determinant of the linear map $x \mapsto \alpha x$. Taking $1, \sqrt[3]{k}, \sqrt[3]{k^2}$ to be the basis and $\alpha = \sqrt[3]{k} + a$, we compute the linear maps:

$$\begin{aligned} (\sqrt[3]{k} + a)1 &= a + \sqrt[3]{k} + 0\sqrt[3]{k^2} \\ (\sqrt[3]{k} + a)\sqrt[3]{k} &= 0 + a\sqrt[3]{k} + \sqrt[3]{k^2} \\ (\sqrt[3]{k} + a)\sqrt[3]{k^2} &= k + 0\sqrt[3]{k} + a\sqrt[3]{k^2} \end{aligned}$$

Hence we get

$$N_{\mathbb{Q}}^{K}(\sqrt[3]{k} + a) = \det(A) = \begin{vmatrix} a & 0 & k \\ 1 & a & 0 \\ 0 & 1 & a \end{vmatrix} = a^3 + k$$

Remark 2. Trace and norm functions have property of transitivity, i.e. if K, L, M are number fields such that $K \subset L \subset M$, then for all $\alpha \in M$ we have $T_K^L(T_L^M(\alpha)) = T_K^M(\alpha)$ and $N_K^L(N_L^M(\alpha)) = N_K^M(\alpha)$. For proof see pp. 24 of [1].

Definition 7 (Discriminant of n-tuple)**.** Let $\sigma_1, \ldots, \sigma_n$ denote the $n = [K : \mathbb{Q}]$ embeddings of K in $\mathbb{C}$. For any n-tuple of elements $\alpha_1, \alpha_2, \ldots, \alpha_n \in K$, we define discriminant of $\alpha_1, \alpha_2, \ldots, \alpha_n$ to be

$$\text{disc}\,(\alpha_1, \alpha_2, \ldots, \alpha_n) = \det(\sigma_i(\alpha_j))^2$$

where $\sigma_i(\alpha_j)$ denote element in the i^{th} row and j^{th} column.

Remark 3. Using simple matrix algebra we can prove that

$$\text{disc}\,(\alpha_1, \alpha_2, \ldots, \alpha_n) = \det(T_{\mathbb{Q}}^{K}(\alpha_i\alpha_j))$$

where $T_{\mathbb{Q}}^{K}(\alpha_i\alpha_j)$ denote element in the i^{th} row and j^{th} column. This enables us to conclude that $\text{disc}\,(\alpha_1, \alpha_2, \ldots, \alpha_n) \in \mathbb{Q}$. Also if all $\alpha_i \in \mathcal{O}_K$ then $\text{disc}\,(\alpha_1, \alpha_2, \ldots, \alpha_n) \in \mathbb{Z}$.

Theorem 3. *In $\mathcal{O}_K$ discriminant is an invariant.*

Proof. We will prove two assertions to justify the invariance of the discriminant in this case.

Claim 1 Let $\{\beta_1, \ldots, \beta_n\}$ and $\{\gamma_1, \ldots, \gamma_n\}$ be two integral basis for $\mathcal{O}_K$. Then

$$\text{disc}(\beta_1, \ldots, \beta_n) = \text{disc}(\gamma_1, \ldots, \gamma_n)$$

and we shall denote this constant by $\text{disc}(\mathcal{O}_K)$.

We can write one basis in terms of other as

$$\begin{bmatrix} \beta_1 \\ \vdots \\ \beta_n \end{bmatrix} = M \begin{bmatrix} \gamma_1 \\ \vdots \\ \gamma_n \end{bmatrix}$$

where M is a $n \times n$ matrix over $\mathbb{Z}$. Applying each embedding σ_j to each of the n equations formed above, we get

$$\begin{bmatrix} \sigma_1(\beta_1) & \sigma_2(\beta_1) & \dots & \sigma_n(\beta_1) \\ \vdots & \vdots & \ddots & \vdots \\ \sigma_1(\beta_n) & \sigma_2(\beta_n) & \dots & \sigma_n(\beta_n) \end{bmatrix} = M \begin{bmatrix} \sigma_1(\gamma_1) & \sigma_2(\gamma_1) & \dots & \sigma_n(\gamma_1) \\ \vdots & \vdots & \ddots & \vdots \\ \sigma_1(\gamma_n) & \sigma_2(\gamma_n) & \dots & \sigma_n(\gamma_n) \end{bmatrix}$$

Taking the determinant and squaring we get

$$\operatorname{disc}(\beta_1, \dots, \beta_n) = \det(M)^2 \operatorname{disc}(\gamma_1, \dots, \gamma_n)$$

Clearly $\det(M) \in \mathbb{Z}$ since M is a matrix over $\mathbb{Z}$. This implies that $\operatorname{disc}(\gamma_1, \dots, \gamma_n)$ is a divisor of $\operatorname{disc}(\beta_1, \dots, \beta_n)$, and both have the same sign. Similarly we can show that $\operatorname{disc}(\beta_1, \dots, \beta_n)$ is a divisor of $\operatorname{disc}(\gamma_1, \dots, \gamma_n)$. We conclude that both the discriminants are equal.

Claim 2 If $\alpha_1, \dots, \alpha_n \in \mathcal{O}_K$ then they form an integral basis for $\mathcal{O}_K$ if and only if

$$\operatorname{disc}(\alpha_1, \dots, \alpha_n) = \operatorname{disc}(\mathcal{O}_K)$$

Form Claim 1 it's clear that if $\{\alpha_1, \dots, \alpha_n\}$ for an integral basis for $\mathcal{O}_K$ then

$$\operatorname{disc}(\alpha_1, \dots, \alpha_n) = \operatorname{disc}(\mathcal{O}_K)$$

All we need to prove is its converse. As stated earlier, $\mathcal{O}_K$ is a free abelian group of rank n. If H, G are two free abelian subgroups of rank n in K, with $H \subset G$, then from first isomorphism theorem

$$G/H \cong \mathbb{Z}/k_1\mathbb{Z} \times \mathbb{Z}/k_2\mathbb{Z} \times \cdots \mathbb{Z}/k_n\mathbb{Z}$$

where $k_1, \dots, k_n \in \mathbb{Z}_{>0}$, hence G/H is finite abelian group. Then G/H is a direct sum of at most n cyclic groups. Thus if G has a generating set $\beta_1, \dots, \beta_n$ then there exist appropriate integers $k_1, \dots, k_n$ such that $k_1\beta_1, \dots, k_n\beta_n$ is a generating set for H. Moreover, since

$$\begin{bmatrix} k_1\beta_1 \\ k_2\beta_2 \\ \vdots \\ k_n\beta_n \end{bmatrix} = \begin{bmatrix} k_1 & 0 & \dots & 0 \\ 0 & k_2 & \dots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \dots & k_n \end{bmatrix} \begin{bmatrix} \beta_1 \\ \beta_2 \\ \vdots \\ \beta_n \end{bmatrix}$$

and $|G/H| = k_1 \cdot k_2 \cdots k_n$. As in previous case, we conclude that

$$\operatorname{disc}(H) = |G/H|^2 \operatorname{disc}(G)$$

In this put H to the group generated by $\{\alpha_1, \dots, \alpha_n\}$ and $G = \mathcal{O}_K$. Now thus $\operatorname{disc}(H) = \operatorname{disc}(G)$ we get $|G/H| = 1$ implying that $H = G$.

□

Remark 4. If $\alpha_1, \dots, \alpha_n \in \mathcal{O}_K$ and $\operatorname{disc}(\alpha_1, \dots, \alpha_n)$ is square free, then $\{\alpha_1, \dots, \alpha_n\}$ for an integral basis for $\mathcal{O}_K$ (see pp. 45, [1]).

Theorem 4 (Stickelberger's Criterion). $\operatorname{disc}(\mathcal{O}_K) \equiv 0, 1 \pmod 4$

Proof. K is a number field of order n over $\mathbb{Q}$ and $\sigma_1, \ldots, \sigma_n$ are the embeddings of K in $\mathbb{C}$. Given algebraic integers $\alpha_1, \ldots, \alpha_n \in K$, we know that $d = \operatorname{disc}(\alpha_1, \ldots, \alpha_n) \in \mathbb{Z}$. Note that

$$\det(\sigma_i(\alpha_j)) = \sum_{\rho \in S_n} \operatorname{sgn}(\rho) \prod_{i=1}^{n} \sigma_i \left(\alpha_{\rho(i)}\right)$$

where S_n is the group of permutations of $\{1, 2, \ldots, n\}$ and sgn is $+1$ if ρ is an even permutation and -1 otherwise. Hence the determinant is a sum of $n!$ terms. Let $\mathcal{P}$ denote the sum of terms corresponding to even permutations, and let $\mathcal{N}$ denote the sum of the terms (without negative signs) corresponding to odd permutations. Thus

$$d = (\mathcal{P} - \mathcal{N})^2 = (\mathcal{P} + \mathcal{N})^2 - 4\mathcal{P}\mathcal{N} \tag{2.1}$$

Extending K to a normal extension L of $\mathbb{Q}$, each embedding of K extends to $[L : K]$ embeddings of L, all of which are automorphism of L since L is normal. Note that $\mathcal{P} + \mathcal{N}$ and $\mathcal{P}\mathcal{N}$ lie in L, so we can apply the embeddings to them. Moreover since all σ_i are automorphisms now, we have two possibilities

$$\begin{cases} \sigma_i(\mathcal{P}) = \mathcal{P} \quad \text{and} \quad \sigma_i(\mathcal{N}) = \mathcal{N} \\ \sigma_i(\mathcal{P}) = \mathcal{N} \quad \text{and} \quad \sigma_i(\mathcal{N}) = \mathcal{P} \end{cases}$$

Hence we have $\sigma_i(\mathcal{P}+\mathcal{N}) = \mathcal{P}+\mathcal{N}$ and $\sigma_i(\mathcal{P}\mathcal{N}) = \mathcal{P}\mathcal{N}$ for any σ_i. Since $\mathcal{P}+\mathcal{N}$ and $\mathcal{P}\mathcal{N}$ are the fixed elements of L over $\mathbb{Q}$, we conclude that $\mathcal{P}+\mathcal{N}, \mathcal{P}\mathcal{N} \in \mathbb{Q}$. But, $\mathcal{P}+\mathcal{N}$ and $\mathcal{P}\mathcal{N}$ are algebraic integers since $\alpha_1, \ldots, \alpha_n$ are algebraic integers. We know that the only algebraic integers in $\mathbb{Q}$ are the ordinary integers (see pp. 15, [1]). Therefore, $\mathcal{P} + \mathcal{N}, \mathcal{P}\mathcal{N} \in \mathbb{Z}$ and using this fact in (2.1), we conclude that

$$d \equiv (\mathcal{P} + \mathcal{N})^2 \equiv 0, 1 \pmod 4$$

In particular we have $\operatorname{disc}(\mathcal{O}_K) \equiv 0, 1 \pmod 4$. □

Theorem 5 (Relative discriminant). *Let $K \subset L \subset M$ be number fields, $[L : K] = n, [M : L] = m$, and let $\{\alpha_1, \ldots, \alpha_n\}$ and $\{\beta_1, \ldots, \beta_m\}$ be bases for L over K and M over L, respectively. Then we have*

$$\operatorname{disc}_K^M(\alpha_1\beta_1, \ldots, \alpha_n\beta_m) = \left(\operatorname{disc}_K^L(\alpha_1, \ldots, \alpha_n)\right)^m N_K^L\left(\operatorname{disc}_L^M(\beta_1, \ldots, \beta_m)\right)$$

where, for example, $\operatorname{disc}_K^L(\alpha_1, \ldots, \alpha_n) = \det(\sigma_i(\alpha_j))^2 = \det(T_K^L(\alpha_i\alpha_j))$ *where the embeddings σ_i of L in $\mathbb{C}$ fix K point-wise.*

Proof. Let $\sigma_1, \ldots, \sigma_n$ be the embeddings of L in $\mathbb{C}$ fixing K point-wise, and $\tau_1, \ldots, \tau_m$ be the embeddings of M in $\mathbb{C}$ fixing L point-wise. Fix a normal extension N of $\mathbb{Q}$ such that $M \subset N$, then we can extend all σ_i's and τ_j's to automorphisms of N; fix one extension of each and again denote these extensions by σ_i and τ_j. We define two $mn \times mn$ matrices A and B:

$$A = \begin{bmatrix} A_1 & 0 & \ldots & 0 \\ 0 & A_2 & \ldots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \ldots & A_n \end{bmatrix}$$

$$B = \begin{bmatrix} \sigma_1(\alpha_1)I_m & \sigma_2(\alpha_1)I_m & \ldots & \sigma_n(\alpha_1)I_m \\ \sigma_1(\alpha_2)I_m & \sigma_2(\alpha_2)I_m & \ldots & \sigma_n(\alpha_2)I_m \\ \vdots & \vdots & \ddots & \vdots \\ \sigma_1(\alpha_n)I_m & \sigma_2(\alpha_1)I_m & \ldots & \sigma_n(\alpha_n)I_m \end{bmatrix}$$

where

$$A_i = \begin{bmatrix} \sigma_i(\tau_1(\beta_1)) & \sigma_i(\tau_1(\beta_2)) & \dots & \sigma_i(\tau_1(\beta_m)) \\ \sigma_i(\tau_2(\beta_1)) & \sigma_i(\tau_2(\beta_2)) & \dots & \sigma_i(\tau_2(\beta_m)) \\ \vdots & \vdots & \ddots & \vdots \\ \sigma_i(\tau_m(\beta_1)) & \sigma_i(\tau_1(\beta_2)) & \dots & \sigma_i(\tau_m(\beta_m)) \end{bmatrix} \quad \text{and} \quad I_m = \begin{bmatrix} 1 & 0 & \dots & 0 \\ 0 & 1 & \dots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \dots & 0 \end{bmatrix}$$

are $m \times m$ matrices. Therefore A has $\sigma_i(\tau_h(\beta_k))$ in row $m(i-1)+h$ and column $m(i-1)+k$; B has $\sigma_i(\alpha_j)$ in row $m(i-1)+t$ and column $m(j-1)+t$ for each $t = 1, \dots, m$ and zeros everywhere else. Note that

$$\text{disc}_K^M(\alpha_1\beta_1, \dots, \alpha_n\beta_m) = \det(AB)^2$$

And we have

$$\det(A)^2 = \prod_{i=1}^{n} \det(A_i)^2 = \prod_{i=1}^{n} \sigma_i(\text{disc}_L^M(\beta_1, \dots, \beta_m)) = N_K^L\left(\text{disc}_L^M(\beta_1, \dots, \beta_m)\right)$$

$$\det(B)^2 = [(\det(\sigma_i(\alpha_j))^m]^2 = [(\det(\sigma_i(\alpha_j))^2]^m = (\text{disc}_K^L(\alpha_1, \dots, \alpha_n))^m$$

□

Corollary 2. *Let K and L be number fields such that $[K : \mathbb{Q}] = n$, $[L : \mathbb{Q}] = m$, $[KL : \mathbb{Q}] = mn$ and $\gcd(\text{disc}(\mathcal{O}_K), \text{disc}(\mathcal{O}_L)) = 1$. Then we have*

$$\text{disc}(\mathcal{O}_{KL}) = (\text{disc}\,(\mathcal{O}_K))^{[L:\mathbb{Q}]}\,(\text{disc}\,(\mathcal{O}_L))^{[K:\mathbb{Q}]}$$

Definition 8 (Discriminant of α). Let α be an algebraic integer of degree n over $\mathbb{Q}$ such that $K = \mathbb{Q}[\alpha]$ then we define

$$\text{disc}\,(\alpha) = \text{disc}\,(1, \alpha, \dots, \alpha^{n-1})$$

Remark 5. Suppose $K = \mathbb{Q}[\alpha]$, and let $\alpha_1, \dots, \alpha_n$ denote the conjugates of α over $\mathbb{Q}$. Then

$$\text{disc}(\alpha) = \prod_{1 \le r < s \le n} (\alpha_r - \alpha_s)^2 = \begin{cases} N_{\mathbb{Q}}^K(f'(\alpha)) & \text{if} \quad n \equiv 0, 1 \pmod 4 \\ -N_{\mathbb{Q}}^K(f'(\alpha)) & \text{if} \quad n \equiv 2, 3 \pmod 4 \end{cases}$$

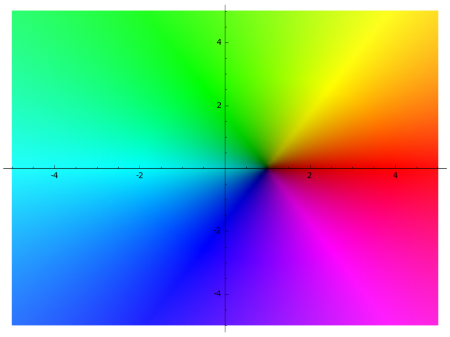
where f is the minimal polynomial for α over $\mathbb{Q}$. The proof uses Vandermonde determinant formula, see pp. 26, [1])

2.1 Cyclotomic Fields

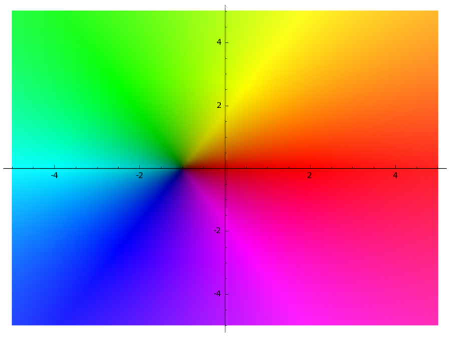
As we have seen in previous chapter, the attempt to prove FLT required a good understanding of m^{th} cyclotomic field $\mathbb{Q}[\zeta_m]$ where $\zeta_m = e^{\frac{2\pi i}{m}}$ with $i = \sqrt{-1}$ and $m \in \mathbb{Z}_{>0}$. $\mathbb{Q}[\zeta_m]$ has degree $\varphi(m) = \#\{k : \gcd(k, m) = 1, 1 \le k \le m\}$, over $\mathbb{Q}$ (pp. 18, [1])

Definition 9 (Cyclotomic Polynomial). It is the monic polynomial with integer coefficients, which is the minimal polynomial of over the field of the rational numbers of any primitive m^{th} root of unity.

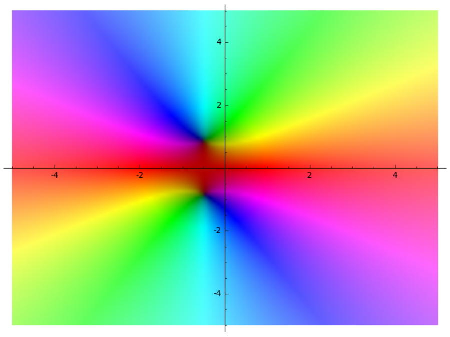
$$\Phi_m(x) = \prod_{\substack{1 \le k \le m \\ \gcd(k,m)=1}} \left(x - e^{\frac{2i\pi k}{m}}\right) = \prod_{\substack{1 \le k \le m \\ \gcd(k,m)=1}} \left(x - \zeta_m^k\right)$$



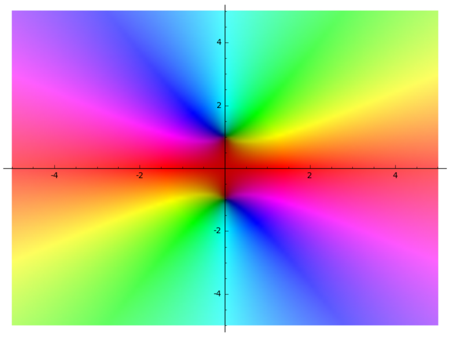
$\Phi_1(x) = x - 1$



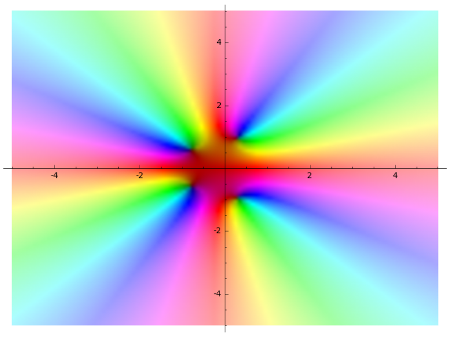
$\Phi_2(x) = x + 1$



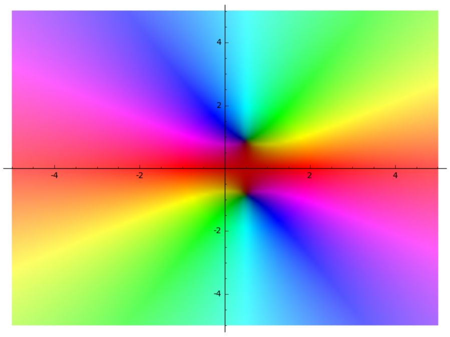
$\Phi_3(x) = x^2 + x + 1$



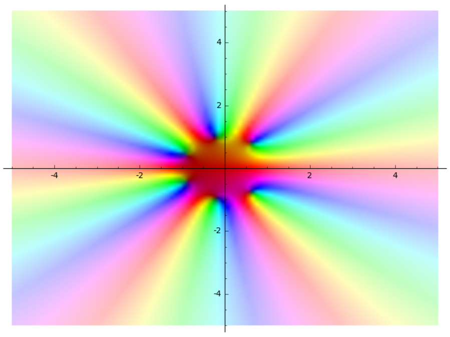
$\Phi_4(x) = x^2 + 1$



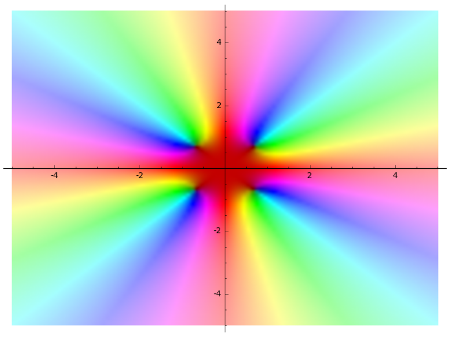
$\Phi_5(x) = x^4 + x^3 + x^2 + x + 1$



$\Phi_6(x) = x^2 - x + 1$

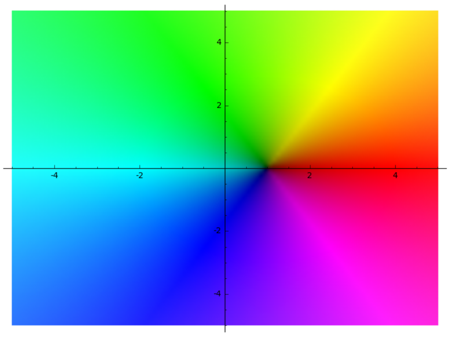


$\Phi_7(x) = x^6 + x^5 + x^4 + x^3 + x^2 + x + 1$

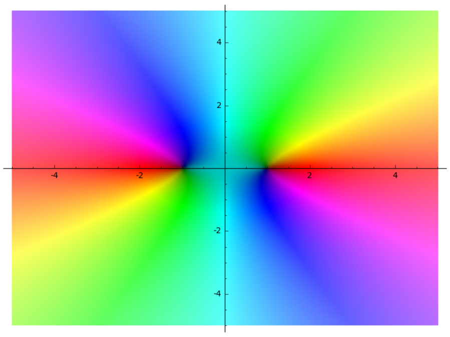


$\Phi_8(x) = x^4 + 1$

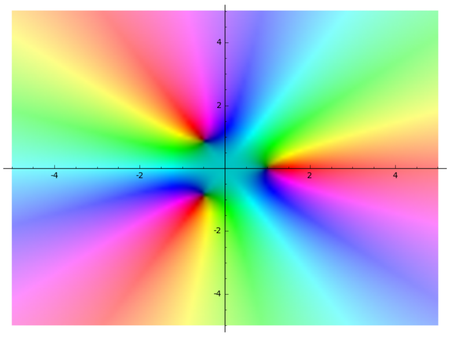
Graphs generated using `complex_plot(f(z),(-5,5),(-5,5))` in SageMath version 7.2



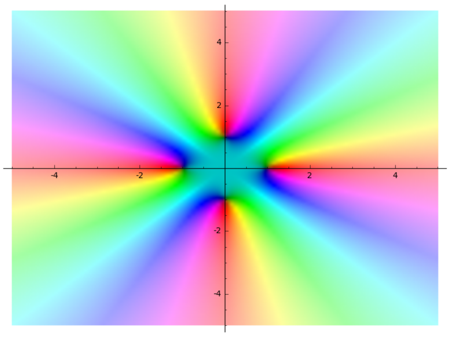
$x = 1$



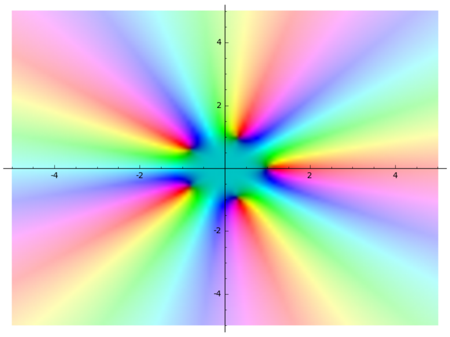
$x^2 = 1$



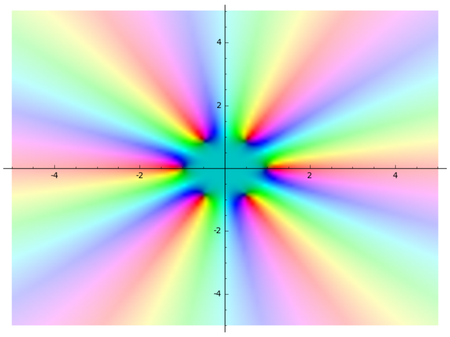
$x^3 = 1$



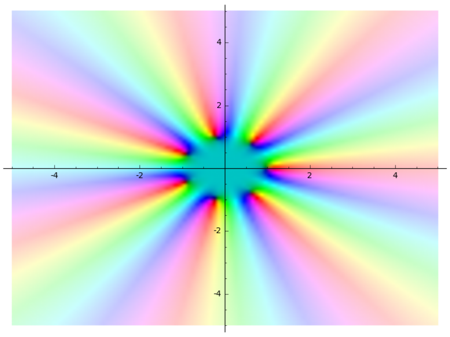
$x^4 = 1$



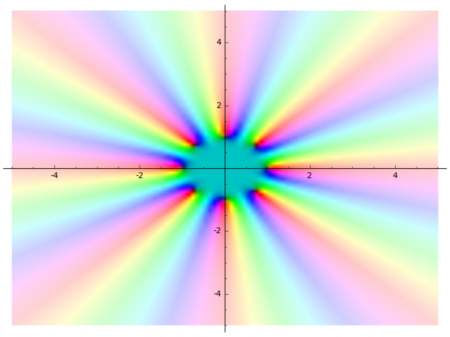
$x^5 = 1$



$x^6 = 1$



$x^7 = 1$



$x^8 = 1$

Graphs generated using `complex_plot(f(z),(-5,5),(-5,5))` in SageMath version 7.2

These are complex plane plots[1] of the first eight cyclotomic polynomials followed by first to eighth roots of unity.

These plots suggest that for odd m, $\Phi_m(-x) = \Phi_{2m}(x)$. This symmetry can be explained by the fact that for odd m, $2m^{th}$ roots of unity are in $\mathbb{Q}[\zeta_m]$. For example[2] the third cyclotomic field is equal to sixth cyclotomic field: $\zeta_6 = -\zeta_6^4 = -(\zeta_6^2)^2$, which shows that $\mathbb{Q}[\zeta_6] = \mathbb{Q}[\zeta_6^2] = \mathbb{Q}[\zeta_3]$. In general, for odd m, $\zeta_{2m} = -\zeta_{2m}^{m+1} \in \mathbb{Q}[\zeta_{2m}^2] = \mathbb{Q}[\zeta_m]$. In fact, we will now prove that for odd m the m^{th} cyclotomic field is the same as $2m^{th}$ and for even m, all cyclotomic fields are distinct.

Theorem 6. *The number of roots of unity in* $\mathbb{Q}[\zeta_m]$ *is* $\operatorname{lcm}(2, m)$.

Proof. If $\mathbb{Q}[\zeta_m]$ contains some r^{th} root of unity then $\mathbb{Q}[\zeta_r] \subset \mathbb{Q}[\zeta_m]$ and using the fact about degree of a cyclotomic field stated earlier, $\varphi(r) \leq \varphi(m)$.

Also, then $\zeta_m \zeta_r = \zeta_{\operatorname{lcm}(m,r)}$ is in $\mathbb{Q}[\zeta_m]$. Hence we have $\operatorname{lcm}(m, r) \leq r$. But least common multiple of two numbers can't be less than any one of them, therefore $\operatorname{lcm}(m, r) = r$. Thus r is a multiple of m, let $r = ms$ for some integer s.

Now by a standard identity for Euler's totient function

$$\varphi(r) = \varphi(ms) = \varphi(m)\varphi(s)\frac{\gcd(m, s)}{\varphi(\gcd(m, s))}$$

Moreover by definition of φ we have $\varphi(a) \leq a$ for any positive integer a, hence

$$\varphi(r) \geq \varphi(m)\varphi(s)$$

Now for some maximal r, $\mathbb{Q}[\zeta_m] = \mathbb{Q}[\zeta_r]$ and in that case we have $\varphi(m) = \varphi(r)$. Using above identity, we conclude

$$\varphi(m) \geq \varphi(m)\varphi(s)$$

Therefore, $\varphi(s) \leq 1$, but by definition of φ it can't be less than one. Hence, $\varphi(s) = 1$ and it implies that $s = 1$ or $s = 2$. Thus $r = m$ or $r = 2m$. This shows that the number of roots of unity in $\mathbb{Q}[\zeta_m]$ can either be m or $2m$. But as a special case of the standard identity for Euler's totient function used above, we have

$$\varphi(2m) = \begin{cases} 2\varphi(m) & \text{if } m \text{ is even} \\ \varphi(m) & \text{if } m \text{ is odd} \end{cases}$$

Since $\varphi(r)$ should not be greater than $\varphi(m)$, we conclude that

$$r = \begin{cases} m & \text{if } m \text{ is even} \\ 2m & \text{if } m \text{ is odd} \end{cases}$$

Thus completing the proof of the theorem. □

Remark 6. The Galois group of $\mathbb{Q}[\zeta_m]$ over $\mathbb{Q}$, $\operatorname{Gal}(\mathbb{Q}[\zeta_m]/\mathbb{Q})$ is isomorphic to the multiplicative group of integers $\mod m$

$$\mathbb{Z}_m^* = \{k : 1 \leq k \leq m, \gcd k, m = 1\}$$

For each $k \in \mathbb{Z}_m^*$ the corresponding automorphism in the Galois group sends ζ_m to ζ_m^k. See pp. 18, [1].

[1] These colour maps are obtained by a stereographic projection from the surface of the three-dimensional colour space (in the hue-lightness-saturation system) onto the complex plane. The hue represents the argument (also called phase angle) of the complex number z. The absolute value (also called magnitude or modulus) is given by the lightness of the colour. All colours of the colour map have the maximal saturation (with respect to the given lightness). Positive real numbers always appear red. The primary colours appear at phase angles $\frac{2\pi}{3}$ (green) and $\frac{4\pi}{3}$ (blue). The subtractive colours yellow, cyan, and magenta have the phases $\frac{\pi}{3}$, π, and $\frac{5\pi}{3}$. The poles of a complex function are white, the zeros are black.

[2] Note that first two cyclotomic fields are both just $\mathbb{Q}$ since $\zeta_1 = 1$ and $\zeta_2 = -1$.

Theorem 7. *If $K = \mathbb{Q}[\zeta_m]$ then $\mathcal{O}_K = \mathbb{Z}[\zeta_m]$.*

Proof. We will prove $\mathcal{O}_K = \mathbb{Z}[\zeta_m]$ by induction on m.

Step 1 If m is power of a prime number, then $\mathcal{O}_K = \mathbb{Z}[\zeta_m]$.

Claim 1 For all $m \geq 3$, $\mathbb{Z}[1-\zeta_m] = \mathbb{Z}[\zeta_m]$ and $\operatorname{disc}(1-\zeta_m) = \operatorname{disc}(\zeta_m)$.
Since $\zeta_m = 1-(1-\zeta_m)$, we get $\mathbb{Z}[1-\zeta_m] = \mathbb{Z}[\zeta_m]$. By Remark 5 we get

$$\operatorname{disc}(\zeta_m) = \prod_{1\leq r<s\leq n} (\alpha_r - \alpha_s)^2 = \prod_{1\leq r<s\leq n} ((1-\alpha_r)-(1-\alpha_s))^2 = \operatorname{disc}(1-\zeta_m)$$

where α_i runs through the conjugates of ζ_m and $1-\alpha_i$ runs through the conjugates of $1-\zeta_m$.

Claim 2 For $m = p^r$, p is a prime number,

$$p = \prod_{\substack{1\leq k\leq m\\ \gcd(k,m)=1}} \left(1-\zeta_m^k\right)$$

This is stronger version of the fact used in third claim of Theorem 1 and can be proved by same approach. Consider

$$f(x) = \frac{x^{p^r}-1}{x^{p^{r-1}}-1} = 1 + x^{p^{r-1}} + x^{2p^{r-1}} + \ldots + x^{(p-1)p^{r-1}}$$

Then all ζ_m^k where $1 \leq k \leq m$ and $\gcd(k,m) = 1$, are roots of f since they are roots of $x^{p^r}-1$ but not of $x^{p^{r-1}}-1$. Thus in fact

$$f(x) = \prod_{\substack{1\leq k\leq m\\ \gcd(k,m)=1}} \left(1-\zeta_m^k\right)$$

where # values of $k = \varphi(m) = \varphi(p^r) = (p-1)p^{r-1}$. Finally put $x = 1$.

Claim 3 $\mathcal{O}_K = \mathbb{Z}[1-\zeta_m]$
Using the fact that $\mathcal{O}_K$ is a free abelian group of rank n, every $\alpha \in \mathcal{O}_K$ can be expressed in the form (pp. 29, [1])

$$\alpha = \frac{k_1 + k_2(1-\zeta_m) + \cdots + k_n(1-\zeta_m)^{n-1}}{d}$$

where $n = \varphi(p^r)$, all $k_i \in \mathbb{Z}$ and $d = \operatorname{disc}(1-\zeta_m) = \operatorname{disc}(\zeta_m)$ [by Claim 1]. Also by using the fact that $\mathbb{Q}[\zeta_m]$ has degree $\varphi(m)$ over $\mathbb{Q}$ and Remark 5 we conclude that $\operatorname{disc}(\zeta_m)$ divides $m^{\varphi(m)}$ (pp. 27, [1]). Hence in this case d is a power of p.
On the contrary assume that $\mathcal{O}_K \neq \mathbb{Z}[1-\zeta_m]$, then there must be some α for which not all k_i are divisible by d. It follows that $\mathcal{O}_K$ contains an element of form

$$\beta = \frac{k_j(1-\zeta_m)^{j-1} + k_{j+1}(1-\zeta_m)^j + \cdots + k_n(1-\zeta_m)^{n-1}}{p}$$

for some $j \leq n$ and k_j not divisible by p. Claim 2 shows that $p/(1-\zeta_m)^n \in \mathbb{Z}[\zeta_m]$ since $1-\zeta_m^k$ is easily seen to be divisible in $\mathbb{Z}[\zeta_m]$ by $1-\zeta_m$. Then $p/(1-\zeta_m)^j \in \mathbb{Z}[\zeta_m]$ and hence $\beta p/(1-\zeta_m)^j \in \mathcal{O}_K$. Subtracting the terms which are obviously in $\mathcal{O}_K$, we obtain $k_j/(1-\zeta_m) \in \mathcal{O}_K$. Therefore, $N_{\mathbb{Q}}^K(1-\zeta_m)|N_{\mathbb{Q}}^K(k_j)$. But this is impossible since $N_{\mathbb{Q}}^K(k_j) = k_j^n$ and $N_{\mathbb{Q}}^K(1-\zeta_m) = p$ (Use Remark 5 in Claim 2). Hence proving our claim.

Finally, by Claim 1, $\mathcal{O}_K = \mathbb{Z}[\zeta_m]$ if m is power of a prime number.

Step 2 Let $m = m_1 \times m_2$, for some relatively prime integers $m_1, m_2 > 1$ such that $K_1 = \mathbb{Q}[\zeta_{m_1}]$ and $K_2 = \mathbb{Q}[\zeta_{m_2}]$. If $\mathcal{O}_{K_1} = \mathbb{Z}[\zeta_{m_1}]$ and $\mathcal{O}_{K_2} = \mathbb{Z}[\zeta_{m_2}]$ then $\mathcal{O}_K = \mathbb{Z}[\zeta_m]$.

We have following result:

> Let K and L be two number fields, then KL is the smallest subfield of $\mathbb{C}$ containing K and L. If $[KL : \mathbb{Q}] = mn$ and $\gcd(\operatorname{disc}(\mathcal{O}_K), \operatorname{disc}(\mathcal{O}_L)) = 1$, then $\mathcal{O}_{KL} = \mathcal{O}_K\mathcal{O}_L$. (pp. 34, [1])

To be able to apply this result, we must prove that the required conditions are satisfied.

Claim 1 $K = K_1K_2$

Clearly, $\zeta_m^{m_1} = \zeta_{m_2}$ and $\zeta_m^{m_2} = \zeta_{m_1}$. Since m_1 and m_2 are coprime, it follows that $\zeta_m = \zeta_{m_1}^r\zeta_{m_2}^s$ for some $r, s \in \mathbb{Z}$ such that $rm_2 + sm_1 = 1$ and hence $K = K_1K_2$.

Claim 2 $[K_1K_2 : \mathbb{Q}] = \varphi(m)\varphi(n)$ and $\gcd(\operatorname{disc}(\mathcal{O}_{K_1}), \operatorname{disc}(\mathcal{O}_{K_2})) = 1$

Since m_1 and m_2 are coprime, $[K : \mathbb{Q}] = \varphi(m) = \varphi(m_1)\varphi(m_2) = [K_1K_2 : \mathbb{Q}]$. As stated in third claim of first step of this proof, $\operatorname{disc}(\zeta_{m_i})$ divides $m_i^{\varphi(m_i)}$ for $i = 1, 2$ and also by Theorem 3, we conclude that

$$\gcd(\operatorname{disc}(\mathcal{O}_{K_1}), \operatorname{disc}(\mathcal{O}_{K_2})) = \gcd(\operatorname{disc}(\zeta_{m_1}), \operatorname{disc}(\zeta_{m_2})) = \gcd(m_1, m_2) = 1$$

Claim 1 also implies that $\mathbb{Z}[\zeta_m] = \mathbb{Z}[\zeta_{m_1}]\mathbb{Z}[\zeta_{m_2}]$ and using the result stated in box above we complete proof of this step.

Combining both the steps above, we complete the proof. □

Theorem 8. *Let p be a prime number, then $\operatorname{disc}(\zeta_p) = \pm p^{p-2}$, where $+$ sign holds iff $p \equiv 1, 2 \pmod 4$.*

Proof. This is direct application of Remark 5. We wish to use following formula

$$\operatorname{disc}(\zeta_p) = \begin{cases} N_{\mathbb{Q}}^{\mathbb{Q}[\zeta_p]}(f'(\zeta_p)) & \text{if} \quad p-1 \equiv 0, 1 \pmod 4 \\ -N_{\mathbb{Q}}^{\mathbb{Q}[\zeta_p]}(f'(\zeta_p)) & \text{if} \quad p-1 \equiv 2, 3 \pmod 4 \end{cases}$$

We know that the cyclotomic polynomial (i.e. minimal polynomial) is

$$f(x) = 1 + x + x^2 + \ldots + x^{p-1} = \frac{x^p - 1}{x - 1}$$

The easiest way to compute $f'(\zeta_p)$ is to write $(x-1)f(x) = x^p - 1$ and differentiate

$$f(x) + (x-1)f'(x) = px^{p-1}$$

Therefore since $\zeta_p^p = 1$ and $\varphi(p) = p - 1$, we have

$$N_{\mathbb{Q}}^{\mathbb{Q}[\zeta_p]}(f'(\zeta_p)) = N_{\mathbb{Q}}^{\mathbb{Q}[\zeta_p]}\left(\frac{p}{\zeta_p(\zeta_p - 1)}\right) = \frac{N_{\mathbb{Q}}^{\mathbb{Q}[\zeta_p]}(p)}{N_{\mathbb{Q}}^{\mathbb{Q}[\zeta_p]}(\zeta_p)N_{\mathbb{Q}}^{\mathbb{Q}[\zeta_p]}(\zeta_p - 1)} = \frac{p^{p-1}}{1 \times p}$$

since $N_{\mathbb{Q}}^{\mathbb{Q}[\zeta_p]}(\zeta_p - 1) = N_{\mathbb{Q}}^{\mathbb{Q}[\zeta_p]}(1 - \zeta_p)$ because $p - 1$ is even and $N_{\mathbb{Q}}^{\mathbb{Q}[\zeta_p]}(1 - \zeta_p) = p$ follows from the fact used in third claim of Theorem 1. □

Remark 7. We can use Corollary 2 to derive general formula for discriminant of ζ_m for any m, but the calculations are said to be messy, hence I will just state the result

$$\operatorname{disc}(\zeta_m) = \frac{(-1)^{\frac{\varphi(m)}{2}} m^{\varphi(m)}}{\prod_{p|m} p^{\frac{\varphi(m)}{(p-1)}}}$$

2.2 Real Cyclotomic Fields

Based upon cyclotomic fields, we define m^{th} real cyclotomic field as $\mathbb{Q}[\xi_m]$ where $\xi_m = \zeta_m + \zeta_m^{-1} = 2\cos(\frac{2\pi}{m}) \in \mathbb{R}$.

Theorem 9. *If $K = \mathbb{Q}[\xi_m]$ then $\mathcal{O}_K = \mathbb{Z}[\xi_m]$ for $m \geq 3$.*

Proof. We will divide the proof in several parts

Claim 1 $\mathbb{Q}[\zeta_m]$ is of degree 2 over the field $K = \mathbb{Q}[\xi_m]$.

By definition of ξ_m we have that ζ_m is a root of

$$f(x) = x^2 - \xi_m x + 1$$

Hence ζ_m is root of a irreducible monic polynomial of degree 2 over K, proving our claim.

Claim 2 $\mathbb{Q}[\xi_m]$ is the fixed field of the automorphism σ of $\mathbb{Q}[\zeta_m]$ determined by $\sigma(\zeta_m) = \zeta_m^{-1}$.

Note that $\zeta_m^{-1} = \overline{\zeta_m}$, therefore σ is just complex conjugation. The result follows.

Claim 3 $K = \mathbb{Q}[\xi_m] = \mathbb{R} \cap \mathbb{Q}[\zeta_m]$

Since $\xi_m = \zeta_m + \overline{\zeta_m} = 2\Re(\zeta_m)$ and from Claim 2 we get

$$\mathbb{Q}[\xi_m] \subset \mathbb{R} \cap \mathbb{Q}[\zeta_m] \subset \mathbb{Q}[\zeta_m]$$

From Claim 1 we know that $[\mathbb{Q}\,[\zeta_m] : \mathbb{Q}\,[\xi_m]] = 2$. Also since

$$\mathbb{Q}[\zeta_m] = \{a + b\zeta_m : a, b \in \mathbb{R} \cap \mathbb{Q}[\zeta_m]\}$$

we have $[\mathbb{Q}\,[\zeta_m] : \mathbb{R} \cap \mathbb{Q}\,[\zeta_m]] = 2$. Therefore, since both are extensions of same degree and one is subset of other, we conclude that $\mathbb{Q}[\xi_m] = \mathbb{R} \cap \mathbb{Q}[\zeta_m]$.

Claim 4 $\mathcal{O}_K = \mathbb{R} \cap \mathbb{Z}[\zeta_m]$

Note that $\mathbb{Z}[\zeta_m] = \mathbb{A} \cap \mathbb{Q}[\zeta_m]$. Now use Claim 3 to get

$$\mathbb{R} \cap \mathbb{Z}[\zeta_m] = \mathbb{A} \cap \mathbb{Q}[\xi_m] = \mathcal{O}_K$$

Claim 5 If $n = \frac{\varphi(m)}{2}$, then $\{\xi_m^i \zeta_m^j : i = 0, 1, \ldots, n-1; j = 0, 1\}$ is an integral basis for $\mathbb{Z}[\zeta_m]$

Note that, $[\mathbb{Q}[\zeta_m] : K][K : \mathbb{Q}] = [\mathbb{Q}[\zeta_m] : \mathbb{Q}]$, therefore from Claim 1 and the fact stated in previous section we get (since $m \geq 3$)

$$[K : \mathbb{Q}] = \frac{[\mathbb{Q}[\zeta_m] : \mathbb{Q}]}{[\mathbb{Q}[\zeta_m] : K]} = \frac{\varphi(m)}{2} = n$$

Thus we can write

$$\mathbb{Z}[\zeta_m] = \{a_0 + a_1\zeta_m + \ldots + a_n\zeta_m^n + a_{n+1}\zeta_m^{n+1} + \ldots + a_{2n-2}\zeta_m^{2n-2} + a_{2n-1}\zeta_m^{2n-1} : a_i \in \mathbb{Z}\}$$

But $\zeta_m^{2n} = 1$, thus we can rewrite above set as

$$\mathbb{Z}[\zeta_m] = \{a_0 + a_1\zeta_m + \ldots + a_n\zeta_m^n + a_{n+1}\zeta_m^{-(n-1)} + \ldots + a_{2n-2}\zeta_m^{-2} + a_{2n-1}\zeta_m^{-1} : a_i \in \mathbb{Z}\}$$

Now using $\xi_m = \zeta_m + \zeta_m^{-1}$ we get

$$\mathbb{Z}[\zeta_m] = \{a_0 + \ldots + a_n\zeta_m^n + a_{n+1}(\xi_m - \zeta_m)^{n-1} + \ldots + a_{2n-1}(\xi_m - \zeta_m) : a_i \in \mathbb{Z}\}$$

Since, as stated in Claim 1, $\zeta_m^2 - \xi_m\zeta_m + 1 = 0$ we conclude that all ζ_m^i for $i = 2, \ldots, n$ will vanish, for example:

$$\zeta_m^3 = (\xi_m\zeta_m - 1)\zeta_m = \xi_m\zeta_m^2 - \zeta_m = \xi_m(\xi_m\zeta_m - 1) - \zeta_m = \xi_m^2\zeta_m - \xi_m - \zeta_m$$

$$\zeta_m^4 = (\xi_m\zeta_m - 1)^2 = \xi_m^2\zeta_m^2 + 1 - 2\xi_m\zeta_m = \xi_m^2(\xi_m\zeta_m - 1) + 1 - 2\xi_m\zeta_m = \xi_m^3\zeta_m - \xi_m^2 - 2\xi_m\zeta_m + 1$$

Hence proving our claim. (Note that the claim is correct since dimension is still $2n$.)

Claim 6 $\{1, \xi_m, \xi_m^2, \ldots, \xi_m^{n-1}\}$ is an integral basis for $\mathcal{O}_K$

According to Claim 4, we just need to show that $\{1, \xi_m, \xi_m^2, \ldots, \xi_m^{n-1}\}$ is an integral basis for $\mathbb{R} \cap \mathbb{Z}[\zeta_m]$. Since $\xi_m = 2\Re(\zeta_m)$ implies that $\Re(\zeta_m)$ is linearly dependent on ξ_m. Therefore, $\mathbb{R} \cap \mathbb{Z}[\zeta_m]$ has claimed basis by eliminating all dependent elements from the integral basis in Claim 5.

From Claim 6 we conclude that $\mathcal{O}_K = \mathbb{Z}[\xi_m]$. □

Theorem 10. *Let p be an odd prime number, then* $\operatorname{disc}(\xi_p) = p^{\frac{p-3}{2}}$.

Proof. We have $\mathbb{Q} \subset \mathbb{Q}[\xi_p] \subset \mathbb{Q}[\zeta_p]$, and $[\mathbb{Q}[\xi_p] : \mathbb{Q}] = \frac{\varphi(p)}{2} = n$, $[\mathbb{Q}[\zeta_p] : \mathbb{Q}[\xi_p]] = 2$.

Also, from previous theorem, I know that the integral basis for $\mathbb{Q}[\xi_p]/\mathbb{Q}$ is $\{1, \xi_p, \ldots, \xi_p^{n-1}\}$ and the integral basis for $\mathbb{Q}[\zeta_p]/\mathbb{Q}[\xi_p]$ is $\{1, \zeta_p\}$.

We will use Theorem 5 to calculate discriminant:

$$\operatorname{disc}_{\mathbb{Q}}^{\mathbb{Q}[\zeta_p]}(1, \zeta_p, \xi_p, \xi_p\zeta_p, \ldots, \xi_p^{n-1}, \xi_p^{n-1}\zeta_p) = \left(\operatorname{disc}_{\mathbb{Q}}^{\mathbb{Q}[\xi_p]}(1, \xi_p, \ldots, \xi_p^{n-1})\right)^2 N_{\mathbb{Q}}^{\mathbb{Q}[\xi_p]}\left(\operatorname{disc}_{\mathbb{Q}[\xi_p]}^{\mathbb{Q}[\zeta_p]}(1, \zeta_p)\right)$$

Keeping in mind Theorem 3 and using Theorem 7, Theorem 9 along with Remark 5 we get (note that the ± signs cancel out on both sides)

$$\operatorname{disc}_{\mathbb{Q}}^{\mathbb{Q}[\zeta_p]}(\zeta_p) = \left(\operatorname{disc}_{\mathbb{Q}}^{\mathbb{Q}[\xi_p]}(\xi_p)\right)^2 N_{\mathbb{Q}}^{\mathbb{Q}[\xi_p]}\left(N_{\mathbb{Q}[\xi_p]}^{\mathbb{Q}[\zeta_p]}(f'(\zeta_p))\right)$$

where $f(x) = x^2 - \xi_p x + 1$, is the minimal polynomial for $\mathbb{Q}[\zeta_p]$ over $\mathbb{Q}[\xi_p]$. Using Remark 2 we can re-write it as

$$\operatorname{disc}_{\mathbb{Q}}^{\mathbb{Q}[\zeta_p]}(\zeta_p) = \left(\operatorname{disc}_{\mathbb{Q}}^{\mathbb{Q}[\xi_p]}(\xi_p)\right)^2 N_{\mathbb{Q}}^{\mathbb{Q}[\zeta_p]}(f'(\zeta_p)) \tag{2.2}$$

Note that $\xi_p = \zeta_p + \zeta_p^{-1}$, therefore

$$N_{\mathbb{Q}}^{\mathbb{Q}[\zeta_p]}(f'(\zeta_p)) = N_{\mathbb{Q}}^{\mathbb{Q}[\zeta_p]}(2\zeta_p - \xi_p) = N_{\mathbb{Q}}^{\mathbb{Q}[\zeta_p]}(\zeta_p - \zeta_p^{-1}) = \frac{N_{\mathbb{Q}}^{\mathbb{Q}[\zeta_p]}(\zeta_p - 1)\, N_{\mathbb{Q}}^{\mathbb{Q}[\zeta_p]}(\zeta_p + 1)}{N_{\mathbb{Q}}^{\mathbb{Q}[\zeta_p]}(\zeta_p)}$$

Observe that $\Phi_p(x-1)$ is the minimal polynomial for ζ_p+1 where $\Phi_p(x) = 1+x+\ldots+x^{p-1}$, therefore $N_{\mathbb{Q}}^{\mathbb{Q}[\zeta_p]}(1+\zeta_p)$ is equal to constant term in $\Phi_p(x-1) = 1+(x-1)+\ldots+(x-1)^{p-1}$, since $p-1$ is even we will have $\frac{p-1}{2}$ times -1 and $\frac{p-1}{2}+1$ times $+1$, thus leaving $+1$ as constant term. Hence[3] $N_{\mathbb{Q}}^{\mathbb{Q}[\zeta_p]}(1+\zeta_p) = 1$. Using this along with Theorem 8 in (2.2) we get(note that we already cancelled out sign arising due to p)

$$\operatorname{disc}_{\mathbb{Q}}^{\mathbb{Q}[\xi_p]}(\xi_p) = \operatorname{disc}(\xi_p) = \pm\sqrt{\frac{p^{p-2}}{p}} = \pm p^{\frac{p-3}{2}}$$

But + sign must hold since, $\mathbb{Q}[\xi_p]$ contains $\sqrt{\operatorname{disc}(\xi_p)}$ (algebraic closure property of number field). □

2.3 Quadratic Fields

Let K be a number field and $d = \operatorname{disc}(\mathcal{O}_K)$. By definition $\sqrt{d}$ is the determinant of a matrix with entries in the normal closure of K. Thus the normal closure of K contains $\mathbb{Q}[\sqrt{d}]$. But, $\mathbb{Q}[\sqrt{d}]$ is not always a quadratic field. It can be the case that d is a square, and that the normal closure contains no quadratic field. We will come back to this idea towards the end of this section.

[3] We can use similar argument to calculate $N(1-\zeta_p)$ in Theorem 8.

Theorem. *Let $K = \mathbb{Q}[\sqrt{m}]$ where m be squarefree integer.*

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

For proof see Theorem 1.7.8 of [21].

Remark 8. We can write $\mathcal{O}_K$ explicitly as

$$\mathcal{O}_K = \begin{cases} a + b\sqrt{m} & \text{if} \quad m \equiv 2, 3 \pmod 4 \quad \text{and} \quad a, b \in \mathbb{Z} \\ \dfrac{a + b\sqrt{m}}{2} & \text{if} \quad m \equiv 1 \pmod 4 \quad \text{and} \quad a \equiv b \pmod 2 \end{cases}$$

Theorem 11. *Let $K = \mathbb{Q}[\sqrt{m}]$ where m be squarefree integer.*

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

Proof. We can prove this by using any of the four different formulas known to us, I will use the basic definition. Note that the complex embeddings of $\mathbb{Q}[\sqrt{m}]$ are:

$$\begin{aligned} \sigma_1 : a + b\sqrt{m} &\mapsto a + b\sqrt{m} \\ \sigma_2 : a + b\sqrt{m} &\mapsto a - b\sqrt{m} \end{aligned}$$

$$\operatorname{disc}(1, \sqrt{m}) = \begin{vmatrix} \sigma_1(1) & \sigma_1(\sqrt{m}) \\ \sigma_2(1) & \sigma_2(\sqrt{m}) \end{vmatrix}^2 = \begin{vmatrix} 1 & \sqrt{m} \\ 1 & -\sqrt{m} \end{vmatrix}^2 = 4m$$

$$\operatorname{disc}\left(1, \frac{1+\sqrt{m}}{2}\right) = \begin{vmatrix} \sigma_1(1) & \sigma_1\left(\frac{1+\sqrt{m}}{2}\right) \\ \sigma_2(1) & \sigma_2\left(\frac{1+\sqrt{m}}{2}\right) \end{vmatrix}^2 = \begin{vmatrix} 1 & \frac{1+\sqrt{m}}{2} \\ 1 & \frac{1-\sqrt{m}}{2} \end{vmatrix}^2 = m$$

□

Remark 9. The minimal polynomial for α can be computed by equating it to x and getting rid of fractional powers. Here, minimal polynomial for $\sqrt{m}$ is $f(x) = x^2 - m$ and for $\frac{1+\sqrt{m}}{2}$ is $f(x) = x^2 - x + \frac{1-m}{4}$.

Theorem 12. *Every quadratic field is contained in a cyclotomic field.*

Proof. We will prove this theorem in two steps

Claim 1 $\mathbb{Q}[\zeta_8]$ contains $\mathbb{Q}[\sqrt{2}]$.

It's enough to show that eigth cyclotomic field contains $\sqrt{2}$

$$\zeta_8 = e^{2\pi i/8} = \cos\left(\frac{\pi}{4}\right) + i\sin\left(\frac{\pi}{4}\right) = \frac{1}{\sqrt{2}} + i\frac{1}{\sqrt{2}}$$

$$\sqrt{2} = \left(\frac{1}{\sqrt{2}} + i\frac{1}{\sqrt{2}}\right) + \left(\frac{1}{\sqrt{2}} + i\frac{1}{\sqrt{2}}\right) = \zeta_8 + \zeta_8^{-1} = \zeta_8 + \zeta_8^7$$

Claim 2 Let p be an odd prime then $\mathbb{Q}[\zeta_p]$ contains $\sqrt{p}$ if $p \equiv 1 \pmod 4$, and $\sqrt{-p}$ if $p \equiv 3 \pmod 4$.

From Theorem 8 we know that

$$\operatorname{disc}(\zeta_p) = \begin{cases} p^{p-2} & \text{if} \quad p \equiv 1 \pmod 4 \\ -p^{p-2} & \text{if} \quad p \equiv 3 \pmod 4 \end{cases}$$

Taking square-root of both sides we get

$$\frac{\sqrt{\mathrm{disc}(\zeta_p)}}{p^{(p-3)/2}} = \begin{cases} \sqrt{p} & \text{if} \quad p \equiv 1 \pmod 4 \\ \sqrt{-p} & \text{if} \quad p \equiv 3 \pmod 4 \end{cases}$$

Now our claim follows using Remark 5

$$\frac{1}{p^{(p-3)/2}} \prod_{1 \le r < s \le p-1} |\zeta_p^r - \zeta_p^s| = \begin{cases} \sqrt{p} & \text{if} \quad p \equiv 1 \pmod 4 \\ \sqrt{-p} & \text{if} \quad p \equiv 3 \pmod 4 \end{cases}$$

Claim 3 $K = \mathbb{Q}[\sqrt{m}]$ for a squarefree m is contained in the d^{th} cyclotomic field, where $d = \mathrm{disc}(\mathcal{O}_K)$.

Note that $\sqrt{-1} = i = e^{\frac{2\pi i}{4}} = \zeta_4 = \zeta_8^2$. Hence, if the q^{th} cyclotomic field contains $\mathbb{Q}[\sqrt{p}]$, the $4q^{th}$ cyclotomic field contains $\mathbb{Q}[\sqrt{-p}]$ because it must contain the fourth root of unity i along with $\sqrt{p}$. Since m is square free, $m = \pm p_1 \cdot p_2 \cdots p_k$ for k distinct primes. Also, from Theorem 11 we know that

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

Thus completing the proof of the claim.

We could have proved this theorem without third claim, by proving a weaker result. Note that if $r|s$, then $\mathbb{Q}[\zeta_r] \subset \mathbb{Q}[\zeta_s]$ since $\zeta_r = \zeta_s^{s/r}$. From this and the previous observations, $\sqrt{m} \in \mathbb{Q}[\zeta_8, \zeta_{p_1}, \ldots, \zeta_{p_k}] \subset \mathbb{Q}[\zeta_{8m}]$. Hence the cyclotomic field $\mathbb{Q}[\zeta_{8m}]$ contains $\mathbb{Q}[\sqrt{m}]$. □

Remark 10. We can use the method used to prove second claim above to express $\sqrt{-3} = \zeta_3 - \zeta_3^2$ and $\sqrt{5} = \zeta_5 - \zeta_5^2 - \zeta_5^3 + \zeta_5^4$

2.4 Pure Cubic Fields

Unlike the number fields discussed so far, these are not Galois extensions. These fields were first studied by Richard Dedekind (pp. 105, [5]).

Theorem 13. *Let $K = \mathbb{Q}[\sqrt[3]{m}]$ where m be a cubefree integer. Let $\alpha = \sqrt[3]{m}$ and $m = hk^2$, where h and k are squarefree and relatively prime. Then an integral basis for $\mathcal{O}_K$ consists of*

$$\begin{cases} \left\{1, \alpha, \frac{\alpha^2}{k}\right\} & \textit{if} \quad m \not\equiv \pm 1 \pmod 9 \quad \textit{or} \quad h^2 \not\equiv k^2 \pmod 9 \\ \left\{1, \alpha, \frac{\alpha^2 \pm k^2\alpha + k^2}{3k}\right\} & \textit{if} \quad m \equiv \pm 1 \pmod 9 \quad \textit{or} \quad h^2 \equiv k^2 \pmod 9 \end{cases}$$

with the ± sign corresponding in the obvious way.

Proof. We will use the following result:

Let $K = \mathbb{Q}[\alpha]$ and $\alpha \in \mathcal{O}_K$ such that it has degree n over $\mathbb{Q}$. Then there is an integral basis

$$\left\{1, \frac{f_1(\alpha)}{d_1}, \ldots, \frac{f_{n-1}(\alpha)}{d_{n-1}}\right\}$$

where f_i are monic polynomials of degree i over $\mathbb{Z}$ and $d_i \in \mathbb{Z}\backslash\{0\}$ are uniquely determined such that $d_1 \Big| d_2 \Big| \ldots \Big| d_{n-1}$. (pp. 36, [1])

Following facts can also be established (pp. 49, [1])

(i) $\operatorname{disc}(\alpha) = (d_1 \cdot d_2 \cdots d_{n-1})^2 \operatorname{disc}(\mathcal{O}_K)$

(ii) $d_1 \cdot d_2 \cdots d_{n-1}$ is the order of the group $\mathcal{O}_K/\mathbb{Z}[\alpha]$ (follows from second claim of Theorem 3)

(iii) If $i + j < n$ then $d_i d_j \Big| d_{i+j}$

(iv) For $i < n$, $d_1^i \Big| d_i$ and $d_1^{n(n-1)} \Big| \operatorname{disc}(\alpha)$.

By the above result, the ring $\mathcal{O}_K$ has an integral basis of the form $\left\{1, \frac{f_1(\alpha)}{d_1}, \frac{f_2(\alpha)}{d_2}\right\}$.

Claim 1 $d_1 = 1$ and $f_1(\alpha) = \alpha$

By Remark 5, $\operatorname{disc}(\alpha) = -N_{\mathbb{Q}}^{\mathbb{Q}[\alpha]}(g'(\alpha))$ where $g(x) = x^3 - m$. Therefore, $\operatorname{disc}(\alpha) = -27\alpha^6 = -27m^2$. Now using the fact (iv) stated above we conclude that $d_1 = 1$ except possibly when $9|m$, in which case $d_1 = 1$ or 3.

Suppose $9|m$ and $\beta = (\alpha + a)/3$ for some integer a, is an element of $\mathcal{O}_K$. Using Example 1 we can compute

$$\begin{aligned} T_{\mathbb{Q}}^{\mathbb{Q}[\alpha]}(\beta^3) =& T_{\mathbb{Q}}^{\mathbb{Q}[\alpha]}\left(\frac{\alpha^3 + 3a\alpha^2 + 3a^2\alpha + a^3}{27}\right) \\ =& \frac{1}{27}\left(T_{\mathbb{Q}}^{\mathbb{Q}[\alpha]}(\alpha^3) + 3aT_{\mathbb{Q}}^{\mathbb{Q}[\alpha]}(\alpha^2) + 3a^2T_{\mathbb{Q}}^{\mathbb{Q}[\alpha]}(\alpha) + 3a^3\right) \end{aligned}$$

Note that

$$T_{\mathbb{Q}}^{\mathbb{Q}[\alpha]}(\alpha) = \text{sum of roots} = \alpha_1 + \alpha_2 + \alpha_3 = 0$$

and we know following two identities from school days:

$$\begin{aligned} \alpha_1^2 + \alpha_2^2 + \alpha_3^2 =& (\alpha_1 + \alpha_2 + \alpha_3)^2 - 2(\alpha_1\alpha_2 + \alpha_2\alpha_3 + \alpha_3\alpha_1) \\ \alpha_1^3 + \alpha_2^3 + \alpha_3^3 =& (\alpha_1 + \alpha_2 + \alpha_3)(\alpha_1^2 + \alpha_2^2 + \alpha_3^2 - \alpha_1\alpha_2 + \alpha_2\alpha_3 + \alpha_3\alpha_1) + 3\alpha_1\alpha_2\alpha_3 \end{aligned}$$

Moreover

$$\alpha_1\alpha_2 + \alpha_2\alpha_3 + \alpha_3\alpha_1 = \text{the sum of product of two roots taken at a time} = 0$$

We conclude that

$$\begin{aligned} T_{\mathbb{Q}}^{\mathbb{Q}[\alpha]}(\alpha^2) = \alpha_1^2 + \alpha_2^2 + \alpha_3^2 =& 0 \\ T_{\mathbb{Q}}^{\mathbb{Q}[\alpha]}(\alpha^3) = T_{\mathbb{Q}}^{\mathbb{Q}[\alpha]}(m) = \alpha_1^3 + \alpha_2^3 + \alpha_3^3 =& 3m \end{aligned}$$

Giving us

$$T_{\mathbb{Q}}^{\mathbb{Q}[\alpha]}(\beta^3) = \frac{1}{27}\left(3m + 3a^3\right)$$

Now since $T_{\mathbb{Q}}^{\mathbb{Q}[\alpha]}(\beta^3) \in \mathbb{Z}$ for $\beta \in \mathcal{O}_K$ and $9|m$, we conclude that $3|a$. Hence $\alpha/3 \in \mathcal{O}_K$ and $N_{\mathbb{Q}}^{\mathbb{Q}[\alpha]}(\alpha/3) \in \mathbb{Z}$, implying that $27|m$. But we are given that $9|m$, hence contradicting the assumption (requirements are higher than initially stated). Therefore $d_1 = 3$ is not possible.

Since $d_1 = 1$, we can take $f_1(\alpha) = \alpha$.

Claim 2 $\dfrac{\alpha^2}{k} \in \mathcal{O}_K$

Clearly $\alpha^2/k \in K$ and observe that it's also an algebraic integer since $\frac{\alpha^2}{k} = \sqrt[3]{\frac{h^2k^4}{k^3}} = \sqrt[3]{h^2k}$ is a root of $h(x) = x^3 - h^2k$, which is irreducible over $\mathbb{Z}$. Therefore, $\alpha^2/k \in \mathbb{A} \cap K = \mathcal{O}_K$.

Claim 3 $\beta = \dfrac{(\alpha \mp 1)^2}{3} \in \mathcal{O}_K$ when $m \equiv \pm 1 \pmod 9$, with the signs corresponding in obvious way.

Note that

$$\left(\beta - \frac{1}{3}\right)^3 = \left(\frac{(\alpha \mp 1)^2}{3} - \frac{1}{3}\right)^3 = \left(\frac{\alpha^2 \mp 2\alpha}{3}\right)^3$$

Therefore,

$$\begin{aligned}
\left(\beta^3 - \beta^2 + \frac{\beta}{3} - \frac{1}{27}\right) - \left(\frac{\alpha^6 \mp 8\alpha^3 \mp 6\alpha^5 + 12\alpha^4}{27}\right) &= 0\\
\left(\beta^3 - \beta^2 + \frac{\beta}{3} - \frac{1}{27}\right) - \left(\frac{m^2 \mp 8m \mp 6m\alpha^2 + 12m\alpha}{27}\right) &= 0\\
\left(\beta^3 - \beta^2 + \frac{\beta}{3}\right) - \left(\frac{(m \mp 1)^2 \mp 6m(1 + \alpha^2 \mp 2\alpha)}{27}\right) &= 0\\
\left(\beta^3 - \beta^2 + \frac{\beta}{3}\right) - \left(\frac{(m \mp 1)^2 \mp 6m(\alpha \mp 1)^2}{27}\right) &= 0\\
\left(\beta^3 - \beta^2 + \frac{\beta}{3}\right) - \left(\frac{(m \mp 1)^2 \mp 18m\beta}{27}\right) &= 0\\
\beta^3 - \beta^2 + \left(\frac{1 \pm 2m}{3}\right)\beta - \frac{(m \mp 1)^2}{27} &= 0
\end{aligned}$$

Hence β is root of an irreducible monic polynomial with coefficients in $\mathbb{Z}$ (since $m \equiv \pm 1 \pmod 9$). Since $\beta \in K$, we conclude that $\beta \in \mathcal{O}_K$.

Claim 4 $\dfrac{\alpha^2 \pm k^2\alpha + k^2}{3k} \in \mathcal{O}_K$ when $m \equiv \pm 1 \pmod 9$, with signs corresponding in obvious way.

Follows from Claim 2 and Claim 3 since sum and product of two elements from given ring of integers belongs to same ring of integers. So let's find this linear combination for one sign combination ($m \equiv 1 \pmod 9$)

$$\frac{\alpha^2 + k^2\alpha + k^2}{3k} = A\frac{\alpha^2}{k} + B\frac{(\alpha - 1)^2}{3} + C\alpha$$

Equating coefficients of powers of α we get:

$$\begin{cases} k^2 = Bk & \Rightarrow B = k \\ 3Ck - 2Bk = k^2 & \Rightarrow C = k \\ 3A + kB = 1 & \Rightarrow A = \frac{1-k^2}{3} \end{cases}$$

Now since $m = hk^2 \equiv 1 \pmod 9$, note that $x^2 \equiv 1, 4, 7 \pmod 9$ and $4 \cdot 7 \equiv 1 \pmod 9$. Therefore, $k^2 \equiv 1 \pmod 3$ and $A \in \mathbb{Z}$. Similarly we can find A, B, C for other sign combination. Hence our claim is true.

Claim 5 $k|d_2$ when $m \not\equiv \pm 1 \pmod 9$ and $3k|d_2$ when $m \equiv \pm 1 \pmod 9$

From Claim 2 and Claim 4 we can conclude this.

Claim 6 $d_2|3m$

Using fact (i) from the result in box stated initially, we conclude that $d_2|\sqrt{\operatorname{disc}(\alpha)}$. From Claim 1 we know that $\operatorname{disc}(\alpha) = -27m^2$. Since $d_2 \in \mathbb{Z}$, $d_2|3m$.

Claim 7 Let p be a prime number such that $p \neq 3, p|m, p^2 \not| m$ then $p \not| d_2$.

On the contrary assume that $p|d_2$ and let $f_2(\alpha) = \alpha^2 + b\alpha + c$ for $b, c \in \mathbb{Z}$. Then $f_2(\alpha)/p \in \mathcal{O}_K$ and as in Claim 1, we can compute its trace:

$$T_{\mathbb{Q}}^{\mathbb{Q}[\alpha]}\left(\frac{\alpha^2 + b\alpha + c}{p}\right) = \frac{3c}{p} \in \mathbb{Z}$$

Therefore, $p|c$; hence $(\alpha^2 + b\alpha)/p \in \mathcal{O}_K$. By cubing and considering its trace

$$\begin{aligned} T_{\mathbb{Q}}^{\mathbb{Q}[\alpha]}\left(\frac{\alpha^6 + b^3\alpha^3 + 3b\alpha^5 + 3b^2\alpha^4}{p^3}\right) &= T_{\mathbb{Q}}^{\mathbb{Q}[\alpha]}\left(\frac{m^2 + b^3m + 3bm\alpha^2 + 3b^2m\alpha}{p^3}\right) \\ &= \frac{3m^2}{p^3} + \frac{3b^3m}{p^3} + 0 + 0 \in \mathbb{Z} \end{aligned}$$

Since $p \neq 3$, $p^3|(m^2 + b^3m)$; hence $p^2|m$. Thus contradicting our assumption and proving our claim.

Claim 8 Let p be a prime number such that $p \neq 3$ and $p^2|m$ then $p^2 \not| d_2$.

As seen in proof of Claim 7, if $p|d_2$ then $p^2|m$. Hence $p^2 \not| d_2$.

Claim 9 Let $f_2(\alpha) = \alpha^2 + b\alpha + c$ for $b, c \in \mathbb{Z}$, then d_2 divides $b^2 + 2c$, $m + 2bc$ and $c^2 + 2bm$.

Square and verify.

$$\begin{aligned} \left(\frac{f_2(\alpha)}{d_2}\right)^2 &= \frac{\alpha^4 + b^2\alpha^2 + c^2 + 2b\alpha^3 + 2bc\alpha + 2c\alpha^2}{d_2^2} \\ &= \frac{m\alpha + b^2\alpha^2 + c^2 + 2bm + 2bc\alpha + 2c\alpha^2}{d_2^2} \\ &= \frac{(b^2 + 2c)\alpha^2 + (m + 2bc)\alpha + c^2 + 2bm}{d_2^2} \end{aligned}$$

Claim 10 Let $3 \not| m$ then $3 \not| d_2$ if $m \not\equiv \pm 1 \pmod 9$ and $3|d_2$ if $m \equiv \pm 1 \pmod 9$.

Note that Claim 6 implies that $9 \not| d_2$. When $m \equiv \pm 1 \pmod 9$ we already know that $3|d_2$ (Claim 5).

Now for $m \not\equiv \pm 1 \pmod 9$, on the contrary assume that $3|d_2$. Then Claim 9 implies that $c \equiv 1 \pmod 3$ and $b \equiv m \pmod 3$. This implies that $(\alpha^2 + m\alpha + 1)/3 \in \mathcal{O}_K$. Now if $m \equiv 1 \pmod 3$, then $(\alpha - 1)^2/3 \in \mathcal{O}_K$. Raising it to fourth power and considering the trace

$$T_{\mathbb{Q}}^{\mathbb{Q}[\alpha]}\left(\frac{(\alpha - 1)^8}{3^4}\right) = \frac{1 - 56m + 28m^2}{27} \in \mathbb{Z}$$

Hence $m \equiv 1 \pmod 9$, contrary to our assumption. Similarly we can obtain contradiction for $m \equiv 2 \pmod 3$.

Claim 11 Let $3|m$ but $9 \not| m$ then $3 \not| d_2$.

Assuming $3|d_2$, Claim 9 implies that $3|b$ and $3|c$. Thus $\alpha^2/3 \in \mathcal{O}_K$ and computing trace of sixth power (i.e. till trace is non-zero and denominator have higher exponent than numerator)

$$T_{\mathbb{Q}}^{\mathbb{Q}[\alpha]}\left(\frac{\alpha^{12}}{3^6}\right) = \frac{m^4}{3^5} \in \mathbb{Z}$$

This contradicts the condition that $9 \not| m$.

Claim 12 Let $9|m$ then $9 \not| d_2$.

Assume $9|d_2$, Claim 9 implies that $9|c$, hence $(\alpha^2 + b\alpha)/9 \in \mathcal{O}_K$. Now proceed as in Claim 7 to obtain a contradiction.

Claim 13 d_2 is not larger that k when $m \not\equiv \pm 1 \pmod 9$ and $3k$ when $m \equiv \pm 1 \pmod 9$.

Combining all claims from Claim 6 to Claim 12 we obtain this.

Claim 14 $d_2 = k$ and $f_2(\alpha) = \alpha^2$ when $m \not\equiv \pm 1 \pmod 9$; $d_2 = 3k$ and $f_2(\alpha) = \alpha^2 + \pm k^2\alpha + k^2$ $d_2 = 3k$ when $m \equiv \pm 1 \pmod 9$.

From Claim 5 and Claim 13 we conclude that $d_2 = k$ when $m \not\equiv \pm 1 \pmod 9$ and $d_2 = 3k$ when $m \equiv \pm 1 \pmod 9$. Combining this with Claim 2 and Claim 4, the claim follows.

Combining Claim 1 and Claim 14 proves the theorem. □

Remark 11. For a square free integer m, if $\alpha = \sqrt[3]{m}$ then

$$\mathcal{O}_K = \begin{cases} a + b\alpha + c\alpha^2 & \text{if} \quad m \not\equiv \pm 1 \pmod 9 \quad \text{and} \quad a,b,c \in \mathbb{Z} \\ \dfrac{a + b\alpha + c\alpha^2}{3} & \text{if} \quad m \equiv \pm 1 \pmod 9 \quad \text{and} \quad a \equiv \pm b \equiv c \pmod 3 \end{cases}$$

with the ± sign corresponding in the obvious way.

Theorem 14. *Let $K = \mathbb{Q}[\sqrt[3]{m}]$ where m is squarefree integer.*

$$\operatorname{disc}(\mathcal{O}_K) = \begin{cases} -27m^2 & \textit{if} \quad m \not\equiv \pm 1 \pmod 9 \\ -3m^2 & \textit{if} \quad m \equiv \pm 1 \pmod 9 \end{cases}$$

Proof. If m is square free then we can set $k = 1, h = m$ in previous theorem to get

$$\mathcal{O}_K = \begin{cases} \mathbb{Z}[\sqrt[3]{m}] = \{a + b\sqrt[3]{m} + c\sqrt[3]{m^2} : a,b,c \in \mathbb{Z}\} & \text{if} \quad m \not\equiv \pm 1 \pmod 9 \\ \left\{\frac{a+b\sqrt[3]{m}+c\sqrt[3]{m^2}}{3} : a \equiv c \equiv \pm b \pmod 3\right\} & \text{if} \quad m \equiv \pm 1 \pmod 9 \end{cases}$$

with the ± sign corresponding in the obvious way. We will use basic definition to compute the discriminant. As stated in Example 1, following are the three complex embeddings in this number field (put $\alpha = \sqrt[3]{m}$ for the sake of clarity):

$$\begin{aligned} \sigma_1 : a + b\alpha + c\alpha^2 &\mapsto a + b\alpha + c\alpha^2 \\ \sigma_2 : a + b\alpha + c\alpha^2 &\mapsto a + b\omega\alpha + c\omega^2\alpha^2 \\ \sigma_3 : a + b\alpha + c\alpha^2 &\mapsto a + b\omega^2\alpha + c\omega\alpha^2 \end{aligned}$$

where a, b, c are rational numbers and $\omega = e^{\frac{2\pi i}{3}}$. Also using the fact $\omega + \omega^2 + 1 = 0$, we get[4]

$$\operatorname{disc}(1, \alpha, \alpha^2) = \begin{vmatrix} \sigma_1(1) & \sigma_1(\alpha) & \sigma_1(\alpha^2) \\ \sigma_2(1) & \sigma_2(\alpha) & \sigma_2(\alpha^2) \\ \sigma_3(1) & \sigma_3(\alpha) & \sigma_3(\alpha^2) \end{vmatrix}^2 = \begin{vmatrix} 1 & \alpha & \alpha^2 \\ 1 & \omega\alpha & \omega^2\alpha^2 \\ 1 & \omega^2\alpha & \omega\alpha^2 \end{vmatrix}^2 = -27\alpha^6$$

[4] Note that in this case $\operatorname{disc}(\mathcal{O}_K) = \operatorname{disc}(\alpha)$ which was calculated in previous theorem, again calculated here for fun.

$$\operatorname{disc}\left(1,\alpha,\tfrac{\alpha^2\pm\alpha+1}{3}\right)=\begin{vmatrix}\sigma_1(1) & \sigma_1(\alpha) & \sigma_1\left(\frac{\alpha^2\pm\alpha+1}{3}\right)\\ \sigma_2(1) & \sigma_2(\alpha) & \sigma_2\left(\frac{\alpha^2\pm\alpha+1}{3}\right)\\ \sigma_3(1) & \sigma_3(\alpha) & \sigma_3\left(\frac{\alpha^2\pm\alpha+1}{3}\right)\end{vmatrix}^2=\begin{vmatrix}1 & \alpha & \frac{\alpha^2\pm\alpha+1}{3}\\ 1 & \omega\alpha & \frac{\omega^2\alpha^2\pm\omega\alpha+1}{3}\\ 1 & \omega^2\alpha & \frac{\omega\alpha^2\pm\omega^2\alpha+1}{3}\end{vmatrix}^2=-3\alpha^6$$

□

2.5 Biquadratic Fields

A biquadratic field $K=\mathbb{Q}[\sqrt{m},\sqrt{n}]=\mathbb{Q}[\sqrt{m}+\sqrt{n}]$ where m and n are distinct squarefree integers, is a Galois extension of the rational number field $\mathbb{Q}$ with Galois group the Klein four-group (pp. 116, [1]). It consists of three quadratic fields $\mathbb{Q}[\sqrt{m}],\mathbb{Q}[\sqrt{n}]$ and $\mathbb{Q}[\sqrt{k}]$ where $k=\frac{mn}{[\gcd(m,n)]^2}$. We can see this in two ways, depending on how we represent the elements of the permutation group[8]:

◇ Let $a=\sqrt{m},b=-\sqrt{m},c=\sqrt{n},d=-\sqrt{n}$, then

$$\operatorname{Gal}(K/\mathbb{Q})=\{1,(a,b),(c,d),(a,b)(c,d)\}\cong V_4$$

◇ Let $e=\sqrt{m}+\sqrt{n},f=\sqrt{m}-\sqrt{n},g=-\sqrt{m}+\sqrt{n},h=-\sqrt{m}-\sqrt{n}$

$$\operatorname{Gal}(K/\mathbb{Q})=\{1,(e,f)(g,h),(e,g)(f,h),(e,h)(f,g)\}\cong V_4$$

Lemma 2. *Let $K=\mathbb{Q}[\sqrt{m},\sqrt{n}]$ be a biquadratic field and $\alpha\in K$. Then $\alpha\in\mathcal{O}_K$ if and only if $N^K_{\mathbb{Q}[\sqrt{m}]}(\alpha)$ and $T^K_{\mathbb{Q}[\sqrt{m}]}(\alpha)$ are algebraic integers.*

Proof. One side of implication that if $\alpha\in\mathcal{O}_K$ then $N^K_{\mathbb{Q}[\sqrt{m}]}(\alpha)$ and $T^K_{\mathbb{Q}[\sqrt{m}]}(\alpha)$ are algebraic integers follows from Remark 1.

For other side of the implication note that norm and trace of an element belong to $\mathbb{Z}$ characterizes the elements of the ring of integers only for quadratic extensions since the monic minimal polynomial in that case is $x^2-T^{\mathbb{Q}[\sqrt{m}]}_{\mathbb{Q}}(\alpha)x+N^{\mathbb{Q}[\sqrt{m}]}_{\mathbb{Q}}(\alpha)$. Let $N^K_{\mathbb{Q}[\sqrt{m}]}(\alpha)$ and $T^K_{\mathbb{Q}[\sqrt{m}]}(\alpha)$ be algebraic integers and since K is a quadratic extension of $\mathbb{Q}[\sqrt{m}]$ the result follows. □

Theorem 15. *Let $K=\mathbb{Q}[\sqrt{m},\sqrt{n}]$ be a biquadratic field. Then an integral basis for $\mathcal{O}_K$ consists of*

$$\begin{cases}\left\{1,\sqrt{m},\sqrt{n},\dfrac{\sqrt{n}+\sqrt{k}}{2}\right\} & \textit{if}\quad m\equiv 3\pmod 4,\quad n\equiv k\equiv 2\pmod 4\\ \left\{1,\dfrac{1+\sqrt{m}}{2},\sqrt{n},\dfrac{\sqrt{n}+\sqrt{k}}{2}\right\} & \textit{if}\quad m\equiv 1\pmod 4,\quad n\equiv k\equiv 2,3\pmod 4\\ \left\{1,\dfrac{1+\sqrt{m}}{2},\dfrac{1+\sqrt{n}}{2},\left(\dfrac{1+\sqrt{m}}{2}\right)\left(\dfrac{1+\sqrt{k}}{2}\right)\right\} & \textit{if}\quad m\equiv n\equiv k\equiv 1\pmod 4\end{cases}$$

Proof. We divide the proof in 4 parts

Claim 1 $m\equiv 3\pmod 4, n\equiv k\equiv 2\pmod 4$ then the basis of $\mathcal{O}_K$ is $\left\{1,\sqrt{m},\sqrt{n},\dfrac{\sqrt{n}+\sqrt{k}}{2}\right\}$

We can write $\alpha\in\mathcal{O}_K$ as linear combination of $1,\sqrt{m},\sqrt{n},\sqrt{k}$ with rational coefficients

$$\alpha=A+B\sqrt{m}+C\sqrt{n}+D\sqrt{k}$$

Now to determine A, B, C, D we will take trace with respect to every quadratic subfield

$$\begin{aligned}
T^K_{\mathbb{Q}[\sqrt{m}]}(\alpha) &= \left(A + B\sqrt{m} + C\sqrt{n} + D\sqrt{k}\right) + \left(A + B\sqrt{m} - C\sqrt{n} - D\sqrt{k}\right) \\
&= 2A + 2B\sqrt{m} \\
T^K_{\mathbb{Q}[\sqrt{n}]}(\alpha) &= \left(A + B\sqrt{m} + C\sqrt{n} + D\sqrt{k}\right) + \left(A - B\sqrt{m} + C\sqrt{n} - D\sqrt{k}\right) \\
&= 2A + 2C\sqrt{n} \\
T^K_{\mathbb{Q}[\sqrt{k}]}(\alpha) &= \left(A + B\sqrt{m} + C\sqrt{n} + D\sqrt{k}\right) + \left(A - B\sqrt{m} - C\sqrt{n} + D\sqrt{k}\right) \\
&= 2A + 2D\sqrt{k}
\end{aligned}$$

As per Lemma 2 each of them must be an algebraic integer. Therefore, for some $a, b, c, d \in \mathbb{Z}$

$$A = \frac{a}{2} \quad , \quad B = \frac{b}{2} \quad , \quad C = \frac{c}{2} \quad \text{and} \quad D = \frac{d}{2}$$

Therefore, we can write

$$\alpha = \frac{a + b\sqrt{m} + c\sqrt{n} + d\sqrt{k}}{2}$$

Now we will consider $N^K_{\mathbb{Q}[\sqrt{m}]}(\alpha)$ to find relations between a, b, c and d. Note that $\sqrt{k} = \frac{\sqrt{m}\sqrt{n}}{\gcd(m,n)}$, hence

$$\begin{aligned}
N^K_{\mathbb{Q}[\sqrt{m}]}(\alpha) &= \left(\frac{a + b\sqrt{m} + c\sqrt{n} + d\sqrt{k}}{2}\right)\left(\frac{a + b\sqrt{m} - c\sqrt{n} - d\sqrt{k}}{2}\right) \\
&= \frac{(a + b\sqrt{m})^2 - (c\sqrt{n} + d\sqrt{k})^2}{4} \\
&= \frac{a^2 + b^2m + 2ab\sqrt{m} - c^2n - d^2k - \frac{2cdn}{\gcd(m,n)}\sqrt{m}}{4} \\
&= \frac{a^2 + b^2m - c^2n - d^2k}{4} + \frac{\gcd(m,n)ab - cdn}{2\gcd(m,n)}\sqrt{m}
\end{aligned}$$

But by Lemma 2 this must be an algebraic integer in $\mathbb{Z}[\sqrt{m}]$, hence a and b must be even and $c \equiv d \pmod 2$. Using this fact we can rewrite α such that all the coefficients lie in $\mathbb{Z}$:

$$\begin{aligned}
\alpha &= \frac{a + b\sqrt{m} + c\sqrt{n} - d\sqrt{n} + d\sqrt{n} + d\sqrt{k}}{2} \\
&= \frac{a}{2} + \frac{b}{2}\sqrt{m} + \left(\frac{c-d}{2}\right)\sqrt{n} + d\left(\frac{\sqrt{n} + \sqrt{k}}{2}\right)
\end{aligned}$$

Claim 2 $m \equiv 1 \pmod 4$, $n \equiv k \equiv 2, 3 \pmod 4$ then the basis of $\mathcal{O}_K$ is $\left\{1, \frac{1+\sqrt{m}}{2}, \sqrt{n}, \frac{\sqrt{n}+\sqrt{k}}{2}\right\}$

We can write $\alpha \in \mathcal{O}_K$ as linear combination of $1, \sqrt{m}, \sqrt{n}, \sqrt{k}$ with rational coefficients

$$\alpha = A + B\sqrt{m} + C\sqrt{n} + D\sqrt{k}$$

Now to determine A, B, C, D we will take trace with respect to every quadratic subfield and as in previous case

$$\begin{aligned}
T^K_{\mathbb{Q}[\sqrt{m}]}(\alpha) &= 2A + 2B\sqrt{m} = 2A - 2B + 4B\left(\frac{\sqrt{m}+1}{2}\right) \\
T^K_{\mathbb{Q}[\sqrt{n}]}(\alpha) &= 2A + 2C\sqrt{n} \\
T^K_{\mathbb{Q}[\sqrt{k}]}(\alpha) &= 2A + 2D\sqrt{k}
\end{aligned}$$

As per Lemma 2 each of them must be an algebraic integer. Therefore, for some $a, b, c, d \in \mathbb{Z}$

$$A = \frac{a}{2} \quad , \quad B = \frac{b}{2} \quad , \quad C = \frac{c}{2} \quad \text{and} \quad D = \frac{d}{2}$$

Therefore, we can write

$$\alpha = \frac{a + b\sqrt{m} + c\sqrt{n} + d\sqrt{k}}{2}$$

Now we will consider $N^K_{\mathbb{Q}[\sqrt{m}]}(\alpha)$ to find relations between a, b, c and d. Note that $\sqrt{k} = \frac{\sqrt{m}\sqrt{n}}{\gcd(m,n)}$ and as in previous case

$$\begin{aligned} N^K_{\mathbb{Q}[\sqrt{m}]}(\alpha) &= \frac{a^2 + b^2m - c^2n - d^2k}{4} + \frac{\gcd(m,n)ab - cdn}{2\gcd(m,n)}\sqrt{m} \\ &= \frac{a^2+b^2m-c^2n-d^2k-2ab+\frac{2cdn}{\gcd(m,n)}}{4} + \left(ab - \frac{cdn}{\gcd(m,n)}\right)\left(\frac{\sqrt{m}+1}{2}\right) \end{aligned}$$

But by Lemma 2 this must be an algebraic integer in $\mathbb{Z}[\frac{\sqrt{m}+1}{2}]$, hence $a \equiv b \pmod 2$ and $c \equiv d \pmod 2$. Using this fact we can rewrite α such that all the coefficients lie in $\mathbb{Z}$:

$$\begin{aligned} \alpha &= \frac{a + b\sqrt{m} - b + b + c\sqrt{n} - d\sqrt{n} + d\sqrt{n} + d\sqrt{k}}{2} \\ &= \frac{a-b}{2} + b\left(\frac{1+\sqrt{m}}{2}\right) + \left(\frac{c-d}{2}\right)\sqrt{n} + d\left(\frac{\sqrt{n}+\sqrt{k}}{2}\right) \end{aligned}$$

Claim 3 $m \equiv n \equiv k \equiv 1 \pmod 4$ then the basis of $\mathcal{O}_K$ is $\left\{1, \frac{1+\sqrt{m}}{2}, \frac{1+\sqrt{n}}{2}, \left(\frac{1+\sqrt{m}}{2}\right)\left(\frac{1+\sqrt{k}}{2}\right)\right\}$

We can write $\alpha \in \mathcal{O}_K$ as linear combination of $1, \sqrt{m}, \sqrt{n}, \sqrt{k}$ with rational coefficients

$$\alpha = A + B\sqrt{m} + C\sqrt{n} + D\sqrt{k}$$

Now to determine A, B, C, D we will take trace with respect to every quadratic subfield and as in previous case

$$\begin{aligned} T^K_{\mathbb{Q}[\sqrt{m}]}(\alpha) &= 2A - 2B + 4B\left(\frac{\sqrt{m}+1}{2}\right) \\ T^K_{\mathbb{Q}[\sqrt{n}]}(\alpha) &= 2A - 2C + 4C\left(\frac{\sqrt{n}+1}{2}\right) \\ T^K_{\mathbb{Q}[\sqrt{k}]}(\alpha) &= 2A - 2D + 4D\left(\frac{\sqrt{k}+1}{2}\right) \end{aligned}$$

As per Lemma 2 each of them must be an algebraic integer. Therefore, for some $a, b, c, d \in \mathbb{Z}$ such that $a \equiv b \equiv c \equiv d \pmod 2$

$$A = \frac{a}{4} \quad , \quad B = \frac{b}{4} \quad , \quad C = \frac{c}{4} \quad \text{and} \quad D = \frac{d}{4}$$

Therefore, we can write

$$\alpha = \frac{a + b\sqrt{m} + c\sqrt{n} + d\sqrt{k}}{4}$$

where $a \equiv b \equiv c \equiv d \pmod 2$.

Now consider another algebraic number $\beta \in K$

$$\beta = v\left(\frac{1+\sqrt{m}}{2}\right)\left(\frac{1+\sqrt{k}}{2}\right) = \frac{v + v\sqrt{m} + vm\sqrt{n} + v\sqrt{k}}{4}$$

since $m \equiv 1 \pmod 4$, for all $v \in \mathbb{Z}$, $\beta \in \mathcal{O}_K$. By closure property, $\alpha + \beta \in \mathcal{O}_K$.

$$\gamma = \alpha + \beta = \frac{a + v + (b+v)\sqrt{m} + (c+vm)\sqrt{n} + (d+v)\sqrt{k}}{4}$$

If $d + v = 0$, then $a + v \equiv b + v \equiv c + vm \equiv 0 \pmod 2$ implying that

$$\gamma = \frac{r + s\sqrt{m} + t\sqrt{n}}{2}$$

for some $r, s, t \in \mathbb{Z}$. Now by using norm condition we conclude that $r + s + t \equiv 0 \pmod 2$. Using this fact we can rewrite α such that all the coefficients lie in $\mathbb{Z}$:

$$\alpha = (a - b - c - dm) + \left(\tfrac{b-d}{2}\right)\left(\tfrac{1+\sqrt{m}}{2}\right) + \left(\tfrac{c-dm}{2}\right)\left(\tfrac{1+\sqrt{n}}{2}\right) + d\left(\tfrac{1+\sqrt{m}}{2}\right)\left(\tfrac{1+\sqrt{k}}{2}\right)$$

Claim 4 The above three cases are unique upto rearrangement of m, n and k and there is no other case possible.

It's clear that the cases are unique upto rearrangement of m, n, k. Let's see why the only other possible case is invalid. If $m \equiv 3 \pmod 4$ and $n \equiv 3 \pmod 4$ then $mn \equiv 1 \pmod 4$, implying $k = 1$ and hence $m = n$.

This completes the proof. □

Theorem 16. *Let $K = \mathbb{Q}[\sqrt{m}, \sqrt{n}]$ be a biquadratic field. Then $\operatorname{disc}(\mathcal{O}_K)$ is the product of the discriminants of the three quadratic subfields. Therefore*

$$\operatorname{disc}(\mathcal{O}_K) = \begin{cases} 64mnk & \textit{if} \quad m \equiv 3 \pmod 4, \quad n \equiv k \equiv 2 \pmod 4 \\ 16mnk & \textit{if} \quad m \equiv 1 \pmod 4, \quad n \equiv k \equiv 2, 3 \pmod 4 \\ mnk & \textit{if} \quad m \equiv n \equiv k \equiv 1 \pmod 4 \end{cases}$$

Proof. The complex embeddings for this field are (note that $\sqrt{k} = \frac{\sqrt{m}\sqrt{n}}{\gcd(m,n)}$)

$$\begin{aligned}
\sigma_1 &: a + b\sqrt{m} + c\sqrt{n} + d\sqrt{k} \mapsto a + b\sqrt{m} + c\sqrt{n} + d\sqrt{k} \\
\sigma_2 &: a + b\sqrt{m} + c\sqrt{n} + d\sqrt{k} \mapsto a - b\sqrt{m} + c\sqrt{n} - d\sqrt{k} \\
\sigma_3 &: a + b\sqrt{m} + c\sqrt{n} + d\sqrt{k} \mapsto a + b\sqrt{m} - c\sqrt{n} - d\sqrt{k} \\
\sigma_4 &: a + b\sqrt{m} + c\sqrt{n} + d\sqrt{k} \mapsto a - b\sqrt{m} - c\sqrt{n} + d\sqrt{k}
\end{aligned}$$

Now using previous theorem

Case 1 $m \equiv 3 \pmod 4$, $\quad n \equiv k \equiv 2 \pmod 4$

$$\operatorname{disc}\left(1,\sqrt{m},\sqrt{n},\frac{\sqrt{n}+\sqrt{k}}{2}\right)=\begin{vmatrix}\sigma_1\left(1\right) & \sigma_1\left(\sqrt{m}\right) & \sigma_1\left(\sqrt{n}\right) & \sigma_1\left(\frac{\sqrt{n}+\sqrt{k}}{2}\right)\\ \sigma_2\left(1\right) & \sigma_2\left(\sqrt{m}\right) & \sigma_2\left(\sqrt{n}\right) & \sigma_2\left(\frac{\sqrt{n}+\sqrt{k}}{2}\right)\\ \sigma_3\left(1\right) & \sigma_3\left(\sqrt{m}\right) & \sigma_3\left(\sqrt{n}\right) & \sigma_3\left(\frac{\sqrt{n}+\sqrt{k}}{2}\right)\\ \sigma_4\left(1\right) & \sigma_4\left(\sqrt{m}\right) & \sigma_4\left(\sqrt{n}\right) & \sigma_4\left(\frac{\sqrt{n}+\sqrt{k}}{2}\right)\end{vmatrix}^2$$

$$=\begin{vmatrix}1 & \sqrt{m} & \sqrt{n} & \frac{\sqrt{n}+\sqrt{k}}{2}\\ 1 & -\sqrt{m} & \sqrt{n} & \frac{\sqrt{n}-\sqrt{k}}{2}\\ 1 & \sqrt{m} & -\sqrt{n} & \frac{-\sqrt{n}-\sqrt{k}}{2}\\ 1 & -\sqrt{m} & -\sqrt{n} & \frac{-\sqrt{n}+\sqrt{k}}{2}\end{vmatrix}^2$$

$$=\left(8\sqrt{mnk}\right)^2=64mnk$$

Case 2 $m\equiv 1 \pmod 4, \quad n\equiv k\equiv 2,3 \pmod 4$

$$\operatorname{disc}\left(1,\frac{1+\sqrt{m}}{2},\sqrt{n},\frac{\sqrt{n}+\sqrt{k}}{2}\right)=\begin{vmatrix}\sigma_1(1) & \sigma_1\left(\frac{1+\sqrt{m}}{2}\right) & \sigma_1\left(\sqrt{n}\right) & \sigma_1\left(\frac{\sqrt{n}+\sqrt{k}}{2}\right)\\ \sigma_2(1) & \sigma_2\left(\frac{1+\sqrt{m}}{2}\right) & \sigma_2\left(\sqrt{n}\right) & \sigma_2\left(\frac{\sqrt{n}+\sqrt{k}}{2}\right)\\ \sigma_3(1) & \sigma_3\left(\frac{1+\sqrt{m}}{2}\right) & \sigma_3\left(\sqrt{n}\right) & \sigma_3\left(\frac{\sqrt{n}+\sqrt{k}}{2}\right)\\ \sigma_4(1) & \sigma_4\left(\frac{1+\sqrt{m}}{2}\right) & \sigma_4\left(\sqrt{n}\right) & \sigma_4\left(\frac{\sqrt{n}+\sqrt{k}}{2}\right)\end{vmatrix}^2$$

$$=\begin{vmatrix}1 & \frac{1+\sqrt{m}}{2} & \sqrt{n} & \frac{\sqrt{n}+\sqrt{k}}{2}\\ 1 & \frac{1-\sqrt{m}}{2} & \sqrt{n} & \frac{\sqrt{n}-\sqrt{k}}{2}\\ 1 & \frac{1+\sqrt{m}}{2} & -\sqrt{n} & \frac{-\sqrt{n}-\sqrt{k}}{2}\\ 1 & \frac{1-\sqrt{m}}{2} & -\sqrt{n} & \frac{-\sqrt{n}+\sqrt{k}}{2}\end{vmatrix}^2$$

$$=\left(4\sqrt{mnk}\right)^2=16mnk$$

Case 3 $m\equiv n\equiv k\equiv 1 \pmod 4$

$$\operatorname{disc}\left(1,\frac{1+\sqrt{m}}{2},\frac{1+\sqrt{n}}{2},\left(\frac{1+\sqrt{m}}{2}\right)\left(\frac{1+\sqrt{k}}{2}\right)\right)=\begin{vmatrix}\sigma_1\left(1\right) & \sigma_1\left(\frac{1+\sqrt{m}}{2}\right) & \sigma_1\left(\frac{1+\sqrt{n}}{2}\right) & \sigma_1\left(\left(\frac{1+\sqrt{m}}{2}\right)\left(\frac{1+\sqrt{k}}{2}\right)\right)\\ \sigma_2\left(1\right) & \sigma_2\left(\frac{1+\sqrt{m}}{2}\right) & \sigma_2\left(\frac{1+\sqrt{n}}{2}\right) & \sigma_2\left(\left(\frac{1+\sqrt{m}}{2}\right)\left(\frac{1+\sqrt{k}}{2}\right)\right)\\ \sigma_3\left(1\right) & \sigma_3\left(\frac{1+\sqrt{m}}{2}\right) & \sigma_3\left(\frac{1+\sqrt{n}}{2}\right) & \sigma_3\left(\left(\frac{1+\sqrt{m}}{2}\right)\left(\frac{1+\sqrt{k}}{2}\right)\right)\\ \sigma_4\left(1\right) & \sigma_4\left(\frac{1+\sqrt{m}}{2}\right) & \sigma_4\left(\frac{1+\sqrt{n}}{2}\right) & \sigma_4\left(\left(\frac{1+\sqrt{m}}{2}\right)\left(\frac{1+\sqrt{k}}{2}\right)\right)\end{vmatrix}^2$$

$$=\begin{vmatrix}1 & \frac{1+\sqrt{m}}{2} & \frac{1+\sqrt{n}}{2} & \left(\frac{1+\sqrt{m}}{2}\right)\left(\frac{1+\sqrt{k}}{2}\right)\\ 1 & \frac{1-\sqrt{m}}{2} & \frac{1+\sqrt{n}}{2} & \left(\frac{1-\sqrt{m}}{2}\right)\left(\frac{1-\sqrt{k}}{2}\right)\\ 1 & \frac{1+\sqrt{m}}{2} & \frac{1-\sqrt{n}}{2} & \left(\frac{1+\sqrt{m}}{2}\right)\left(\frac{1-\sqrt{k}}{2}\right)\\ 1 & \frac{1-\sqrt{m}}{2} & \frac{1-\sqrt{n}}{2} & \left(\frac{1-\sqrt{m}}{2}\right)\left(\frac{1+\sqrt{k}}{2}\right)\end{vmatrix}^2$$

$$=mnk$$

□

Chapter 3

Ideals of Ring of Integers

In 1876, Richard Dedekind extended applicability of Kummer's ideal numbers to ring of integers other than those defined by roots of unity, like $\mathbb{Z}[\sqrt{-5}]$ and hence ideals are also known as *Dedekind's ideals*[12]. In our discussion, $\mathbb{Q} \subset K \subset L$ are the number fields with prime ideals $\wp = \langle p \rangle = p\mathbb{Z}$, $\mathfrak{p}$ and $\mathfrak{P}$ of $\mathbb{Z}$, $\mathcal{O}_K$ and $\mathcal{O}_L$ respectively.

Definition 10 (Dedekind Domain). An integral domain R such that

1. Every ideal is finitely generated
2. Every non-zero prime ideal is a maximal ideal
3. R is integrally closed in its field of fractions

$$F = \left\{ \frac{\alpha}{\beta} : \alpha, \beta \in R, \beta \neq 0 \right\}$$

Remark 12. $\mathcal{O}_K$ is a Dedekind domian; see pp. 56, [1].

Remark 13. Every ideal in a Dedekind domain R is uniquely representable as a product of prime ideals. (pp. 59, [1])

Lemma 3. *If $\mathfrak{a}$ and $\mathfrak{b}$ are ideals in a Dedekind domain R, then $\mathfrak{a}|\mathfrak{b}$ iff $\mathfrak{b} \subset \mathfrak{a}$.*

Proof. One direction is trivial, $\mathfrak{a}|\mathfrak{b}$ implies $\mathfrak{b} \subset \mathfrak{a}$. Conversely, assuming $\mathfrak{b} \subset \mathfrak{a}$, fix $\mathfrak{c}$ such that $\mathfrak{ac}$ is principal (pp. 57, [1]), $\mathfrak{ac} = \langle \alpha \rangle$, for some $\alpha \in R$. Note that the set $\mathfrak{d} = \frac{1}{\alpha}\mathfrak{bc}$ is an ideal in R and that $\mathfrak{ad} = \mathfrak{b}$. □

Remark 14. From this lemma, we conclude that "multiple" means sub-ideal and "divisor" means larger ideal.

Definition 11 (Greatest common divisor of two ideals). It is the smallest ideal containing both the given ideals. Therefore, $\gcd(\mathfrak{a}, \mathfrak{b}) = \mathfrak{a} + \mathfrak{b}$.

Definition 12 (Least common multiple of two ideals). It is the largest ideal contained in both of the given ideals. Therefore, $\operatorname{lcm}(\mathfrak{a}, \mathfrak{b}) = \mathfrak{a} \cap \mathfrak{b}$.

Theorem 17. *Let $\mathfrak{a}$ be an ideal in a Dedekind domain R, and let α be any non-zero element of $\mathfrak{a}$. Then there exist $\beta \in \mathfrak{a}$ such that $\mathfrak{a} = \langle \alpha, \beta \rangle$.*

Proof. We will construct $\beta \in R$ such that $\mathfrak{a} = \gcd(\langle \alpha \rangle, \langle \beta \rangle)$. Then β will be obviously in $\mathfrak{a}$.

Let $\mathfrak{p}_1^{n_1}\mathfrak{p}_2^{n_2} \cdots \mathfrak{p}_r^{n_r}$ be the prime decomposition of $\mathfrak{a}$, where $\mathfrak{p}_i$ are distinct. Then $\langle \alpha \rangle$ is divisible by all $\mathfrak{p}_i^{n_i}$. Let $\mathfrak{q}_1, \mathfrak{q}_2, \ldots, \mathfrak{q}_s$ denote the other primes (if any) which divide $\langle \alpha \rangle$. We must construct β such that none of $\mathfrak{q}_j$ divide $\langle\beta\rangle$, and for each i, $\mathfrak{p}_i^{n_i}$ is the exact power of $\mathfrak{p}_i$ dividing $\langle\beta\rangle$. Equivalently,

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

We will use Chinese Remainder Theorem:

> Let $\mathfrak{a}_1, \mathfrak{a}_2, \dots, \mathfrak{a}_n$ be pairwise relatively prime ideals in a ring R. The the mapping
>
> $$R\Big/\bigcap_{i=1}^{n}\mathfrak{a}_i \mapsto R/\mathfrak{a}_1 \times \cdots R/\mathfrak{a}_n$$
>
> is an isomorphism. (pp. 253, [1])

Fix $\beta_i \in \mathfrak{p}_i^{n_i} - \mathfrak{p}_i^{n_i+1}$ which is necessarily non-empty by unique factorization) and let β satisfy the congruence

$$\begin{array}{rcll} \beta & \equiv & \beta_i \pmod{\mathfrak{p}_i^{n_i+1}} & i = 1, 2, \dots, r \\ \beta & \equiv & 1 \pmod{\mathfrak{q}_j} & j = 1, 2, \dots, s \end{array}$$

Such a β exists because the powers of $\mathfrak{p}_i$ and the $\mathfrak{q}_j$ are pairwise co-maximal (i.e. coprime), thus the sum of any two of them is R. □

Remark 15. Let K be a number field, $\mathfrak{a}$ be a non-zero ideal of $\mathcal{O}_K$. Then $|\mathcal{O}_K/\mathfrak{a}|$ divides $N_{\mathbb{Q}}^{K}(\alpha)$ for all $\alpha \in \mathfrak{a}$ and equality holds iff $\mathfrak{a} = \langle\alpha\rangle$

Definition 13 (Norm of ideal)**.** Let L be a number field lying over K such that L is a normal extension of K. Then $|\operatorname{Gal}(L/K)| = [L : K] = n$. For an ideal $\mathfrak{b}$ of $\mathcal{O}_L$ we define $N_K^L(\mathfrak{b})$ to be the ideal such that

$$N_K^L(\mathfrak{b}) = \mathcal{O}_K \bigcap \prod_{\sigma\in\operatorname{Gal}(L/K)} \sigma(\mathfrak{b})$$

Remark: Property of transitivity is satisfied by norm function. If $K \subset L \subset M$ are number fields then $N_K^M(\mathfrak{B}) = N_K^L(N_L^M(\mathfrak{B}))$ for and ideal $\mathfrak{B} \in \mathcal{O}_M$. (pp. 85, [1]).

Definition 14 (Lying over/Lying under)**.** Let $K \subset L$ be number fields. If $\mathfrak{p}$ and $\mathfrak{P}$ are prime ideals of $\mathcal{O}_K$ and $\mathcal{O}_L$ respectively, such that $\mathfrak{p} \subset \mathfrak{P}$ then we say that $\mathfrak{P}$ lies over $\mathfrak{p}$ or $\mathfrak{p}$ lies under $\mathfrak{P}$.

Remark 16. The prime ideals lying over a given prime ideal $\mathfrak{p}$ of $\mathcal{O}_K$ are the ones which occur in the prime decomposition of $\mathfrak{p}\mathcal{O}_L$, where $K \subset L$ are number fields. (pp. 63, [1])

Definition 15 (Ramification index)**.** The exponents with which the prime ideals lying over a given prime ideal $\mathfrak{p}$ of $\mathcal{O}_K$ occur in the prime decomposition of $\mathfrak{p}\mathcal{O}_L$ is called their ramification indices. For example, if $\mathfrak{p}\mathcal{O}_L = \mathfrak{P}_1^{e1} \cdots \mathfrak{P}_r^{e_r}$ then e_i is the ramification index of $\mathfrak{P}_i$ over $\mathfrak{p}$, denoted by $e(\mathfrak{P}_i/\mathfrak{p})$

Definition 16 (Inertial degree)**.** Let $K \subset L$ are number fields and $\mathfrak{p} \subset \mathfrak{P}$ are prime ideals in $\mathcal{O}_K$ and $\mathcal{O}_L$ respectively. Then the finite field $\mathcal{O}_L/\mathfrak{P}$ is an extension of finite degree f over the finite field $\mathcal{O}_K/\mathfrak{p}$. Here f is called the inertial degree of $\mathfrak{P}$ over $\mathfrak{p}$ and is denoted by $f(\mathfrak{P}/\mathfrak{p}) = [\mathcal{O}_L/\mathfrak{P} : \mathcal{O}_K/\mathfrak{p}]$.

When we write A/B where A, B are two algebraic structures, slash (/) imparts different meanings in different contexts. Some of them are:

- ◇ If B is a normal subgroup of A, then A/B represents a quotient group (read as: $A \mod B$)
- ◇ If B is an ideal of a ring A, then A/B represents a quotient ring (read as: $A \mod B$)
- ◇ If A and B are fields, then A/B represents that A is an field extension over B (read as: A over B) and if A is a Galois extension of B then $\mathrm{Gal}(A/B)$ represents the collection of automorphism of A which keep elements of B fixed.
- ◇ If A and B are prime ideals, then A/B represents that A lies over B (read as: A over B)
- ◇ If A and B are ring of integers of number fields, then A/B represents A lies over B (read as: A over B)

Lemma 4 (Multiplicative in towers)**.** *If $\mathfrak{p} \subset \mathfrak{P} \subset P$ are prime ideals of $\mathcal{O}_K \subset \mathcal{O}_L \subset \mathcal{O}_M$, then*

$$e(P/\mathfrak{p}) = e(P/\mathfrak{P})e(\mathfrak{P}/\mathfrak{p}) \quad \textit{and} \quad f(P/\mathfrak{p}) = f(P/\mathfrak{P})f(\mathfrak{P}/\mathfrak{p})$$

Proof. For ramification index, note that know that maximum exponents dividing the product of an ideal lying below it with the ring $\mathfrak{P}^{e(\mathfrak{P}/\mathfrak{p})}|\mathfrak{p}\mathcal{O}_L$, $P^{e(P/\mathfrak{P})}|\mathfrak{P}\mathcal{O}_M$ and $P^{e(P/\mathfrak{p})}|\mathfrak{p}\mathcal{O}_M$. Therefore we get (in terms of the maximum exponents)

$$\begin{aligned} & \left(P^{e(P/\mathfrak{P})}\right)^{e(\mathfrak{P}/\mathfrak{p})} \Big| \mathfrak{P}^{e(\mathfrak{P}/\mathfrak{p})}\mathcal{O}_M^{e(\mathfrak{P}/\mathfrak{p})} \\ \Rightarrow \quad & P^{e(P/\mathfrak{P})e(\mathfrak{P}/\mathfrak{p})} \Big| \mathfrak{p}\mathcal{O}_M \end{aligned}$$

since $\mathcal{O}_L \subset \mathcal{O}_M$ and multiplication of a ring by its sub-ring is the ring itself.

For inertial degree, note that $f(\mathfrak{P}/\mathfrak{p}) = [\mathcal{O}_L/\mathfrak{P} : \mathcal{O}_K/\mathfrak{p}]$, $f(P/\mathfrak{P}) = [\mathcal{O}_M/P : \mathcal{O}_L/\mathfrak{P}]$ and $f(P/\mathfrak{p}) = [\mathcal{O}_M/P : \mathcal{O}_K/\mathfrak{p}]$. From field theory we know that (for proof see pp. 523 of Dummit-Foote[1]).

$$[\mathcal{O}_M/P : \mathcal{O}_L/\mathfrak{P}][\mathcal{O}_L/\mathfrak{P} : \mathcal{O}_K/\mathfrak{p}] = [\mathcal{O}_M/P : \mathcal{O}_K/\mathfrak{p}]$$

□

Remark 17. Let $\mathfrak{p}$ be any prime ideal of $\mathcal{O}_K$, then $\mathfrak{p}$ lies over a unique prime ideal (pp. 63, [1]) $\wp = \langle p \rangle$ of $\mathbb{Z}$. Therefore, $\mathcal{O}_K/\mathfrak{p}$ is a field of order p^f, there $f = f(\mathfrak{p}/\wp)$.

Theorem 18. *Let $K \subset L$ are number fields and $n = [L : K]$. If $\mathfrak{P}_1, \ldots, \mathfrak{P}_r$ are the prime ideals of $\mathcal{O}_L$ lying over a prime ideal $\mathfrak{p}$ of $\mathcal{O}_K$ with $e_1, \ldots, e_r$ and $f_1, \ldots, f_r$ the corresponding ramification indices and inertial degrees then*

$$\sum_{i=1}^{r} e_i f_i = n$$

Proof. We have $\mathfrak{p}\mathcal{O}_L = \prod_{i=1}^{r} \mathfrak{P}_i^{e_i}$ and we know following result

[1] *Abstract Algebra.* John Wiley & Sons, Inc.

Let $K \subset L$ be number fields and $n = [L : K]$ then (pp. 66, [1])

(a) For ideals $\mathfrak{a}$ and $\mathfrak{b}$ of $\mathcal{O}_K$, $|\mathcal{O}_K/\mathfrak{a}\mathfrak{b}| = |\mathcal{O}_K/\mathfrak{a}|\,|\mathcal{O}_K/\mathfrak{b}|$

(b) Let $\mathfrak{a}$ be an ideal of $\mathcal{O}_K$. For an $\mathcal{O}_L$-ideal $\mathfrak{a}\mathcal{O}_L$, $|\mathcal{O}_L/\mathfrak{a}\mathcal{O}_L| = |\mathcal{O}_K/\mathfrak{a}|^n$

(c) Let $\alpha \in \mathcal{O}_K$, $\alpha \neq 0$. For the principal ideal $\langle\alpha\rangle$, $|\mathcal{O}_K/\langle\alpha\rangle| = \left|N_{\mathbb{Q}}^{K}(\alpha)\right|$

hence using (a) we get

$$|\mathcal{O}_L/\mathfrak{p}\mathcal{O}_L| = \left|\mathcal{O}_L/\prod_{i=1}^{r}\mathfrak{P}_i^{e_i}\right| = \prod_{i=1}^{r}|\mathcal{O}_L/\mathfrak{P}_i^{e_i}| = \prod_{i=1}^{r}|\mathcal{O}_L/\mathfrak{P}_i|^{e_i}$$

But by definition of inertial degree, we know that $|\mathcal{O}_L/\mathfrak{P}_i| = |\mathcal{O}_K/\mathfrak{p}|^{f_i}$, therefore

$$|\mathcal{O}_L/\mathfrak{p}\mathcal{O}_L| = \prod_{i=1}^{r}|\mathcal{O}_K/\mathfrak{p}|^{f_i e_i} = |\mathcal{O}_K/\mathfrak{p}|^{\sum_{i=1}^{r} e_i f_i}$$

Now using (b) we get

$$|\mathcal{O}_L/\mathfrak{p}\mathcal{O}_L| = |\mathcal{O}_K/\mathfrak{p}|^n$$

and the result follows. □

Theorem 19. *Let L be a normal extension of K and $\mathfrak{p}$ is a prime ideal of $\mathcal{O}_K$. Let $\mathfrak{P}$ and $\mathfrak{P}'$ be two prime ideals of $\mathcal{O}_L$ lying over the prime same prime $\mathfrak{p}$ of $\mathcal{O}_K$. Then $\sigma(\mathfrak{P}) = \mathfrak{P}'$ for some $\sigma \in \mathrm{Gal}(L/K)$.*

Proof. Clearly, the Galois group $\mathrm{Gal}(L/K)$ permutes the prime ideals lying over $\mathfrak{p}$. If $\mathfrak{P}$ lies over $\mathfrak{p}$ and $\sigma \in \mathrm{Gal}(L/K)$, then $\sigma(\mathfrak{P})$ is a prime ideal in $\sigma(\mathcal{O}_L) = \mathcal{O}_L$, lying over $\sigma(\mathfrak{p}) = \mathfrak{p}$. Here we wish to prove that the Galois group permutes them transitively.

On the contrary, suppose $\sigma(\mathfrak{P}) \neq \mathfrak{P}'$ for all $\sigma \in \mathrm{Gal}(L/K)$. Then by Chinese remainder theorem (stated in Theorem 17) there is a solution to the system of congruences

$$\begin{aligned} x &\equiv 0 \pmod{\mathfrak{P}'} \\ x &\equiv 1 \pmod{\sigma(\mathfrak{P})} \quad \text{for all } \sigma \in \mathrm{Gal}(L/K) \end{aligned}$$

Let $\alpha \in \mathcal{O}_L$ be such a solution, we have

$$N_K^L(\alpha) \in \mathcal{O}_K \cap \mathfrak{P}' = \mathfrak{p}$$

since one of the factors of $N_K^L(\alpha)$ is $\alpha \in \mathfrak{P}'$. On the other hand we have $\alpha \notin \sigma(\mathfrak{P})$ for each $\sigma \in \mathrm{Gal}(L/K)$, hence $\sigma^{-1}(\alpha) \notin \mathfrak{P}$. We can express $N_K^L(\alpha)$ as the product of all $\sigma^{-1}(\alpha)$, and since none of these are in prime ideal $\mathfrak{P}$, it follows that $N_K^L(\alpha) \notin \mathfrak{P}$. But we have already seen that $N_K^L(\alpha) \in \mathfrak{p} \subset \mathfrak{P}$. □

Corollary 3. *If L is normal over K and $\mathfrak{P}$ and $\mathfrak{P}'$ are two prime ideals lying over $\mathfrak{p}$, then $e(\mathfrak{P}/\mathfrak{p}) = e(\mathfrak{P}'/\mathfrak{p})$ and $f(\mathfrak{P}/\mathfrak{p}) = f(\mathfrak{P}'/\mathfrak{p})$.*

Proof. $e(\mathfrak{P}/\mathfrak{p}) = e(\mathfrak{P}'/\mathfrak{p})$ follows from the unique factorization property stated in Remark 13.

$f(\mathfrak{P}/\mathfrak{p}) = f(\mathfrak{P}'/\mathfrak{p})$ is obtained by establishing an isomorphism between $\mathcal{O}_L/\mathfrak{P}$ and $\mathcal{O}_L/\mathfrak{P}'$ □

Definition 17 (Ramified prime)**.** A prime ideal $\mathfrak{p}$ of $\mathcal{O}_K$ is said to be ramified in $\mathcal{O}_L$ (or in L) if and only if $e(\mathfrak{P}/\mathfrak{p}) > 1$ for some prime ideal $\mathfrak{P}$ of $\mathcal{O}_L$ lying over $\mathfrak{p}$.

Remark 18. A prime ideal $\wp = \langle p \rangle$ of $\mathbb{Z}$ is ramified in $\mathcal{O}_K$ iff $p|\operatorname{disc}(\mathcal{O}_K)$.

Definition 18 (Fractional ideal)**.** Let R be a Dedekind domain and F be its field of fractions. A fractional ideal $\mathfrak{f}$ of F is a set of form $\alpha\mathfrak{a}$, for some $\alpha \in F$ and some ideal $\mathfrak{a}$ of R.

Remark 19. Considering F as an $R-$module, $\mathfrak{f}$ is a fractional ideal iff it is a finitely generated submodule of F (pp. 92, [1]). Therefore, a fractional $R-$ideal is a full $R-$lattice in F (pp. 47, [6]).

Definition 19 (Inverse fractional ideal)**.** Let R be a Dedekind domain and F be its field of fractions. If $\mathfrak{f}$ is a fractional ideal of F, then the inverse fractional ideal $\mathfrak{f}^{-1}$ is defined as

$$\mathfrak{f}^{-1} = \{\alpha \in F : \alpha\mathfrak{f} \subset R\}$$

Remark 20. Note that $\mathfrak{f}\mathfrak{f}^{-1} = R$. Also, the fractional ideals of F form a free abelian group under multiplication. Equivalently, every fractional ideal of F is uniquely representable as a product of distinct prime ideals of R (pp. 92, [1] and pp. 47, [6]).

Definition 20 (Complementary fractional Ideal)**.** Let $K \subset L$ be number fields and $\mathfrak{f}$ is a fractional ideal of L, then the complementary fractional ideal $\mathfrak{f}^*$ is defined as

$$\mathfrak{f}^* = \{\alpha \in L : T_K^L(\alpha\mathfrak{f}) \subset \mathcal{O}_K\}$$

Remark 21. If we consider $\mathfrak{f}$ to be a fractional $\mathcal{O}_L-$ideal of L, then $\mathfrak{f}^*$ is an $\mathcal{O}_L-$submodule of L, which is an $R-$lattice. Thus $\mathfrak{f}^*$ is also a fractional $\mathcal{O}_L-$ideal of L. (pp. 60, [6])

Definition 21 (Different Ideal)**.** Let $K \subset L$ be number fields, then the different ideal $\operatorname{diff}(\mathcal{O}_L/\mathcal{O}_K)$ of $\mathcal{O}_L$ with respect to $\mathcal{O}_K$ is the inverse of the complement of $\mathcal{O}_L$.

$$\operatorname{diff}(\mathcal{O}_L/\mathcal{O}_K) = (\mathcal{O}_L^*)^{-1} = \{\alpha \in L : \alpha\mathcal{O}_L^* \subset \mathcal{O}_L\}$$

Remark 22. $\mathcal{O}_L$ is a fractional ideal of L and because $\mathcal{O}_L \subset \mathcal{O}_L^*$ the inverse of $\mathcal{O}_L^*$ is a fractional ideal inside $\mathcal{O}_L$, hence an ideal (or, what we may refer as *integral* ideal). Therefore, this is a special ideal of $\mathcal{O}_L$ which is divisible by exactly those prime ideals $\mathfrak{P}$ of $\mathcal{O}_L$ which are ramified over $\mathcal{O}_K$. Hence a generalization of Remark 18. (pp. 73, [1])

Definition 22 (Decomposition group)**.** Let K and L be number fields such that L is a normal extension of K. Then for each prime ideal $\mathfrak{P}$ of $\mathcal{O}_L$ lying over the prime ideal $\mathfrak{p}$ of $\mathcal{O}_K$ we define the decomposition group $D(\mathfrak{P}/\mathfrak{p})$ as

$$D(\mathfrak{P}/\mathfrak{p}) = \{\sigma \in \operatorname{Gal}(L/K) : \sigma(\mathfrak{P}) = \mathfrak{P}\}$$

Remark 23. From Corollary 3 we know that if there are r prime ideals $\mathfrak{P}_i$ of $\mathcal{O}_L$ lying over prime ideal $\mathfrak{p}$ of $\mathcal{O}_K$ then they all have same ramification index e and inertial degree f. Therefore, by Theorem 18 we conclude that $ref = n = [L : K] = |\operatorname{Gal}(L/K)|$.

Definition 23 (Inertia group)**.** Let K and L be number fields such that L is a normal extension of K. Then for each prime ideal $\mathfrak{P}$ of $\mathcal{O}_L$ lying over the prime ideal $\mathfrak{p}$ of $\mathcal{O}_K$ we define the inertia group $E(\mathfrak{P}/\mathfrak{p})$ as

$$E(\mathfrak{P}/\mathfrak{p}) = \{\sigma \in \operatorname{Gal}(L/K) : \sigma(\alpha) \equiv \alpha \pmod{\mathfrak{P}} \quad \text{for all } \alpha \in \mathcal{O}_L\}$$

Remark 24. Clearly $D(\mathfrak{P}/\mathfrak{p})$ and $E(\mathfrak{P}/\mathfrak{p})$ are subgroups of $\operatorname{Gal}(L/K)$. Also we can express decomposition group as

$$D(\mathfrak{P}/\mathfrak{p}) = \{\sigma \in \operatorname{Gal}(L/K) : \sigma(\alpha) \equiv 0 \pmod{\mathfrak{P}} \quad \text{iff} \quad \alpha \equiv 0 \pmod{\mathfrak{P}}\}$$

therefore $E(\mathfrak{P}/\mathfrak{p})$ is a normal subgroup of $D(\mathfrak{P}/\mathfrak{p})$. (pp. 114, [1])

Definition 24 (Decomposition field). Let L be a normal extension of K and a prime ideal $\mathfrak{P}$ of $\mathcal{O}_L$ lying over the prime ideal $\mathfrak{p}$ of $\mathcal{O}_K$. The fixed field of the decomposition group $D = D(\mathfrak{P}/\mathfrak{p})$ is called decomposition field as is denoted by L_D.

Definition 25 (Inertia Field). Let L be a normal extension of K and a prime ideal $\mathfrak{P}$ of $\mathcal{O}_L$ lying over the prime ideal $\mathfrak{p}$ of $\mathcal{O}_K$. The fixed field of the inertia group $E = E(\mathfrak{P}/\mathfrak{p})$ is called decomposition field as is denoted by L_E.

Theorem 20. *Let L be a normal extension of K and there be r prime ideals $\mathfrak{P}$ of $\mathcal{O}_L$ lying the over prime ideal $\mathfrak{p}$ of $\mathcal{O}_L$ with $e(\mathfrak{P}/\mathfrak{p}) = e$ and $f(\mathfrak{P}/\mathfrak{p}) = f$. If $D = D(\mathfrak{P}/\mathfrak{p})$ and $E = E(\mathfrak{P}/\mathfrak{p})$, then*

(a) $[L_D : K] = r$, $e(\mathfrak{P}_D/\mathfrak{p}) = 1$ *and* $f(\mathfrak{P}_D/\mathfrak{p}) = 1$

(b) $[L_E : L_D] = f$, $e(\mathfrak{P}_E/\mathfrak{P}_D) = 1$ *and* $f(\mathfrak{P}_E/\mathfrak{P}_D) = f$

(c) $[L : L_E] = e$, $e(\mathfrak{P}/\mathfrak{P}_E) = e$ *and* $f(\mathfrak{P}/\mathfrak{P}_E) = 1$

where $\mathfrak{P}_E$ and $\mathfrak{P}_D$, respectively are the unique prime ideals of the ring of integers of L_E and L_D lying under $\mathfrak{P}$.

Proof. I will give an outline of proof, for details see pp. 100, [1].

(a) By the fundamental theorem of Galois theory we know that $[L_D : K]$ is same as the index of D in $\mathrm{Gal}(L/K)$. So, prove that the index of D in $\mathrm{Gal}(L/K)$ is r. Notice that $\mathfrak{P}$ is the only prime ideal of $\mathcal{O}_L$ lying over $\mathfrak{P}_D$, since such primes are permuted transitively by $\mathrm{Gal}(L/L_D)$ (Theorem 19). Apply Theorem 18 to $[L : L_D] = e(\mathfrak{P}/\mathfrak{P}_D)f(\mathfrak{P}/\mathfrak{P}_D)$ and conclude that $e(\mathfrak{P}/\mathfrak{P}_D) = e$ and $f(\mathfrak{P}/\mathfrak{P}_D) = f$, implying that $e(\mathfrak{P}_D/\mathfrak{p}) = 1$ and $f(\mathfrak{P}_D/\mathfrak{p}) = 1$.

(b) Assume $f(\mathfrak{P}/\mathfrak{P}_E) = 1$ (we will prove it in next part), then together with $f(\mathfrak{P}_D/\mathfrak{p}) = 1$ this shows that $f(\mathfrak{P}_E/\mathfrak{P}_D) = f(\mathfrak{P}/\mathfrak{p}) = f$ (Lemma 4). Then by Theorem 18 we must have $[L_E : L_D] \geq f$, but since E is a normal subgroup of D (Remark 24), we have $[L_E : L_D] = |D/E| \leq f$, hence exactly f. Which implies that $e(\mathfrak{P}_E/\mathfrak{P}_D) = 1$.

(c) Let the ring of integers of L_D be $\mathcal{O}$, then we will show that the Galois group of $\mathcal{O}_L/\mathfrak{P}$ over $\mathcal{O}/\mathfrak{P}_E$ is trivial. This implies that $f(\mathfrak{P}/\mathfrak{P}_E) = 1$. Then we obtain $[L : L_E] = e$ and $e(\mathfrak{P}/\mathfrak{P}_E) = e$ by using Lemma 4.

□

Corollary 4. *If $D = D(\mathfrak{P}/\mathfrak{p})$ is a normal subgroup of $\mathrm{Gal}(L/K)$ then $\mathfrak{p}$ splits into r distinct primes in L_D. If $E = E(\mathfrak{P}/\mathfrak{p})$ is also normal in $\mathrm{Gal}(L/K)$ then each of them remains prime (i.e. inert) in L_E. Finally each one becomes e^{th} power in L.*

Remark 25. Normality condition on D is necessary. For example, if $L = \mathbb{Q}[\sqrt[3]{19}, \omega]$ where $\omega = e^{2\pi i/3}$. Then L is normal of degree 6 over $K = \mathbb{Q}$ with Galois group S_3 (group of permutations of three objects). Here $3\mathcal{O}_K$ doesn't split into three distinct prime ideals in any of the possible decomposition fields $\mathbb{Q}[\sqrt[3]{19}], \mathbb{Q}[\sqrt[3]{\omega 19}]$ and $\mathbb{Q}[\sqrt[3]{\omega^2 19}]$. In fact it is ramified in each since it splits into $\mathfrak{p}_1^2\mathfrak{p}_2$. (pp. 103, [1])

Theorem 21. *Let K be a number field, and let L and M be two extensions of K. Fix a prime ideal $\mathfrak{p}$ of K.*

(a) If $\mathfrak{p}$ is unramified in both L and M, then $\mathfrak{p}$ is unramified in the composite field LM.

(b) If $\mathfrak{p}$ splits completely in both L and M then $\mathfrak{p}$ splits completely in LM.

Proof. We will prove each part separately.

(a) Assuming that $\mathfrak{p}$ is unramified in L and M, let $\mathfrak{P}$ be any prime ideal of LM lying over $\mathfrak{p}$. We have to show that $e(\mathfrak{P}/\mathfrak{p}) = 1$. Let $\mathbb{F}$ be be any normal extension of K containing LM, and let $\mathfrak{P}'$ be any prime ideal of $\mathbb{F}$ lying over $\mathfrak{P}$. Thus, $\mathfrak{P}'$ also lies over $\mathfrak{p}$. Let $E = E(\mathfrak{P}'/\mathfrak{p})$ be the corresponding inertia group, so let $\mathbb{F}_E$ is the inertia field. From previous theorem we can deduce that (pp. 104, [1]) that $\mathbb{F}_E$ contains both L and M, since the primes $\mathfrak{P}' \cap \mathfrak{L}$ and $\mathfrak{P}' \cap M$ are necessarily unramified over $\mathfrak{p}$. Then $\mathbb{F}_E$ also contains LM, implying that $\mathfrak{P}' \cap LM = \mathfrak{P}$ is unramified over $\mathfrak{p}$.

(b) The proof is similar to what we did in (a), just replace inertia group E by decomposition group $D = D(\mathfrak{P}'/\mathfrak{p})$. Note that splitting completely in LM is equivalent to the condition $e(\mathfrak{P}/\mathfrak{p}) = f(\mathfrak{P}/\mathfrak{p}) = 1$ for every prime ideal $\mathfrak{P}$ of LM lying over $\mathfrak{p}$.

□

Definition 26 (Ramification group)**.** Let L be a normal extension of K and a prime ideal $\mathfrak{P}$ of $\mathcal{O}_L$ lying over the prime ideal $\mathfrak{p}$ of $\mathcal{O}_K$. Then for $m \geq 0$ we define ramification group as

$$V_m(\mathfrak{P}/\mathfrak{p}) = \{\sigma \in \mathrm{Gal}(L/K) : \sigma(\alpha) \equiv \alpha \pmod{\mathfrak{P}^{m+1}} \quad \text{for all } \alpha \in \mathcal{O}_L\}$$

Remark 26. $V_0(\mathfrak{P}/\mathfrak{p}) = E(\mathfrak{P}/\mathfrak{p})$ and the $V_m(\mathfrak{P}/\mathfrak{p})$ form a descending chain of normal subgroups of $D(\mathfrak{P}/\mathfrak{p})$. (pp. 121, [1])

Definition 27 (Frobenius automorphism)**.** Let K and L be number fields such that L is a normal extension of K. Then for each prime ideal $\mathfrak{P}$ of $\mathcal{O}_L$ lying over the prime ideal $\mathfrak{p}$ of $\mathcal{O}_K$ we define the Frobenius automorphism of $\mathfrak{P}$ over $\mathfrak{p}$, $\psi(\mathfrak{P}/\mathfrak{p}) \in D(\mathfrak{P}/\mathfrak{p})$ as

$$\psi(\alpha) \equiv \alpha^{|\mathcal{O}_K/\mathfrak{p}|} \pmod{\mathfrak{P}}$$

for all $\alpha \in \mathcal{O}_L$.

Theorem 22. *Let L be a normal extension of K and $\mathfrak{p}$ be a prime ideal of K which is unramified in L. For each prime ideal $\mathfrak{P}$ of L lying over $\mathfrak{p}$ there is a unique Frobenius automorphism $\psi(\mathfrak{P}/\mathfrak{p}) \in \mathrm{Gal}(L/K)$ such that*

$$\psi(\alpha) \equiv \alpha^{|\mathcal{O}_K/\mathfrak{p}|} \pmod{\mathfrak{P}}$$

for all $\alpha \in \mathcal{O}_L$. When $\mathrm{Gal}(L/K)$ is abelian $\psi(\mathfrak{P}/\mathfrak{p})$ depends only on $\mathfrak{p}$, and

$$\psi(\alpha) \equiv \alpha^{|\mathcal{O}_K/\mathfrak{p}|} \pmod{\mathfrak{p}\mathcal{O}_L}$$

for all $\alpha \in \mathcal{O}_L$.

Proof. Assuming that $\mathfrak{p}$ is unramified in L, $\psi(\mathfrak{P}/\mathfrak{p})$ is the only element in $D(\mathfrak{P}/\mathfrak{p})$ with this property, and in fact the only element in $\mathrm{Gal}(L/K)$. Also note that

$$\psi(\sigma\mathfrak{P}/\mathfrak{p}) = \sigma\psi(\mathfrak{P}/\mathfrak{p})\sigma^{-1}$$

for each $\sigma \in \mathrm{Gal}(L/K)$. Since all prime ideals lying over $\mathfrak{p}$ are of this form, we conclude that the conjugacy class of the element $\psi(\mathfrak{P}/\mathfrak{p})$ is uniquely determined by $\mathfrak{p}$.

When G is abelian $\psi(\mathfrak{P}/\mathfrak{p})$ itself is uniquely determined by the unramified prime ideal $\mathfrak{p}$. This $\psi(\mathfrak{P}/\mathfrak{p})$ satisfies the same congruence for all $\mathfrak{P}$, hence it satisfies

$$\psi(\alpha) \equiv \alpha^{|\mathcal{O}_K/\mathfrak{p}|} \pmod{\mathfrak{p}\mathcal{O}_L}$$

□

3.1 Cyclotomic Integer Rings

Theorem 23. *Let $K = \mathbb{Q}[\zeta_m]$ and fix a prime $p \in \mathbb{Z}$ with $\wp = \langle p \rangle$ be the corresponding prime ideal of $\mathbb{Z}$. If $\mathfrak{P}_1, \ldots, \mathfrak{P}_r$ be the distinct prime ideals of $\mathbb{Z}[\zeta_m]$ lying over $\wp$ then*

$$\wp\mathcal{O}_K = (\mathfrak{P}_1 \cdot \mathfrak{P}_2 \cdots \mathfrak{P}_r)^e$$

and each one of them has same inertial degree f. Moreover, if $m = p^k n$, where $p \nmid n$ then $e = \varphi(p^k)$ and f is the multiplicative order of $p \mod n$.

Proof. Since $K = \mathbb{Q}[\zeta_m]$ is a normal extension of $\mathbb{Q}$, using Corollary 3 we conclude that all prime ideals of $\mathbb{Z}[\zeta_m]$ have same ramification index and inertial degree over $\wp$.

Note that $\zeta_m = \zeta_{p^k n} = \zeta_{p^k}\zeta_n$. We will consider how $\wp$ splits in each of the fields $K_1 = \mathbb{Q}[\zeta_{p^k}]$ and $K_2 = \mathbb{Q}[\zeta_n]$, the result for $\mathbb{Q}[\zeta_m]$ will follow.

(A) How $\wp$ splits in $K_1 = \mathbb{Q}[\zeta_{p^k}]$

Case 1 $p \not| m$

Then $k = 0$ and therefore $K_1 = \mathbb{Q}[\zeta_{p^k}] = \mathbb{Q}$ and $e(\wp/\wp) = 1 = \varphi(p^0)$.

Case 2 $p | m$

We will use following fact:

> Let $\zeta_m = e^{2\pi i/m}$, m a positive integer. Then following holds (pp. 47, [1])
>
> (a) If k is relatively prime to m then $1 + \zeta_m + \ldots + \zeta_m^{k-1}$ is a unit in $\mathbb{Z}[\zeta_m]$.
>
> (b) Let $m = p^k$, p be a prime. Then $p = u(1 - \zeta_{p^k})^{\varphi(p^k)}$ where u is a unit in $\mathbb{Z}[\zeta_{p^k}]$. (see second claim of Theorem 7)

Using (b) we know that

$$p = u(1 - \zeta_{p^k})^{\varphi(p^k)}$$

where u is a unit in $\mathbb{Z}[\zeta_{p^k}]$. Also, $\langle 1 - \zeta_{p^k} \rangle^{\varphi(p^k)} = \wp = p\mathbb{Z}$. Since $\varphi(p^k)$ is the degree of K_1 over $\mathbb{Q}$, any further splitting of $\langle 1 - \zeta_{p^k} \rangle$ into primes would violate Theorem 18; thus $\langle 1 - \zeta_{p^k} \rangle$ must be a prime. Therefore, the principal ideal $\langle 1 - \zeta_{p^k} \rangle$ of $\mathbb{Z}[\zeta_{p^k}]$ is a prime ideal lying over $\wp$ and $e(\langle 1 - \zeta_{p^k} \rangle / \wp) = \varphi(p^k)$.

(B) How $\wp$ splits in $K_2 = \mathbb{Q}[\zeta_n]$

Case 1 $p \not| m$

Then $n = m$ and $K_2 = \mathbb{Q}[\zeta_n] = \mathbb{Q}[\zeta_m]$. Therefore this case is same as the next one, i.e. $p \nmid n$.

Case 2 $p | m$

We know that $\wp$ is unramifeid (Remark 18) since $p \nmid n$ and $\operatorname{disc}(\mathbb{Z}[\zeta_n])$ is a divisor of $n^{\varphi(n)}$ as seen in third claim of Theorem 7. Thus we have

$$\wp\mathcal{O}_{K_2} = \wp\mathbb{Z}[\zeta_n] = \mathfrak{p}_1 \cdot \mathfrak{p}_2 \cdots \mathfrak{p}_r$$

where $\mathfrak{p}_i$ are distinct primes of $\mathbb{Z}[\zeta_n]$, each with the same inertial degree f over $\wp$, and $rf = \varphi(n)$.

`Claim:` $f = f(\mathfrak{p}_i/\wp)$ *is the order of* $p \mod n$.

i. As stated in Remark 6, $\operatorname{Gal}(K_2/\mathbb{Q}) \cong \mathbb{Z}_n^*$ and an automorphism σ of K_2 corresponds to the congruence class $[a] \in \mathbb{Z}_n^*$ for $a \in \mathbb{Z}$ iff $\sigma(\zeta_n) = \zeta_n$. In particular, let σ denote the automorphism corresponding to $[p]$. Let $\langle \sigma \rangle$ denote the subgroup of $\operatorname{Gal}(K_2/\mathbb{Q})$ generated by σ. The order of the group $\langle \sigma \rangle$ is the same as the order of the element σ, which is same as the order of $p \mod n$.

ii. Fix any $\mathfrak{p} = \mathfrak{p}_i$, we denote the field $\mathbb{Z}[\zeta_n]/\mathfrak{p}$ has degree f over $\mathbb{Z}_p \cong \mathbb{Z}/p\mathbb{Z}$ since that was the definition of $f = f(\mathfrak{p}/\wp) = [\mathbb{Z}[\zeta_n]/\mathfrak{p} : \mathbb{Z}/p\mathbb{Z}]$. Consequently, the Galois group of $\mathbb{Z}[\zeta_n]/\mathfrak{p}$ over $\mathbb{Z}_p$, generated by the automorphism τ which sends every element to its p^{th} power. Hence the order of the group $\langle\tau\rangle$ is f.

iii. For every $a \in \mathbb{Z}$, $\sigma^a = 1$ iff $\zeta_n^{p^a} = \zeta_n$ and the latter holds iff $p^a \equiv 1 \pmod{n}$. On the other hand, $\tau^a = 1$ iff $\zeta_n^{p^a} \equiv \zeta_n \pmod{\mathfrak{p}}$. Suppose $\zeta_n^{p^a} \equiv \zeta_n \pmod{\mathfrak{p}}$. We can write $p^a \equiv b \pmod{n}$, $1 \leq b \leq n$. Then, $\zeta_n^{p^a} = \zeta_n^b$ and $\zeta_n^b \equiv \zeta_n \pmod{\mathfrak{p}}$. This implies $\zeta_n^{b-1} \equiv 1 \pmod{\mathfrak{p}}$ since ζ_n is a unit in $\mathbb{Z}[\zeta_n]$. As seen in third claim of Theorem 1, we have

$$n = (1-\zeta_n)(1-\zeta_n^2)\cdots(1-\zeta_n^{n-1})$$

This implies that if $b > 1$ then $n \in \mathfrak{p}$, but this is clearly impossible since $p \in \wp \subset \mathfrak{p}$ and $\gcd(n,p) = 1$. Therefore $b = 1$. This proves that if $\zeta_n^{p^a} \equiv \zeta_n \pmod{\mathfrak{p}}$ then $p^a \equiv 1 \pmod{n}$, which in turn implies that $\sigma^a = 1$ iff $\tau^a = 1$, for every $a \in \mathbb{Z}$. Hence proving that $\langle\sigma\rangle$ and $\langle\tau\rangle$ have the same order.

(C) Putting together the results for $\mathbb{Q}[\zeta_{p^k}]$ and $\mathbb{Q}[\zeta_n]$.

Fix primes $\mathfrak{P}_1, \ldots, \mathfrak{P}_r$ of $\mathbb{Z}[\zeta_m]$ lying over $\mathfrak{p}_1, \ldots, \mathfrak{p}_r$ respectively. All $\mathfrak{P}_i$ lie over $\wp$, hence all $\mathfrak{P}_i$ must lie over $\langle 1-\zeta_{p^k}\rangle$ of $\mathbb{Z}[\zeta_{p^k}]$, since we showed that $\langle 1-\zeta_{p^k}\rangle$ is the unique prime ideal of $\mathbb{Z}[\zeta_{p^k}]$ lying over $\wp$.

$$\begin{tikzcd}
 & \mathfrak{P}_i \arrow[dl, dash] \arrow[dr, dash] & \\
\langle 1-\zeta_{p^k}\rangle \arrow[dr, dash] & & \mathfrak{p}_i \arrow[dl, dash] \\
 & \wp &
\end{tikzcd}$$

Figure 3.1: Hasse diagram of the lattice of subideals

From this diagram we conclude that

$$\begin{aligned} e(\mathfrak{P}_i/\wp) &\geq e(\langle 1-\zeta_{p^k}\rangle/\wp) = \varphi(p^k) \\ f(\mathfrak{P}_i/\wp) &\geq f(\mathfrak{p}_i/\wp) = f \end{aligned}$$

Moreover, we have $rf = \varphi(n)$ and $\varphi(p^k)rf = \varphi(m)$. Then by Theorem 18, $\mathfrak{P}_i$ are the only prime ideals of $\mathbb{Z}[\zeta_m]$ lying over $\wp$ and equality must hold in the inequalities above. Therefore, $ref = \varphi(m)$. Thus completing the proof.

□

Corollary 5. *If $p \nmid m$, then $\wp$ splits into $\varphi(m)/f$ distinct prime ideals in $\mathbb{Z}[\zeta_m]$, where f is the order of $p \mod m$. Therefore*

$$\wp\mathcal{O}_K = \prod_{\ell=1}^{\frac{\phi(m)}{f}} \mathfrak{p}_\ell$$

where f is the lease positive integer such that $p^f \equiv 1 \pmod{m}$ and $\mathfrak{p}_\ell$ are prime ideals of $\mathcal{O}_K = \mathbb{Z}[\zeta_m]$ lying over $\wp$.

Theorem 24. *There exist prime integers p and q such that $\mathbb{Q}[\zeta_{pq}]$ contains a subfield K in which*

$$\wp\mathcal{O}_K = (\mathfrak{p}_1 \ldots \mathfrak{p}_r)^e$$

where $\mathfrak{p}_i$ are prime ideals of $\mathcal{O}_K$ lying over $\wp$ with inertial degree f.

Proof. We will prove this by giving necessary criterion for finding p and q satisfying given conditions.

Step 1 There exist primes p and q such that p splits into r disctinct primes in the $\mathbb{Q}[\zeta_q]$.

Given r, then by Corollary 5 such p, q exist because we can find f' such that it is the smallest positive integer satisfying $p^{f'} \equiv 1 \pmod q$ with $f' = \frac{\varphi(q)}{r} = \frac{q-1}{r}$. This is possible since by Fermat's little theorem, f' should be a factor of $q-1$ and this condition can be satisfied here.

Step 2 These p and q can be taken so that $\mathbb{Q}[\zeta_q]$ contains a subfield of degree rf over $\mathbb{Q}$.

From Corollary 4 we can conclude that

> Whenever L is normal over K with cyclic Galois group and $\mathfrak{p}$ (a prime ideal of K) splits into r prime ideals in L, then the decomposition field is the unique intermediate field of degree r over K, and $\mathfrak{p}$ splits into r prime in every intermediate field containing the decomposition field.(pp. 102, [1])

Since $\mathbb{Q}[\zeta_q]$ is normal extension of $\mathbb{Q}$, and by Remark 6 we know that the Galois group is cyclic, we can use this result. Also, $rf|\varphi(q)$ which implies that $rf \mid rf'$ or $f \mid f'$.

Step 3 We can ensure that the condition $p \equiv 1 \pmod e$ is satisfied.

We can choose p for step 1 by keeping this condition in mind, using generalized version of Chinese Remainder Theorem.

We will have to use following two theorems[a]

(a) Let $n_1, n_2, \ldots, n_k$ be positive integers, with $gcd(n_i, n_j) = 1$ whenever $i \neq j$, and let $a_1, a_2, \ldots, a_k$ be any integers. Then the solutions of simultaneous congruences, $x \equiv a_i \ (\mathrm{mod}\ n)_i$ for $1 \leq i \leq k$ form a single congruence class $\mod n$, where $n = n_1 \cdots n_k$.

(b) Let $n = n_1 \cdots n_k$ where the integers n_i are mutually coprime, and let $f(x)$ be a polynomial with integer coefficients. Suppose that for each $i = 1, \ldots, k$ there are N_i congruence classes $x \in \mathbb{Z}_n$, such that $f(x) \equiv 0 \pmod{n_i}$. Then there are $N = N_1 \ldots N_k$ classes $x \in \mathbb{Z}_n$ such that $f(x) \equiv \pmod n$.

[a] pp. 53 and 58 of Jones-Jones, "Elementary Number Theory." Springer Undergraduate Mathematics Series (1998).

Step 4 $\wp$ splits into r prime ideals, each with ramification index e and inertial degree f in a subfield of $\mathbb{Q}[\zeta_{pq}]$, where p and q satisfy above three conditions.

This follows from Theorem 23.

□

Remark 27. For $e = 2, f = 3, r = 5$, an example of such primes is $p = 29, q = 61$. (pp. 117, [1])

Theorem 25. *Let K be a subfield of $\mathbb{Q}[\zeta_m]$ and H be the subgroup of the $\mathbb{Z}_m^*$ fixing K pointwise. For a prime $p \in \mathbb{Z}$ not dividing m, if f is the least positive integer such that $[p^f] \in H$ where square brackets denote the congruence class $\mod m$ then $f = f(\mathfrak{p}/\wp)$ for any prime ideal $\mathfrak{p}$ of K lying over $\wp$.*

Proof. From Remark 6 we know that $\mathrm{Gal}(\mathbb{Q}[\zeta_m]/\mathbb{Q}) \cong \mathbb{Z}_m^*$. Note that K is a normal extension of $\mathbb{Q}$, hence we have Frobenius automorphism $\psi(\mathfrak{P}/\mathfrak{p})$

$$\psi(\alpha) \equiv \alpha^{|\mathbb{Z}/\wp|} \pmod{\mathfrak{p}}$$

for all $\alpha \in \mathcal{O}_K$. Note that, $f(\mathfrak{p}/\wp) = [\mathcal{O}_K/\mathfrak{p} : \mathbb{Z}/\wp] = [\mathcal{O}_K/\mathfrak{p} : \mathbb{Z}_p]$. Therefore $f(\mathfrak{p}/\wp)$ is the order of $\psi(\mathfrak{p}/\wp)$.

Moreover, $\mathbb{Q} \subset K \subset \mathbb{Q}[\zeta_m]$ where $\mathbb{Q}[\zeta_m]$ and K both are normal over $\mathbb{Q}$. If $\mathfrak{P}$ is some prime ideal of $\mathbb{Z}[\zeta_m]$ lying over $\mathfrak{p}$ then $\psi(\mathfrak{p}/\wp)$ is the restriction of $\psi(\mathfrak{P}/\wp)$ to K. (pp. 118, [1]). Therefore $\psi(\mathfrak{p}/\wp)$ has order equal to degree of $p \mod m$. Thus f is the order of $\psi(\mathfrak{p}/\wp)$. □

Theorem 26. *Let $K = \mathbb{Q}[\zeta_p]$, where p is an odd prime. If q is any prime different from p and d is a divisor of $p-1$ then q is a d^{th} power $\mod p$ iff q splits completely in a subfield $\mathbb{F}_d \subset K$ having degree d over $\mathbb{Q}$.*

Proof. From Remark 6 we know that $\mathrm{Gal}(K/\mathbb{Q}) \cong \mathbb{Z}_p^*$ is cyclic group of order $p-1$, hence there is a unique subfield $\mathbb{F}_d \subset K$ having degree d over $\mathbb{Q}$, for each divisor d of $p-1$. In fact, $\mathbb{F}_d$ is the fixed field of the unique subgroup of the Galois group having order $(p-1)/d$. Also, $\mathbb{F}_{d_1} \subset \mathbb{F}_{d_2}$ iff $d_1 \mid d_2$.

From Corollary 5 we know that q splits in r distinct primes in K, where $f = (p-1)/r$ is the order of q in the multiplicative group $\mathbb{Z}_p^*$. Since, $\mathbb{Z}_p^*$ is a cyclic group of order $p-1$, the d^{th} powers form the unique subgroup of order $(p-1)/d$, consisting of all elements whose orders divide $(p-1)/d$. Thus the following holds

$$\begin{aligned} q^f &\equiv 1 \pmod{p} && \text{(since } f \text{ is the order of } q \mod p) \\ q &\equiv x^d \pmod{p} && \text{for some } x \in \mathbb{Z} \\ q^{p-1} &\equiv 1 \pmod{p} && \text{(Fermat's Little Theorem (or) } p-1 \text{ is the order of } \mathbb{Z}_p^*) \end{aligned}$$

Therefore, $f = (p-1)/r$ divides $(p-1)/d$ implying that $d|r$. Hence $\mathbb{F}_d \subset \mathbb{F}_r$.

Observe that $\mathbb{F}_r$ is the decomposition field K_D corresponding to $D(\mathfrak{q}/q\mathbb{Z})$, where $\mathfrak{q}$ is any prime ideal of $\mathbb{O}_K$ lying over the ideal $q\mathbb{Z} = \langle q \rangle$. This is because the decomposition field must have degree r over $\mathbb{Q}$, and $\mathbb{F}_r$ is the only one. Thus by following result

> If $D(\mathfrak{P}/\mathfrak{p})$ is a normal subgroup of $\mathrm{Gal}(L/K)$, then $\mathfrak{p}$ splits completely in K' iff $K' \subset L_D$ (pp. 105, [1])

$\mathbb{F}_d \subset \mathbb{F}_r$ is equivalent to $q\mathbb{Z}$ splitting completely in $\mathbb{F}_d$. □

3.2 Real Cyclotomic Integer Rings

Theorem 27. *Let $K = \mathbb{Q}[\xi_m]$ with $\xi_m = \zeta_m + \zeta_m^{-1}$ and p be a rational prime such that $p \nmid m$ then*

$$\wp\mathcal{O}_K = \prod_{\ell=1}^{\frac{\phi(m)}{2f}} \mathfrak{p}_\ell$$

where the inertial degree f is the smallest positive integer satisfying $p^f \equiv \pm 1 \pmod{m}$ and $\mathfrak{p}_\ell$ are prime ideals of $\mathcal{O}_K = \mathbb{Z}[\xi_m]$ lying over $\wp$.

Proof. We will use Theorem 25. First of all, $H = \{[1], [-1]\}$ (which is not same as $\mathbb{Z}_3^\times$). Therefore, inertial degree f is the least positive integer such that $p^f \equiv \pm 1 \pmod{m}$.

Since $p \nmid m$, Corollary 5 implies that $e(\mathfrak{P}/\wp) = 1$ for any prime ideal $\mathfrak{P}$ of $\mathbb{Z}[\zeta_m]$ lying over $\wp$. Moreover, $\mathbb{Q}[\xi_m]$ is a subfield of $\mathbb{Q}[\zeta_m]$, hence we conclude that its ramification index is also 1.

As seen in proof of Theorem 9, $\mathbb{Q}[\zeta_m]$ has degree 2 over $\mathbb{Q}[\xi_m]$ and degree $\varphi(m)$ over $\mathbb{Q}$. Hence we conclude that $\mathbb{Q}[\xi_m]$ and degree $\frac{\phi(m)}{2}$ over $\mathbb{Q}$.

Let $\wp$ split into r distinct prime ideals $\mathfrak{p}_i$ of $\mathbb{Z}[\xi_m]$, then Theorem 18 implies that $fr = \frac{\phi(m)}{2}$ and we get $r = \frac{\phi(m)}{2f}$. □

3.3 Quadratic Integer Rings

Definition 28 (Legendre symbol)**.** Let p be an odd prime integer and n be another integer not divisible by p, then we define Legendre symbol $\left(\frac{n}{p}\right)$ as

$$\left(\frac{n}{p}\right) = \begin{cases} 1 & \text{if } x \text{ is quadratic residue} \mod p \\ -1 & \text{otherwise} \end{cases}$$

Definition 29 (Jacobi symbol)**.** For $a \in \mathbb{Z}$ and odd $b > 0$, such that $\gcd(a, b) = 1$, we define Jacobi symbol $\left(\frac{a}{b}\right)$ in terms of Legendre symbol as

$$\left(\frac{a}{b}\right) = \prod_{i=1}^{k} \left(\frac{a}{p_i}\right)^{r_i}$$

where $b = \prod_{i=1}^{k} p_i^{r_i}$ with p_i being odd primes.

Theorem 28. *Let $K = \mathbb{Q}[\sqrt{m}]$ where m is a square free integer and p be a prime integer.*

(a) If $p \mid m$ then $\wp\mathcal{O}_K = \langle p, \sqrt{m}\rangle^2$

(b) If $p = 2$ and m is odd then

$$\wp\mathcal{O}_K = \begin{cases} \langle 2, 1+\sqrt{m}\rangle^2 & \textit{if} \quad m \equiv 3 \pmod 4 \\ \langle 2, \frac{1+\sqrt{m}}{2}\rangle\langle 2, \frac{1-\sqrt{m}}{2}\rangle & \textit{if} \quad m \equiv 1 \pmod 8 \\ p\mathcal{O}_K & \textit{if} \quad m \equiv 5 \pmod 8 \end{cases}$$

(c) If p is odd and $p \nmid m$ then

$$\wp\mathcal{O}_K = \begin{cases} \langle p, n+\sqrt{m}\rangle\langle p, n-\sqrt{m}\rangle & \textit{if} \ \left(\frac{m}{p}\right) = 1 \quad \textit{with } m \equiv n^2 \pmod p \\ p\mathcal{O}_K & \textit{if} \ \left(\frac{m}{p}\right) = -1 \end{cases}$$

where $p\mathcal{O}_K = \{px : x \in \mathcal{O}_K\}$ just like[2] *$p\mathbb{Z} = px : x \in \mathbb{Z}$.*

Proof. Firstly, from Theorem 18 we conclude that there are only three possibilities:

$$\wp\mathcal{O}_K = \begin{cases} \mathfrak{p}^2 & \text{with} \quad f(\mathfrak{p}/\wp) = 1 \\ \mathfrak{p} & \text{with} \quad f(\mathfrak{p}/\wp) = 2 \\ \mathfrak{p}_1\mathfrak{p}_2 & \text{with} \quad f(\mathfrak{p}_1/\wp) = f(\mathfrak{p}_2/\wp) = 1 \end{cases}$$

Now we will prove all the cases separately:

(a) $\langle p, \sqrt{m}\rangle^2 = \langle p^2, p\sqrt{m}, m\rangle$. This is contained in $\wp\mathcal{O}_K$ since $p \mid m$. On the other hand, it contains the $\gcd(p^2, m)$, which is p; hence it contains $\wp\mathcal{O}_K$.

(b) We will consider all possibilities separately

[2] Coincidentally $p\mathbb{Z} = \langle p\rangle = \wp$, but every prime ideal is not a principal ideal.

(i) $m \equiv 3 \pmod 4$

We have, $\langle 2, 1+\sqrt{m}\rangle^2 = \langle 4, 1+m+2\sqrt{m}, 2(1+\sqrt{m})\rangle$. Note that 2 divides each one of the three factors. Now the result follows as in (a).

(ii) $m \equiv 1 \pmod 8$

We have, $\langle 2, \frac{1+\sqrt{m}}{2}\rangle\langle 2, \frac{1-\sqrt{m}}{2}\rangle = \langle 4, \frac{1-m}{4}, 1-\sqrt{m}, 1+\sqrt{m}\rangle$. Note that 2 divides each one of the four factors. Now the result follows as in (a).

(iii) $m \equiv 5 \pmod 8$

`Claim:` *If $\mathfrak{p}$ is any prime ideal of $\mathcal{O}_K$ lying over $\wp$, then $\mathcal{O}_K/\mathfrak{p}$ is not isomorphic to $\mathbb{Z}_2$.*

Consider the polynomial $x^2 - x + \frac{1-m}{4}$. Since $m \equiv 1 \pmod 4$, this has a root in $\mathcal{O}_K$ and hence a root in $\mathcal{O}_K/\mathfrak{p}$. But since $m \equiv 5 \pmod 8$ this polynomial reduces to $x^2 - x - 1 \mod 2$ which has no root in $\mathbb{Z}_2$. Therefore, $\mathcal{O}_K/\mathfrak{p}$ is not isomorphic to $\mathbb{Z}_2$.

Since our claim is true, $f = [\mathcal{O}_K/\mathfrak{p} : \mathbb{Z}_p] > 1$ and from our initial observations we conclude that $f = 2$.

(c) We will consider all possibilities separately

(i) $\left(\frac{m}{p}\right) = 1$

We have, $\langle p, n+\sqrt{m}\rangle\langle p, n-\sqrt{m}\rangle = \langle p^2, n^2-m, p(n-\sqrt{m}), p(n+\sqrt{m})\rangle$. Since $m \equiv n^2 \pmod p$, p divides each one of the four factors. Now the result follows as in (a).

(ii) $\left(\frac{m}{p}\right) = -1$

`Claim:` *If $\mathfrak{p}$ is any prime ideal of $\mathcal{O}_K$ lying over $\wp$, then $\mathcal{O}_K/\mathfrak{p}$ is not isomorphic to $\mathbb{Z}_p$.*

Consider the polynomial $x^2 - m$. This has a root in $\mathcal{O}_K$, hence a root in $\mathcal{O}_K/\mathfrak{p}$. But since m is not a quadratic residue $\mod p$, this has no root in $\mathbb{Z}_p$. Therefore, $\mathcal{O}_K/\mathfrak{p}$ is not isomorphic to $\mathbb{Z}_p$.

Since our claim is true, $f = [\mathcal{O}_K/\mathfrak{p} : \mathbb{Z}_p] > 1$ and from our initial observations we conclude that $f = 2$.

□

Theorem 29 (Quadratic Reciprocity Law[3]). *Let p be an odd prime in $\mathbb{Z}$, then*

$$\left(\frac{2}{p}\right) = \begin{cases} 1 & \text{if } p \equiv \pm 1 \pmod 8 \\ -1 & \text{if } p \equiv \pm 3 \pmod 8 \end{cases}$$

and for odd primes q different from p we have

$$\left(\frac{q}{p}\right) = \begin{cases} 1 & \text{if } p \text{ or } q \equiv 1 \pmod 4 \\ -1 & \text{if } p \equiv q \equiv 3 \pmod 4 \end{cases}$$

Proof. From second claim in proof of Theorem 12 we know that $\mathbb{Q}[\zeta_p]$ contains $\mathbb{Q}[\sqrt{p}]$ if $p \equiv 1 \pmod 4$ and $\mathbb{Q}[\sqrt{-p}]$ if $p \equiv 3 \pmod 4$. Therefore we can use Theorem 26 to conclude that for any prime number r, $\left(\frac{r}{p}\right) = 1$ iff $\langle r\rangle$ splits completely in $\mathbb{F}_2 = \mathbb{Q}[\sqrt{\pm p}]$. We restate the splitting conditions from Theorem 28 as

[3] This is claimed to be the theorem with second largest number of proofs, first being the Pythagorean Theorem. I discussed an elementary proof of this theorem in one of my earlier project reports (pp. 13, [21]).

$$\langle r\rangle\mathcal{O}_K \text{ splits in } \mathbb{Q}[\sqrt{p}] \text{ iff either } r = 2 \text{ and } p \equiv 1 \pmod 8 \text{ or } r = q \text{ and } \left(\frac{p}{q}\right) = 1.$$

Now to accommodate the $\mathbb{Q}[\sqrt{-p}]$ case simultaneously, consider following fact

$x^2 + 1 \equiv 0 \pmod p$ has a solution[a] iff $p \equiv 2, 1 \pmod 4$.

[a] $n^2+1 \equiv 0 \pmod p \Rightarrow p \equiv 2, 1 \pmod 4$ can be proved by contradiction, on the contrary assume that $p \equiv 3 \pmod 4$, hence $n^2 + 1 \equiv 3\ell \pmod 4$; using $\mod 2$ conclude that it should satisfy $n^2 + 1 \equiv 3 \pmod 4$ which is impossible. For $p \equiv 2, 1 \pmod 4 \Rightarrow n^2 + 1 \equiv 0 \pmod p$ use the fact that $\mathbb{Z}_p^*$ is cyclic group of order $p - 1$, see pp. 7 of [1]

From this, since p is odd, we conclude that $\left(\frac{-1}{p}\right) = 1$ iff $p \equiv 1 \pmod 4$. Also using definition of Legendre symbol, we can conclude that $\left(\frac{a}{p}\right)\left(\frac{b}{p}\right) = \left(\frac{ab}{p}\right)$ for a, b not divisible by p.

Note that $p \equiv 1 \pmod 4$ holds for $p \equiv 1, -3 \pmod 8$ and $p \equiv 3 \pmod 4$ holds for $p \equiv -1, 3 \pmod 8$. Now combining all this information the theorem follows for $r = 2$. When $p \equiv 1 \pmod 4$, $\mathbb{F}_2 = \mathbb{Q}[\sqrt{p}]$. The condition of splitting stated above implies that $\left(\frac{q}{p}\right) = 1 \iff \left(\frac{p}{q}\right) = 1$, hence is symmetrical in p and q and theorem follows in this case. □

3.4 Pure Cubic Integer Rings

Theorem 30. *Let $K = \mathbb{Q}[\sqrt[3]{m}]$ where m be a cubefree integer with $m = hk^2$ such that h and k are squarefree and relatively prime. Also, p be a rational prime with $\wp = \langle p\rangle$.*

(a) If $p \neq 3$ and $p \nmid m$ then the prime decomposition of $\wp\mathcal{O}_K$ can be determined by factoring $x^3 - m \mod p$.

(b) If $p \neq 3$ and $p \mid m$ then $\wp\mathcal{O}_K = \mathfrak{p}^3$

(c) If $p = 3$ then then

$$\wp\mathcal{O}_K = \begin{cases} \mathfrak{p}^3 & \textit{if} \quad m \not\equiv \pm 1 \pmod 9 \quad \textit{or} \quad h^2 \not\equiv k^2 \pmod 9 \\ \mathfrak{p}_1^2\mathfrak{p}_2 & \textit{if} \quad m \equiv \pm 1 \pmod 9 \quad \textit{or} \quad h^2 \equiv k^2 \pmod 9 \end{cases}$$

Proof. We will prove each part separately:

(a) We will use the following result:

Let L be a field extension of K with $n = [L : K]$. Fix an element $\alpha \in \mathcal{O}_L$ of degree n over K, such that $L = K[\alpha]$. Therefore, $\mathcal{O}_K[\alpha]$ is an additive subgroup of $\mathcal{O}_L$. Since $\mathcal{O}_K[\alpha]$ and $\mathcal{O}_L$ are free abelian groups of rank mn, where $m = [K : \mathbb{Q}]$, $\mathcal{O}_L/\mathcal{O}_K[\alpha]$ is necessarily finite (see second claim of Theorem 3).
Fix a prime ideal $\mathfrak{p}$ of $\mathcal{O}_K$ then if a polynomial $h \in \mathcal{O}_K[x]$, then $[h]$ denote the corresponding polynomial in $(\mathcal{O}_K/\mathfrak{p})\,[x]$ obtained by reducing the coefficients of $h \mod \mathfrak{p}$. Now fix a monic irreducible polynomial $g \in \mathcal{O}_K[x]$ for α. Then $[g]$ factors uniquely into monic irreducible factors in $(\mathcal{O}_K/\mathfrak{p})[x]$ and we can write

$$[g] = [g_1]^{e_1}[g_2]^{e_2}\cdots[g_r]^{e_r}$$

where g_i are monic polynomials over $\mathcal{O}_K$ and $[g_i]$ are distinct.
Let p be the prime of $\mathbb{Z}$ lying under $\mathfrak{p}$. If p doesn't divide $|\mathcal{O}_L/\mathcal{O}_K[\alpha]|$ then

$$\mathfrak{p}\mathcal{O}_L = \mathfrak{P}_1^{e_1}\mathfrak{P}_2^{e_2}\cdots\mathfrak{P}_r^{e_r}$$

where $\mathfrak{P}_i$ is the ideal $\langle \mathfrak{p}, g_i(\alpha)\rangle$ of $\mathcal{O}_L$. In other words, $\mathfrak{P}_i = \mathfrak{p}\mathcal{O}_L + \langle g_i(\alpha)\rangle$ with $f(\mathfrak{P}_i/\mathfrak{p})$ equal to the degree of g_i. (pp. 79, [1])

Here $p \neq 3$ and $p \nmid m$, therefore $p^2 \nmid \operatorname{disc}(\sqrt[3]{m})$ (Theorem 14). As seen in Theorem 3 and Theorem 13, this implies that p does not divide $|\mathcal{O}_K/\mathbb{Z}[\alpha]|$. Now $g(x) = x^3 - m$ is the irreducible monic polynomial for $\sqrt[3]{m}$, hence

$$\wp\mathcal{O}_K = \mathfrak{p}_1^{e_1}\mathfrak{p}_2^{e_2}\cdots\mathfrak{p}_r^{e_r}$$

where $\mathfrak{p}_i = \langle \wp, g_i(\sqrt[3]{m})\rangle$ and $f(\mathfrak{p}_i/\wp)$ equal to the degree of g_i. (then using Theorem 18 we can calculate e_i since r and f_i are known)

(b) Since $\gcd(h,k) = 1$, $p \mid m$ implies that $p \mid k$ or $p \mid h$.

Consider the case when $p \nmid k$. Let $\mathfrak{p}$ be the prime divisor of $\wp$ in $\mathcal{O}_K$. Let $\beta = \frac{\alpha^2}{k} = \sqrt[3]{h^2k}$ (see second claim of Theorem 13). Then $\mathfrak{p}$ divides $\langle h^2k\rangle = \langle \beta^3\rangle$ in $\mathcal{O}_K$, so that $\mathfrak{p}$ must divide $\langle\beta\rangle\mathcal{O}_K$. Then $\mathfrak{p}^3$ divides $\langle\beta^3\rangle = \langle h^2k\rangle$ in $\mathcal{O}_K$. Since $\gcd(h,k) = 1$ and hk is squarefree, we conclude that $h^2k = pb$ for some b not divisible by p. Then $\langle b\rangle\mathcal{O}_K$ is not divisible by $\mathfrak{p}$. Considering the prime decomposition of pb we deduce that $\mathfrak{p}^3$ divides $\wp$ in $\mathcal{O}_K$. Then from Theorem 18 it follows that $\wp\mathcal{O}_K = \mathfrak{p}^3$.

Alternatively, we can just show that $p \nmid |\mathcal{O}_K/\beta|$ and use the result stated in (a). Similarly, the claim holds for $p \nmid k$, just instead of β consider $\alpha = \sqrt[3]{hk^2}$.

(c) If $3 \mid hk$ then $h^2 \not\equiv k^2 \pmod 9$ since hk is squarefree. The desired conclusion then follows from (b), since we can use same argument when $p \mid h$, with β replaced by $\alpha = hk^2$.

Assume that $3 \nmid hk$. We have following result

Let K be a number field of degree n over $\mathbb{Q}$ and $\alpha_1, \ldots, \alpha_n \in K$. (pp. 86, [1])

(i) $\operatorname{disc}_{\mathbb{Q}}^{K}(r\alpha_1, \alpha_2, \ldots, \alpha_n) = r^2 \operatorname{disc}(\alpha_1, \alpha_2, \ldots, \alpha_n)$ for all $r \in \mathbb{Q}$.

(ii) Let β be a linear combination of $\alpha_1, \ldots, \alpha_n$ with coefficients in $\mathbb{Q}$. Then

$$\operatorname{disc}_{\mathbb{Q}}^{K}(\alpha_1 + \beta, \alpha_2, \ldots, \alpha_n) = \operatorname{disc}_{\mathbb{Q}}^{K}(\alpha_1, \ldots, \alpha_n)$$

Let $\gamma = (\alpha - 1)^2/3$, then using above result along with third claim of proof of Theorem 13 we conclude that $\operatorname{disc}_{\mathbb{Q}}^{K}(\gamma) = 4\operatorname{disc}_{\mathbb{Q}}^{K}(\mathcal{O}_K)$. Now, using this with the result stated in (a) we can always compute the factors for $m \equiv \pm 1 \pmod 9$ except possible when $m \equiv \pm 8 \pmod{27}$. But $9 \nmid \mathrm{disc}_{\mathbb{Q}}^{K}(\mathcal{O}_K)$ when $m \equiv \pm 1 \pmod 9$. Finally, using Remark 18, we conclude that $\wp\mathcal{O}_K$ is not the cube of a prime ideal and in fact $\wp\mathcal{O}_K = \mathfrak{p}_1^2\mathfrak{p}_2$. (pp. 89, [1])

□

3.5 Octet Integer Rings

In this section we will discuss the normal closure of pure quartic field (pp. 41, [1]). Let $m \in \mathbb{Z}$, and assume that m is not a square. Then $K = \mathbb{Q}[\sqrt[4]{m}]$ has degree 4 over $\mathbb{Q}$ and $L = \mathbb{Q}[\sqrt[4]{m}, i]$ is its normal closure over $\mathbb{Q}$. The roots of $x^4 - m$ are denoted by the alphabets as $a = \sqrt[4]{m}, b = i\sqrt[4]{m}, c = -\sqrt[4]{m}$ and $d = -i\sqrt[4]{m}$. Now we can represent the Galois group $\mathrm{Gal}(L/\mathbb{Q})$ as permutations of a, b, c, d.

$L = \mathbb{Q}[i][\sqrt[4]{m}]$ is an extension of $\mathbb{Q}[i]$ of degree 4. The four conjugates of $\sqrt[4]{m}$ over $\mathbb{Q}[i]$ are a, b, c, d. Any element of $\mathrm{Gal}(L/\mathbb{Q}[i])$ is determined completely by knowing to which a, b, c, d the element sends $\sqrt[4]{m}$. Let σ be a permutation which maps a to b. Then we have:

$$\begin{aligned}
\sigma(a) &= b \\
\sigma(b) &= \sigma(ia) = i\sigma(a) = ib = c \\
\sigma(c) &= \sigma(-a) = -\sigma(a) = -b = d \\
\sigma(d) &= \sigma(-ia) = -i\sigma(a) = -ib = a
\end{aligned}$$

Therefore, $\sigma = (a, b, c, d)$ and $\mathrm{Gal}(L/\mathbb{Q}[i]) = \{1, \sigma, \sigma^2, \sigma^3\}$.

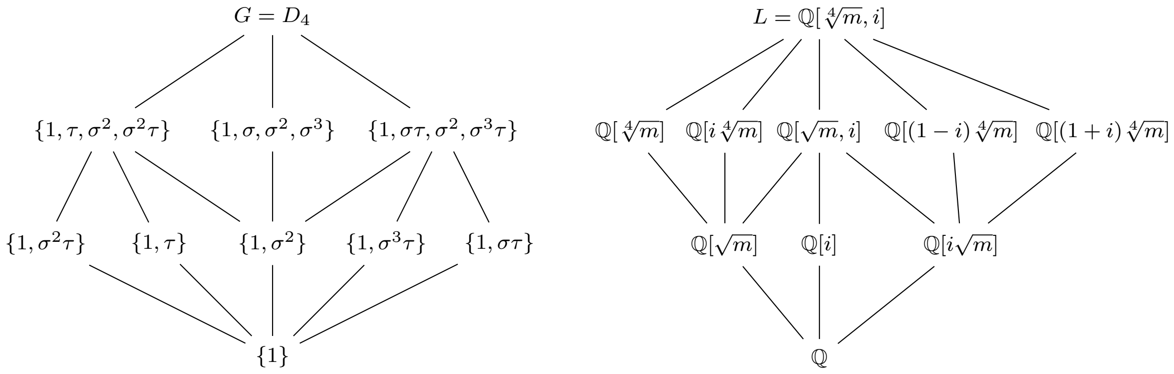
$L = \mathbb{Q}[\sqrt[4]{m}][i]$ is an extension of $K = \mathbb{Q}[\sqrt[4]{m}]$ of degree 2. Since this is normal quadratic extension, we know that the permutation map τ is conjugation map. Therefore, $\tau = (b, d)$ and $\mathrm{Gal}(L/K) = \{1, \tau\}$.

Since τ and σ are independent we conclude that

$$G = \mathrm{Gal}(L/\mathbb{Q}) = \{1, \sigma, \sigma^2, \sigma^3, \tau, \sigma\tau, \sigma^2\tau, \sigma^3\tau\} \cong D_4$$

where D_4 is the Dihedral group of order 8.

We can use this to illustrate *Fundamental Theorem of Galois Theory*


$G = D_4$
$\{1, \tau, \sigma^2, \sigma^2\tau\}$
$\{1, \sigma, \sigma^2, \sigma^3\}$
$\{1, \sigma\tau, \sigma^2, \sigma^3\tau\}$
$\{1, \sigma^2\tau\}$
$\{1, \tau\}$
$\{1, \sigma^2\}$
$\{1, \sigma^3\tau\}$
$\{1, \sigma\tau\}$
$\{1\}$
$L = \mathbb{Q}[\sqrt[4]{m}, i]$
$\mathbb{Q}[\sqrt[4]{m}]$
$\mathbb{Q}[i\sqrt[4]{m}]$
$\mathbb{Q}[\sqrt{m}, i]$
$\mathbb{Q}[(1-i)\sqrt[4]{m}]$
$\mathbb{Q}[(1+i)\sqrt[4]{m}]$
$\mathbb{Q}[\sqrt{m}]$
$\mathbb{Q}[i]$
$\mathbb{Q}[i\sqrt{m}]$
$\mathbb{Q}$

(a) The Hasse diagram of the lattice of subgroups of $\mathrm{Gal}(L/\mathbb{Q}) \cong D_4$

(b) The Hasse diagram of the lattice of subfields of L

Figure 3.2: Note that the subgroup and subfield lattices are in opposite direction, since the containment of fixed fields is opposite to the containment of corresponding Galois groups

Theorem 31. *Let $K = \mathbb{Q}[\sqrt[4]{m}, i]$ where $i = \sqrt{-1}$, $m \in \mathbb{Z}$ and m is not a square. Suppose p is an odd prime not dividing m. Prove that $\wp$ is unramified in K.*

Proof. Since $K = \mathbb{Q}[\sqrt[4]{m}]\mathbb{Q}[i]$, we will use Theorem 21(a) to prove this theorem. All we need to prove is that $\wp$ is unramified in $L = \mathbb{Q}[\sqrt[4]{m}]$ and $M = \mathbb{Q}[i]$. We can refine the arguments for proof of Remark 18 to deduce that

Let $\alpha \in \mathcal{O}_K$, $K = \mathbb{Q}[\alpha]$ and f be any monic polynomial (not necessarily irreducible) over $\mathbb{Z}$ such that $f(\alpha) = 0$. if p is a prime such that $p \nmid N_{\mathbb{Q}}^{K}(f'(\alpha))$, then $\langle p \rangle = \wp$ is unramified in K (pp. 73, 43 of [1])

For $L = \mathbb{Q}[\sqrt[4]{m}]$, $f(x) = x^4 - m$, then $f'(x) = 4x^3$.

$$N_{\mathbb{Q}}^{K}(f'(\alpha)) = N_{\mathbb{Q}}^{K}(4\alpha^3) = 4^4 \left(N_{\mathbb{Q}}^{K}(\alpha)\right)^3 = 2^8(-m)^3 = -2^8 m^3$$

Now since p is odd and $p \nmid m$, $\wp$ is unramified in L.

For $M = \mathbb{Q}[i]$, $f(x) = x^2 + 1$, then $f(x) = 2x$.

$$N_{\mathbb{Q}}^{K}(f'(\alpha)) = N_{\mathbb{Q}}^{K}(2\alpha^3) = 2^2 N_{\mathbb{Q}}^{K}(\alpha) = 2^2$$

Now since p is odd, $\wp$ is unramified in M. □

Remark 28. We can prove more general result that this $\wp$ splits into three primes in pure quadratic field $\mathbb{Q}[\sqrt[4]{m}]$ by using Frobenius automorphism. (pp. 119, [1])

Chapter 4

The Two Groups

In this chapter we shall be concerned with the lattices over the ring of rational integers. Let K be a number field of degree n over $\mathbb{Q}$. Let $\sigma_1, \ldots, \sigma_r$ denote the embeddings of K in $\mathbb{R}$, and $\tau_1, \overline{\tau_1}, \ldots, \tau_s, \overline{\tau_s}$ denote the remaining embeddings of K in $\mathbb{C}$. Thus $r + 2s = n = [K : \mathbb{Q}]$. A mapping $K \to \mathbb{R}^n$ is then obtained by sending each $\alpha \in K$ to the $n-$tuple

$$(\sigma_1(\alpha), \ldots, \sigma_r(\alpha), \Re\tau_1(\alpha), \Im\tau_1(\alpha) \ldots \Re\tau_s(\alpha), \Im\tau_s(\alpha))$$

where $\Re$ and $\Im$ indicate the real and imaginary parts of the complex numbers.

Definition 30 (Fundamental parallelotope)**.** Let Λ be a $n-$dimensional lattice in $\mathbb{R}^n$ then fundamental paralleotope is the following subset

$$\mathbb{R}^n/\Lambda = \{a_1 v_1 + \ldots + a_n v_n : a_i \in [0, 1)\}$$

where $v_1, \ldots, v_n$ is any $\mathbb{Z}-$basis for Λ.

Theorem 32. *The mapping $K \to \mathbb{R}^n$ sends $\mathcal{O}_K$ to an $n-$dimensional lattice Λ_K. A fundamental parallelotope for this lattice has volume*

$$\operatorname{vol}(\mathbb{R}^n/\Lambda_K) = \frac{1}{2^s}\sqrt{|\operatorname{disc}(\mathcal{O}_K)|}$$

Proof. Fix an integral basis $\alpha_1, \alpha_2, \ldots, \alpha_n$ for $\mathcal{O}_K$, these generate $\mathcal{O}_K$ over $\mathbb{Z}$. Therefore their images in $\mathbb{R}^n$ generate Λ_K over $\mathbb{Z}$. We have to show that these images are linearly independent over $\mathbb{R}$. Let M be the $n \times n$ matrix whose i^{th} row consists of the image of α_i.

$$M = \begin{bmatrix} \sigma_1(\alpha_1) & \ldots & \sigma_r(\alpha_1) & \Re\tau_1(\alpha_1) & \Im\tau_1(\alpha_1) & \ldots & \Re\tau_s(\alpha_1) & \Im\tau_s(\alpha_1) \\ \vdots & \ddots & \vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\ \sigma_1(\alpha_n) & \ldots & \sigma_r(\alpha_n) & \Re\tau_1(\alpha_n) & \Im\tau_1(\alpha_n) & \ldots & \Re\tau_s(\alpha_n) & \Im\tau_s(\alpha_n) \end{bmatrix}$$

Now take determinant of this and use the fact that $\Re\tau_j(\alpha_i) = \frac{\tau_j(\alpha_i)+\overline{\tau_j}(\alpha_i)}{2}$ and $\Im\tau_j(\alpha_i) = \frac{\tau_j(\alpha_i)-\overline{\tau_j}(\alpha_i)}{2\sqrt{-1}}$ to get

$$\begin{aligned}
\det(M) =& \begin{vmatrix} \sigma_1(\alpha_1) & \ldots & \sigma_r(\alpha_1) & \frac{\tau_1(\alpha_1)+\overline{\tau_1}(\alpha_1)}{2} & \frac{\tau_1(\alpha_1)-\overline{\tau_1}(\alpha_1)}{2i} & \ldots & \frac{\tau_s(\alpha_1)+\overline{\tau_s}(\alpha_1)}{2} & \frac{\tau_s(\alpha_1)-\overline{\tau_s}(\alpha_1)}{2i} \\ \vdots & \ddots & \vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\ \sigma_1(\alpha_n) & \ldots & \sigma_r(\alpha_n) & \frac{\tau_1(\alpha_n)+\overline{\tau_1}(\alpha_n)}{2} & \frac{\tau_1(\alpha_n)-\overline{\tau_1}(\alpha_n)}{2i} & \ldots & \frac{\tau_s(\alpha_n)+\overline{\tau_s}(\alpha_n)}{2} & \frac{\tau_s(\alpha_n)-\overline{\tau_s}(\alpha_n)}{2i} \end{vmatrix} \\
=& \left(\tfrac{1}{2i}\right)^s \begin{vmatrix} \sigma_1(\alpha_1) & \ldots & \sigma_r(\alpha_1) & \tau_1(\alpha_1) & \tau_1(\alpha_1) - \overline{\tau_1}(\alpha_1) & \ldots & \tau_s(\alpha_1) & \tau_s(\alpha_1) - \overline{\tau_s}(\alpha_1) \\ \vdots & \ddots & \vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\ \sigma_1(\alpha_n) & \ldots & \sigma_r(\alpha_n) & \tau_1(\alpha_n) & \tau_1(\alpha_n) - \overline{\tau_1}(\alpha_n) & \ldots & \tau_s(\alpha_n) & \tau_s(\alpha_n) - \overline{\tau_s}(\alpha_n) \end{vmatrix} \\
=& \left(\frac{1}{2i}\right)^s \begin{vmatrix} \sigma_1(\alpha_1) & \ldots & \sigma_r(\alpha_1) & \tau_1(\alpha_1) & -\overline{\tau_1}(\alpha_1) & \ldots & \tau_s(\alpha_1) & -\overline{\tau_s}(\alpha_1) \\ \vdots & \ddots & \vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\ \sigma_1(\alpha_n) & \ldots & \sigma_r(\alpha_n) & \tau_1(\alpha_n) & -\overline{\tau_1}(\alpha_n) & \ldots & \tau_s(\alpha_n) & -\overline{\tau_s}(\alpha_n) \end{vmatrix} \\
=& \frac{1}{2^s}\sqrt{|\operatorname{disc}(\mathcal{O}_K)|} = \operatorname{vol}(\mathbb{R}^n/\Lambda_K)
\end{aligned}$$

Since the determinant is non-zero, the images in $\mathbb{R}^n$ are independent over $\mathbb{R}$. □

Corollary 6. *The image of K is dense in $\mathbb{R}^n$.*

Definition 31 (Norm on $\mathbb{R}^n$)**.** For each point $\mathbf{x} = \underline{\underline{x}} = (x_1, \ldots, x_n) \in \mathbb{R}^n$ set

$$\mathcal{N}(\mathbf{x}) = x_1 \cdot x_2 \cdots x_r(x_{r+1}^2 + x_{r+2}^2) \cdots (x_{n-1}^2 + x_n^2)$$

Remark 29. If $\alpha \in \mathcal{O}_K$ maps to $\mathbf{x} \in \Lambda_K$, then $\mathcal{N}(\mathbf{x}) = N_{\mathbb{Q}}^K(\alpha)$.

Theorem (Minkowski's convex body theorem)**.** *Let Λ be an $n-$dimensional lattice in $\mathbb{R}^n$ and let E be a convex, Lebesgue measurable, centrally symmetric subset of $\mathbb{R}^n$ such that*

$$\mathrm{vol}(E) > 2^n \,\mathrm{vol}(\mathbb{R}^n/\Lambda)$$

Then E contains some non-zero point in Λ. If E is also compact, then equality can also hold and $>$ can be weakened to $\geq$.

For proof see Theorem 2.2.1 of [22].

Corollary 7. *Suppose $A \subset \mathbb{R}^n$ is a compact, convex and centrally symmetric set with $\mathrm{vol}(A) > 0$. If $\mathbf{a} \in A$ implies that $|\mathcal{N}(\mathbf{a})| \leq 1$, then every $n-$dimensional lattice Λ contains a non-zero point $\mathbf{x}$ with*

$$|\mathcal{N}(\mathbf{x})| \leq \frac{2^n}{\mathrm{vol}(A)} \,\mathrm{vol}(\mathbb{R}^n/\Lambda)$$

4.1 Ideal Class Group

We have already defined what do we mean by an *ideal class* and stated the fact that ideal classes form a finite group in section 1.2. Now we will prove that ideals classes form a group and compute a bound for the size of the group formed by them. The proof for finiteness is based on the relation of size of quotient ring with inertial degree which is related to ideal factorization (pp. 132, [1]).

Theorem 33. *The ideal classes in a Dedekind domain form a group under multiplication.*

Proof. We know that ideal classes of Dedekind domain R are defined by equivalence relation $\sim$. Hence given two ideals $\mathfrak{a}$ and $\mathfrak{b}$ of R, $\mathfrak{a} \sim \mathfrak{b}$ if and only if $\alpha\mathfrak{a} = \beta\mathfrak{b}$ for some α, β in R.

Claim 1 Two ideals in R are isomorphic as $R-$modules iff they are in the same class.

Let $\mathfrak{a}$ and $\mathfrak{b}$ be two ideals in R belonging to same class. Therefore $\mathfrak{a} \sim \mathfrak{b}$ and $\alpha\mathfrak{a} = \beta\mathfrak{b}$ for some $\alpha, \beta \in R$. We can define an R-module isomorphism, $\rho : \mathfrak{a} \to \mathfrak{b}$ such that $\rho(a) = b$ if $\alpha a = \beta b$. Hence, $\mathfrak{a} \cong \mathfrak{b}$.

Let $\mathfrak{a}$ and $\mathfrak{b}$ be two ideals in R which are isomorphic. Let the $R-$module isomorphism be $\rho : \mathfrak{a} \to \mathfrak{b}$ hence for any $a_1, a_2 \in \mathfrak{a}$, $\rho(r \cdot a_1 + s \cdot a_2) = r \cdot \rho(a_1) + s \cdot \rho(a_2)$ for $r, s \in R$. Observe that for $\alpha \in \mathfrak{a}$, $\rho(\alpha) \in \mathfrak{b}$, we have

$$\rho(\alpha)\mathfrak{a} = \{\rho(\alpha)a : a \in \mathfrak{a}\} = \{\rho(\alpha a) : a \in \mathfrak{a}\} = \{\alpha\rho(a) : a \in \mathfrak{a}\} = \{\alpha b : b \in \mathfrak{b}\} = \alpha\mathfrak{b}$$

Therefore $\rho(\alpha)\mathfrak{a} = \alpha\mathfrak{b}$ and $\mathfrak{a} \sim \mathfrak{b}$.

Claim 2 If $\mathfrak{a}$ is an ideal of R and $\alpha\mathfrak{a}$ is principal for some $\alpha \in R$ then $\mathfrak{a}$ is principal. Therefore principal ideals form an ideal class.

Let $\alpha\mathfrak{a} = \langle k \rangle$, then $\alpha\mathfrak{a} = 1 \cdot \langle k \rangle$. Therefore, $\mathfrak{a} \sim \langle k \rangle$ and previous claim implies that $\mathfrak{a}$ and $\langle k \rangle$ are isomorphic as $R-$module. Hence $\mathfrak{a}$ is a principal ideal and principal ideals form an ideal class.

Claim 3 The ideal classes in R form a group iff for every ideal $\mathfrak{a}$ there is an ideal $\mathfrak{b}$ such that $\mathfrak{a}\mathfrak{b}$ is principal.

Product of two ideal classes is obtained by selecting an ideal from each, multiplying them and taking the ideal class which contains the product ideal (product ideal is the set of all finite sums of elements of form ab with $a \in \mathfrak{a}$ and $b \in \mathfrak{b}$). The resulting ideal class doesn't depend on the particular ideal class chosen, but only on the two original ideal classes. Multiplied in this way, the ideal classes form a group. The identity element is the class C_0 consisting of all principal ideals. Therefore, for the existence of inverse it is necessary that for every ideal $\mathfrak{a}$ there is an ideal $\mathfrak{b}$ such that $\mathfrak{a}\mathfrak{b}$ is principal.

Claim 4 For every ideal $\mathfrak{a}$ of R there is an ideal $\mathfrak{b}$ of R such that $\mathfrak{a}\mathfrak{b}$ is principal.

Let α be any non-zero member of $\mathfrak{a}$ and let $\mathfrak{b} = \{\beta \in R : \beta\mathfrak{a} \subset \langle\alpha\rangle\}$. Then $\mathfrak{b}$ is easily seen to be an ideal (non-zero since $\alpha \in \mathfrak{b}$) and clearly $\mathfrak{a}\mathfrak{b} \subset \langle\alpha\rangle$. Now consider following two results (pp. 57, [1])

(a) In a Dedekind domain, every ideal contains a product of prime ideals.

(b) Let $\mathfrak{a}$ be a proper ideal in a Dedekind domain R with field of fractions F. Then there is an element $\gamma \in F\backslash R = F - R$ such that $\gamma\mathfrak{a} \subset R$.

Consider the set $\mathcal{A} = \frac{1}{\alpha}\mathfrak{a}\mathfrak{b}$. Note that $\mathcal{A} \subset R$ since $\mathfrak{a}\mathfrak{b} \subset \langle\alpha\rangle$ and is in fact an ideal. If $\mathcal{A} = R$ then $\mathfrak{a}\mathfrak{b} = \langle\alpha\rangle$ and we are done.

We will prove that $\mathcal{A}$ can't be a proper ideal of R. If $\mathcal{A}$ is a proper ideal then we can use (b) from the box above to conclude that $\gamma\mathcal{A} \subset R$ for some $\gamma \in F\backslash R$. Since R is integrally closed in field of fractions F, it is enough to show that γ is a root of a monic polynomial over R.

Observe that $\mathcal{A}$ contains $\mathfrak{b}$ since $\alpha \in \mathfrak{a}$. Thus $\gamma\mathfrak{b} \subset \gamma\mathcal{A} \subset R$. Since $\gamma\mathfrak{b}$ and $\gamma\mathcal{A}$ both are contained in R, it follows from the definition of $\mathfrak{b}$ that $\gamma\mathfrak{b} \subset \mathfrak{b}$. Now fix a finite generating set $\{\alpha_1, \ldots, \alpha_m\}$ for the ideal $\mathfrak{b}$ and using the relation $\gamma\mathfrak{b} \subset \mathfrak{b}$ we obtain following matrix equation

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

where M is an $m \times m$ matrix over R. By taking determinant we can obtain a monic polynomial over R having γ as a root. Hence completing the proof.

□

Remark 30. The ideal class group of R is isomorphic to the quotient group G/H, where G is the group of fractional ideals of F and H is the subgroup consisting of the principal ideals. (pp. 92, [1])

Theorem 34. *Every ideal class of $\mathcal{O}_K$ contains an ideal $\mathfrak{a}$ with*

$$|\mathcal{O}_K/\mathfrak{a}| \leq \frac{n!}{n^n}\left(\frac{4}{\pi}\right)^s \sqrt{|\operatorname{disc}(\mathcal{O}_K)|}$$

Proof. We will divide the proof in several parts

Claim 1. Every $n-$dimensional lattice Λ in $\mathbb{R}^n$ contains a non-zero point $\mathbf{x}$ with

$$|\mathcal{N}(\mathbf{x})| \leq \frac{n!}{n^n}\left(\frac{8}{\pi}\right)^s \operatorname{vol}(\mathbb{R}^n/\Lambda)$$

We will use Corollary 7, and hence define A as

$$A := \left\{\mathbf{x} = (x_1, \ldots, x_n) : |x_1| + \ldots + |x_r| + 2\left(\sqrt{x_{r+1}^2 + x_{r+2}^2} + \ldots + \sqrt{x_{n-1}^2 + x_n^2}\right) \leq n\right\}$$

This set is clearly centrally symmetric ($-\mathbf{x} \in A \Leftrightarrow \mathbf{x} \in A$) and compact (every open cover has finite subcover). To prove that this set is convex, let $\mathbf{x}, \mathbf{y} \in A$, then we can see that $\mathbf{z} = \frac{\mathbf{x}+\mathbf{y}}{2} \in A$ by using triangle inequality. Since choice of $\mathbf{x}$ and $\mathbf{y}$ was arbitrary, we conclude that A is a convex set. To prove $\mathbf{a} \in A \Rightarrow |\mathcal{N}(\mathbf{a})| \leq 1$, we will use *arithmetic-geometric mean* inequality. Note that geometric mean of coordinates of $\mathbf{a}$ is $\sqrt[n]{|\mathcal{N}(\mathbf{a})|}$ and arithmetic mean of coordinates of $\mathbf{a}$ is at most 1. Therefore,

$$\sqrt[n]{|\mathcal{N}(\mathbf{a})|} \leq 1 \quad \Rightarrow |\mathcal{N}(\mathbf{a})| \leq 1$$

Now we just need to prove that

$$\operatorname{vol}(A) = \frac{n^n}{n!}2^r\left(\frac{\pi}{2}\right)^s \tag{4.1}$$

We will prove this by induction. Let $V_{r,s}(t)$ denote the volume of the subset $\mathbb{R}^{r+2s}$ defined by

$$|x_1| + \ldots + |x_r| + 2\left(\sqrt{x_{r+1}^2 + x_{r+2}^2} + \ldots + \sqrt{x_{r+2s-1}^2 + x_{r+2s}^2}\right) \leq t$$

then

$$V_{r,s}(t) = t^{r+2s}V_{r,s}(1) \tag{4.2}$$

Now we will compute $V_{r,s}(1)$, if $r > 0$ then since it's centrally symmetric (instead of integration -1 to 1 we can integrate 0 to 1 twice) and using the relation between one dimensional Lebesgue measure and $n-$dimensional Lebesgue measure (note that along r we get linear/square regions).

$$\begin{aligned} V_{r,s}(1) &= 2\int_0^1 V_{r-1,s}(1-x)dx \\ &= 2\int_0^1 (1-x)^{r-1+2s}dxV_{r-1,s}(1) \qquad \text{(using (4.2))} \\ &= \frac{2}{r+2s}V_{r-1,s}(1) \end{aligned}$$

Applying this repeatedly we obtain

$$V_{r,s}(1) = \frac{2^{r-1}}{(r+2s)(r+2s-1)\cdots(2s+2)}V_{1,s}(1) \tag{4.3}$$

Now we need to determine $V_{0,s}(1)$ for $s > 0$ (note that along s we get disc/spherical regions)

$$V_{1,s}(1) = \int\int V_{1,s-1}(1 - 2\sqrt{x^2+y^2})dx\,dy$$

with the integral taken over the circular region $x^2+y^2 \leq 1/4$. Transforming to polar coordinates, put $x = k\cos(\theta), y = k\sin(\theta)$ and $dx\,dy = k\,dk\,d\theta$ where $0 \leq \theta \leq 2\pi$ and $0 \leq k \leq \frac{1}{2}$ to get

$$\begin{aligned}
V_{1,s}(1) &= \int_0^{\frac{1}{2}}\int_0^{2\pi} V_{1,s-1}(1-2k)k\,d\theta\,dk \\
&= \int_0^{\frac{1}{2}}\int_0^{2\pi} (1-2k)^{1+2(s-1)}k\,d\theta\,dk\,V_{1,s-1}(1) \qquad \text{(using (4.2))} \\
&= 2\pi\int_0^{\frac{1}{2}} (1-2k)^{2s-1}k\,dk\,V_{1,s-1}(1) \\
&= \frac{\pi}{2}\int_0^{1} c^{2s-1}(1-c)\,dc\,V_{1,s-1}(1) \qquad \text{(substitute } 1-2k=c\text{)} \\
&= \frac{\pi}{2}\times\frac{1}{2s(2s+1)}V_{1,s-1}(1)
\end{aligned}$$

Applying this repeatedly we obtain

$$V_{1,s}(1) = \left(\frac{\pi}{2}\right)^s \frac{1}{(2s+1)!}V_{1,0}(1) \tag{4.4}$$

Now $V_{1,0}(1) = 2$ i.e. length of the set $[-1,1]$ and we conclude that

$$V_{0,s}(1) = \left(\frac{\pi}{2}\right)^s \frac{2}{(2s+1)!}$$

Using this in (4.3) we obtain

$$V_{r,s}(1) = \frac{1}{(r+2s)!}2^r\left(\frac{\pi}{2}\right)^s = \frac{1}{n!}2^r\left(\frac{\pi}{2}\right)^s$$

Using this in (4.2) we obtain

$$V_{r,s}(t) = \frac{t^n}{n!}2^r\left(\frac{\pi}{2}\right)^s$$

Put $t = n$ to obtain (4.1).

Claim 2. Let $\mathfrak{b}$ be a non-zero ideal in $\mathcal{O}_K$, then

$$\operatorname{vol}(\mathbb{R}^n/\Lambda_{\mathfrak{b}}) = \frac{1}{2^s}\sqrt{|\operatorname{disc}(\mathcal{O}_K)|}\,|\mathcal{O}_K/\mathfrak{b}|$$

where $\Lambda_{\mathfrak{b}}$ is the image of $\mathfrak{b}$ in $\mathbb{R}^n$.

As seen in second claim of Theorem 3, taking square root both sides, if M is an n-dimensional sublattice of Λ then $\operatorname{vol}(\mathbb{R}^n/M) = |\Lambda/M|\operatorname{vol}(\mathbb{R}^n/\Lambda)$. Hence

$$\operatorname{vol}(\mathbb{R}^n/\Lambda_{\mathfrak{b}}) = |\Lambda_K/\Lambda_{\mathfrak{b}}|\operatorname{vol}(\mathbb{R}^n/\Lambda_K)$$

Using Theorem 32 and since $\mathfrak{b}$ is an ideal, we conclude that

$$\operatorname{vol}(\mathbb{R}^n/\Lambda_{\mathfrak{b}}) = \frac{1}{2^s}\sqrt{|\operatorname{disc}(\mathcal{O}_K)|}\,|\mathcal{O}_K/\mathfrak{b}|$$

Claim 3. Every non-zero ideal $\mathfrak{b}$ in $\mathcal{O}_K$ contains a non-zero element α with

$$N^K_{\mathbb{Q}}(\alpha) \leq \frac{n!}{n^n}\left(\frac{4}{\pi}\right)^s\sqrt{|\operatorname{disc}(\mathcal{O}_K)|}|\mathcal{O}_K/\mathfrak{b}|$$

This follows by using Remark 29 and second claim in first claim.

Given an ideal class C, consider the inverse class C^{-1} and fix any ideal $\mathfrak{b} \in C^{-1}$. We can obtain α as in third claim. $\mathfrak{b}$ contains the principal ideal $\langle \alpha \rangle$, hence $\langle \alpha \rangle = \mathfrak{b}\mathfrak{a}$ for some ideal $\mathfrak{a} \in C$ (as in Theorem 33). Finally using the fact (a) and (c) from the box given in Theorem 18, we have

$$\left|N_{\mathbb{Q}}^{K}(\alpha)\right| = |\mathcal{O}_K/\langle \alpha \rangle| = |\mathcal{O}_K/\mathfrak{a}\mathfrak{b}| = |\mathcal{O}_K/\mathfrak{a}|\,|\mathcal{O}_K/\mathfrak{b}|$$

and the result follows. □

Corollary 8. $|\operatorname{disc}(\mathcal{O}_K)| > 1$ *whenever* $\mathcal{O}_K \neq \mathbb{Z}$*.*

Example 2 (Cyclotomic Field)**.** *Let* $\zeta = e^{2\pi i/7}$*, then* $\mathbb{Z}[\zeta]$ *is a principal ideal domain.*

Solution. Let $K = \mathbb{Q}[\zeta]$, from Theorem 8 we know the value of discriminant, hence

$$|\mathcal{O}_K/\mathfrak{a}| \leq \frac{6!}{6^6}\left(\frac{4}{\pi}\right)^{\frac{7-1}{2}}\sqrt{|-7^5|} \approx 4.13$$

The possible prime divisors of $\mathfrak{a}$ are necessarily among the prime ideals lying over prime ideals generated by 2 and 3. So we factor $\langle 2 \rangle \mathcal{O}_K$ and $\langle 3 \rangle \mathcal{O}_K$. From Corollary 5 we know know that inertial degree f is the smallest integer such that $p^f \equiv 1 \pmod 7$. For $p = 2, f = 3$ and $p = 3, f = 6$, therefore

$$\langle 2 \rangle \mathcal{O}_K = \mathfrak{p}_1\mathfrak{p}_2 \quad \text{and} \quad \langle 3 \rangle \mathcal{O}_K = \mathfrak{p}$$

Hence $\langle 3 \rangle$ is prime in $\mathcal{O}_K$ and every prime ideal dividing $\langle 3 \rangle$ is equal to $\langle 3 \rangle$ so $\mathfrak{p}$ is principal. For $\langle 2 \rangle$, observe that the minimal polynomial factorizes $\mod 2$ as (following the box in Theorem 30)

$$t^6 + t^5 + t^4 + t^3 + t^2 + t + 1 \equiv (t^3 + t^2 + 1)(t^3 + t + 1) \pmod 2$$

To factorize polynomials $f(x) \mod p$ we can use *Berlekamp's algorithm*. This may be accessed in the PARI/GP package[a] using the `factormod(f,p)` command. For example: $x^3 - 7 \equiv (x+2)(x^2+3x+4) \mod 5$, and in PARI/GP, $\texttt{factormod}(\texttt{x}^3 - 7, 5)$ returns $(1,5) * \texttt{x} + \texttt{Mod}(2,5), 1; \texttt{Mod}(1,5) * \texttt{x}^2 + \texttt{Mod}(3,5) * \texttt{x} + \texttt{Mod}(4,5), 1]$.

[a] Can be accessed directly from web-browser: http://pari.math.u-bordeaux.fr/gp.html

In fact

$$(\zeta^3 + \zeta^2 + 1)(\zeta^3 + \zeta + 1)\zeta^4 = 2$$

so we have

$$\langle 2 \rangle \mathcal{O}_K = \langle \zeta^3 + \zeta^2 + 1 \rangle \langle \zeta^3 + \zeta + 1 \rangle = \mathfrak{p}_1\mathfrak{p}_2$$

hence both $\mathfrak{p}_1$ and $\mathfrak{p}_2$ are principal. It follows that every ideal in $\mathbb{Z}[\zeta]$ is principal.

Remark 31. As observed in this example, whenever $\wp\mathcal{O}_K$ remains a prime ideal, then then the corresponding prime ideal $\mathfrak{p}$ is principal.

Example 3 (Real Cyclotomic Field)**.** *Let* $\xi = e^{2\pi i/11} + e^{-2\pi i/11}$*, then* $\mathbb{Z}[\xi]$ *is a principal ideal domain.*

Solution. Let $K = \mathbb{Q}[\xi]$, from Theorem 10 we know the value of discriminant, hence

$$|\mathcal{O}_K/\mathfrak{a}| \leq \frac{5!}{5^5}\left(\frac{4}{\pi}\right)^0\sqrt{11^4} \approx 4.64$$

The possible prime divisors of $\mathfrak{a}$ are necessarily among the prime ideals lying over prime ideals generated by 2 and 3. So we factor $\langle 2\rangle\mathcal{O}_K$ and $\langle 3\rangle\mathcal{O}_K$. From Theorem 27 we know know that inertial degree f is the smallest integer such that $p^f \equiv \pm 1 \pmod 1 1$. For $p = 2, f = 5$ and $p = 3, f = 5$, therefore

$$\langle 2\rangle\mathcal{O}_K = \mathfrak{p} \quad \text{and} \quad \langle 3\rangle\mathcal{O}_K = \mathfrak{p}'$$

Thus, it follows from Remark 31 that $\mathbb{Z}[\xi]$ is a principal ideal domain.

Example 4 (Quadratic Fields). *If $K = \mathbb{Q}[\sqrt{m}]$, determine the ideal classes in $\mathcal{O}_K$ for $m = 6, 437, -5$ and -39.*

Solution. To compute discriminant we will use Theorem 11 and for factorization of $\wp$ in $\mathcal{O}_K$ we will use Theorem 28.

(a) $m = 6$

$$|\mathcal{O}_K/\mathfrak{a}| \leq \frac{2!}{2^2}\left(\frac{4}{\pi}\right)^0 \sqrt{|4\times 6|} \approx 2.45$$

We need to consider $p = 2$ only. $\langle 2\rangle\mathcal{O}_K = \langle 2, \sqrt{6}\rangle^2$. Now to check whether it's principal or not, check for existence of an element in $\mathcal{O}_K$ whose norm is ± 2. Writing $a^2 - 6b^2 = \pm 2$, we easily find that $2 + \sqrt{6}$ is such an element. This shows that (see box given in Theorem 18)

$$|\mathcal{O}_K/\langle 2+\sqrt{6}\rangle| = |N_{\mathbb{Q}}^K(2+\sqrt{6})| = 2$$

From $|\mathcal{O}_K/\mathfrak{a}\mathfrak{b}| = |\mathcal{O}_K/\mathfrak{a}||\mathcal{O}_K/\mathfrak{b}|$ we conclude that $\langle 2+\sqrt{6}\rangle$ is a prime ideal and that it lies over 2, hence $\langle 2+\sqrt{6}\rangle = \langle 2, \sqrt{6}\rangle$. Hence $\mathcal{O}_K$ is a principal ideal domain (class number is 1).

(b) $m = 437$

$$|\mathcal{O}_K/\mathfrak{a}| \leq \frac{2!}{2^2}\left(\frac{4}{\pi}\right)^0 \sqrt{|437|} \approx 10.45$$

We need to consider $p = 2, 3, 5$ and 7. Note that $m = 19 \times 23 \equiv 5 \pmod 8$, therefore $\langle 2\rangle$ remains inert in $\mathcal{O}_K$. Also, using properties of *Legendre symbol* we get

$$\left(\frac{437}{3}\right) = \left(\frac{2}{3}\right) = -1, \quad \left(\frac{437}{5}\right) = \left(\frac{2}{5}\right) = -1, \quad \left(\frac{437}{7}\right) = \left(\frac{3}{7}\right) = -1$$

Hence $\langle 3\rangle$, $\langle 5\rangle$ and $\langle 7\rangle$ also remain inert in $\mathcal{O}_K$. Therefore, $\mathcal{O}_K$ is a principal ideal domain (class number is 1).

(c) $m = -5$

$$|\mathcal{O}_K/\mathfrak{a}| \leq \frac{2!}{2^2}\left(\frac{4}{\pi}\right) \sqrt{|4\times(-5)|} \approx 2.85$$

We need to consider $p = 2$ only. $\langle 2\rangle\mathcal{O}_K = \langle 2, 1+\sqrt{-5}\rangle^2$. As in (a), we will first check that if $\langle 2, 1+\sqrt{-5}\rangle$ is principal or not. If it were, say $\langle\alpha\rangle$, then

$$|N_{\mathbb{Q}}^K(\alpha)| = |\mathcal{O}_K/\langle\alpha\rangle| = 2$$

hence $N_{\mathbb{Q}}^K = \pm 2$. Writing $\alpha = a + b\sqrt{-5}$ with $a, b \in \mathbb{Z}$ we obtain $a^2 + 5b^2 = \pm 2$ which is impossible. But, $\langle 2, 1+\sqrt{-5}\rangle^2$ is a principal ideal (since product of two principal ideals). Therefore, $\langle 2, 1+\sqrt{-5}\rangle$ is an element of order 2 in the ideal class group. We conclude that ideal class group has two ideal classes (class number is 2).

(d) $m = -39$

$$|\mathcal{O}_K/\mathfrak{a}| \leq \frac{2!}{2^2}\left(\frac{4}{\pi}\right)\sqrt{|-39|} \approx 3.97$$

We need to consider $p = 2$ and 3. We have

$$\langle 2\rangle\mathcal{O}_K = \left\langle 2, \frac{1+\sqrt{-39}}{2}\right\rangle\left\langle 2, \frac{1-\sqrt{-39}}{2}\right\rangle = \mathfrak{p}_1\mathfrak{p}_2 \quad \text{and} \quad \langle 3\rangle\mathcal{O}_K = \langle 3, \sqrt{-39}\rangle^2 = \mathfrak{p}^2$$

Note that $[\mathfrak{p}_1]$ is inverse of $[\mathfrak{p}_2]$ since their product is a principal ideal class. It must be the case that the ideal class group is generated by $[\mathfrak{p}]$ and $[\mathfrak{p}_1]$. Therefore there are either three or four ideal classes.

Consider the ideal $\mathfrak{b} = \langle 3+\sqrt{-39}\rangle$. $N_{\mathbb{Q}}^{K}(3+\sqrt{-39}) = 48 = 2^4 \cdot 3$. Note that 2 does not divide $3+\sqrt{-39}$, yet $\mathfrak{b}$ factors into a product of prime ideals, so only one of $\mathfrak{p}_1$ and $\mathfrak{p}_2$ can divide evenly into $\mathfrak{b}$. So it can't be a cyclic group of order 3 or a Klein 4 group. Therefore, either $\mathfrak{b} = \mathfrak{p}_1^2\mathfrak{p}$ or $\mathfrak{b} = \mathfrak{p}_2^2\mathfrak{p}$ and thus $\mathfrak{p}_1^2\mathfrak{p}$ or $\mathfrak{p}_2^2\mathfrak{p}$ is a principal ideal. This implies that $\mathfrak{p}_1^2$ and $\mathfrak{p}$ belong to same ideal class (or $\mathfrak{p}_2^2$ and $\mathfrak{p}$ belong to same ideal class).

$$\mathfrak{p}^2 \sim 1, \quad \mathfrak{p}_1^2\mathfrak{p} \sim 1 \Rightarrow \mathfrak{p}_1^2 \sim \mathfrak{p} \Rightarrow \mathfrak{p}_1^4 \sim 1$$

Further,

$$\mathfrak{p}_1^4 \sim 1, \quad \mathfrak{p}_1\mathfrak{p}_2 \sim 1 \Rightarrow \mathfrak{p}_1^3 \sim \mathfrak{p}_2$$

where 1 represents a principal ideal. So ideal class group is of form $\{1, [\mathfrak{p}_1][\mathfrak{p}_1^2][\mathfrak{p}_1^3]\}$. Hence the ideal class group if a cyclic group of order 4 (class number is 4).

Example 5 (Pure Cubic Fields). *If $K = \mathbb{Q}[\sqrt[3]{m}]$, determine the ideal classes in $\mathcal{O}_K$ for $m = 6$ and 19.*

Solution. To compute discriminant we will use Theorem 14 and for factorization of $\wp$ in $\mathcal{O}_K$ we will use Theorem 30 (factorize polynomials as done in Example 2). Also following result will be useful:

We can calculate norm of potential principal ideal generators (follow Example 1):

1. $N_{\mathbb{Q}}^{K}(a + b\sqrt[3]{m}) = a^3 + b^3 m$
2. $N_{\mathbb{Q}}^{K}(a + b\sqrt[3]{m} + c\sqrt[3]{m^2}) = a^3 + b^3 m + c^3 m^2 - 3mabc$

(a) $m = 6$

$$|\mathcal{O}_K/\mathfrak{a}| \leq \frac{3!}{3^3}\left(\frac{4}{\pi}\right)\sqrt{|-27(6)^2|} \approx 8.82$$

We need to consider $p = 2, 3, 5$ and 7. Note that since 2 and 3 divide 6, both of them are ramified (Remark 18). Also note that the basis of $\mathcal{O}_K$ is $\{1, \sqrt[3]{6}, \sqrt[3]{6^2}\}$.

$$\begin{aligned}
\langle 2\rangle\mathcal{O}_K &= \mathfrak{p}_1^3 = \langle 2, \sqrt[3]{6}\rangle^3 \\
\langle 3\rangle\mathcal{O}_K &= \mathfrak{p}_2^3 = \langle 3, \sqrt[3]{6}\rangle^3 \\
\langle 5\rangle\mathcal{O}_K &= \mathfrak{p}_3\mathfrak{p}_4 = \left\langle 5, \sqrt[3]{6}-1\right\rangle\left\langle 5, \sqrt[3]{6^2}+\sqrt[3]{6}+1\right\rangle \\
\langle 7\rangle\mathcal{O}_K &= \mathfrak{p}_5\mathfrak{p}_6\mathfrak{p}_7 = \left\langle 7, \sqrt[3]{6}+1\right\rangle\left\langle 7, \sqrt[3]{6^2}-\sqrt[3]{6}+1\right\rangle \\
&= \left\langle 7, \sqrt[3]{6}+1\right\rangle\left\langle 7, \sqrt[3]{6}+2\right\rangle\left\langle 7, \sqrt[3]{6}-3\right\rangle
\end{aligned}$$

Now to check whether $\langle 2, \sqrt[3]{6}\rangle$ is principal or not, check for existence of an element in $\mathcal{O}_K$ whose norm is ± 2. Writing $a^3 + 6b^3 \pm 2$, we easily find that $-2 + \sqrt[3]{6}$ is such an element. Now as seen in first part of previous examples, $\langle -2+\sqrt[3]{6}\rangle = \langle 2, \sqrt[3]{6}\rangle$ and hence $\mathfrak{p}_1$ is principal. Note that $N_{\mathbb{Q}}^{K}(\sqrt[3]{6^2}+\sqrt[3]{6}+1) = 25 = 5^2$. Therefore

$$\begin{aligned}
\langle 2\rangle \mathcal{O}_K &= \mathfrak{p}_1^3 = \langle -2+\sqrt[3]{6}\rangle^3 \\
\langle 5\rangle \mathcal{O}_K &= \mathfrak{p}_3\mathfrak{p}_4 = \left\langle \sqrt[3]{6}-1\right\rangle \left\langle \sqrt[3]{6^2}+\sqrt[3]{6}+1\right\rangle \\
\langle 7\rangle \mathcal{O}_K &= \mathfrak{p}_5\mathfrak{p}_6\mathfrak{p}_7 = \left\langle \sqrt[3]{6}+1\right\rangle \left\langle 7, \sqrt[3]{6}+2\right\rangle \left\langle 7, \sqrt[3]{6}-3\right\rangle
\end{aligned}$$

For $\langle 3\rangle \mathcal{O}_K$ we will use the fact that $2\times 3 = 6$ and $\mathfrak{p}_1$ is principal, thus $\mathfrak{p}_2$ is also a principal ideal (pp. 133,[1]). Note that since one of factor of $\langle 5\rangle \mathcal{O}_K$ and $\langle 7\rangle \mathcal{O}_K$, other factor has to be principal, since their product is a principal ideal. Hence, $\mathcal{O}_K$ is principal ideal domain (class number is 1).

(b) $m = 19$

$$|\mathcal{O}_K/\mathfrak{a}| \leq \frac{3!}{3^3}\left(\frac{4}{\pi}\right)\sqrt{|-3(19)^2|} \approx 9.31$$

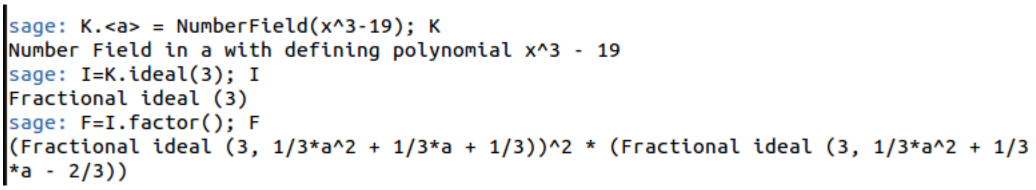
We need to consider $p = 2, 3, 5$ and 7. Let $\alpha = \sqrt[3]{19}$ then the basis elements of $\mathcal{O}_K$ are $1, \alpha, \beta = \frac{1+\alpha+\alpha^2}{3}$ hence

$$\begin{aligned}
\langle 2\rangle \mathcal{O}_K &= \mathfrak{p}_1\mathfrak{p}_2 = \langle 2, \alpha-1\rangle \left\langle 2, \alpha^2+\alpha+1\right\rangle = \langle 2, \alpha-1\rangle \langle 2, 3\beta\rangle \\
\langle 3\rangle \mathcal{O}_K &= \mathfrak{p}_3^2\mathfrak{p}_4 \\
\langle 5\rangle \mathcal{O}_K &= \mathfrak{p}_5\mathfrak{p}_6 = \langle 5, \alpha+1\rangle \left\langle 5, \alpha^2-\alpha+1\right\rangle = \langle 5, \alpha+1\rangle \langle 5, 3\beta-2\rangle \\
\langle 7\rangle \mathcal{O}_K &= \mathfrak{p}_7
\end{aligned}$$

To factorize $\langle 3\rangle \mathcal{O}_K$ I will use computer algebra system (since I don't know any easier way)

The general algorithm for computing prime ideal factorizations is discussed in Cohen's books on computational number theory. See Algorithm 6.2.9 and Algorithm 4.8.17 of *A Course in Computational Algebraic Number Theory*. Springer-Verlag (1996); Algorithm 2.3.22 of *Advanced Topics in Computational Number Theory*. Springer-Verlag (2000).
This may be accessed in the PARI/GP package using command `idealfactor(nfinit(f(x)),p)`. The output is an array where each row is associated to a different prime ideal. A row has the form $[[\mathtt{p}, \mathtt{v}, \mathtt{e}, \mathtt{f}, \mathtt{w}]\mathtt{e}]$, where e and f are the ramification index and residue field degree for that prime ideal. The vector v is related to a second generator γ such that the prime ideal being described is (p, γ) and w is related to the inverse of the prime ideal.

Here is the SageMath code for ideal factorization:

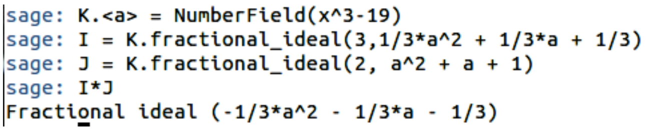


```
sage: K.<a> = NumberField(x^3-19); K
Number Field in a with defining polynomial x^3 - 19
sage: I=K.ideal(3); I
Fractional ideal (3)
sage: F=I.factor(); F
(Fractional ideal (3, 1/3*a^2 + 1/3*a + 1/3))^2 * (Fractional ideal (3, 1/3*a^2 + 1/3
*a - 2/3))
```

Therefore,

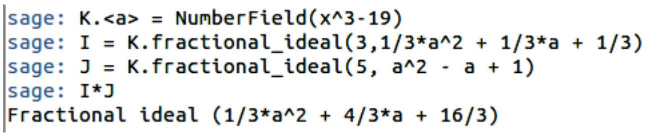
$$\langle 3\rangle \mathcal{O}_K = \left\langle 3, \frac{1+\alpha+\alpha^2}{3}\right\rangle^2 \left\langle 3, \frac{-2+\alpha+\alpha^2}{3}\right\rangle = \langle 3, \beta\rangle^2 \langle 3, \beta-1\rangle$$

We have $\mathfrak{p}_2 \sim \mathfrak{p}_1^{-1}$,$\mathfrak{p}_3^2 \sim \mathfrak{p}_4^{-1}$ and $\mathfrak{p}_6 \sim \mathfrak{p}_5^{-1}$. Hence the class group is generated by $\mathfrak{p}_2, \mathfrak{p}_3$ and $\mathfrak{p}_6$. Now again using SageMath to multiply these:



```
sage: K.<a> = NumberField(x^3-19)
sage: I = K.fractional_ideal(3,1/3*a^2 + 1/3*a + 1/3)
sage: J = K.fractional_ideal(2, a^2 + a + 1)
sage: I*J
Fractional ideal (-1/3*a^2 - 1/3*a - 1/3)
```

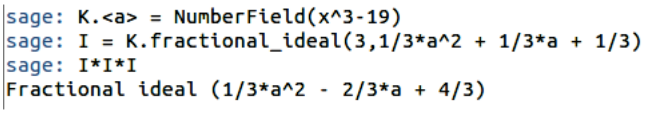
$$\mathfrak{p}_3\mathfrak{p}_2 = \langle 3, \beta\rangle \langle 2, 3\beta\rangle = \langle -\beta\rangle$$



```
sage: K.<a> = NumberField(x^3-19)
sage: I = K.fractional_ideal(3,1/3*a^2 + 1/3*a + 1/3)
sage: J = K.fractional_ideal(5, a^2 - a + 1)
sage: I*J
Fractional ideal (1/3*a^2 + 4/3*a + 16/3)
```

$$\mathfrak{p}_3\mathfrak{p}_6 = \langle 3, \beta\rangle \langle 5, 3\beta - 2\rangle = \langle 5 + \alpha + \beta\rangle$$

Therefore, $\mathfrak{p}_3 \sim \mathfrak{p}_2^{-1} \sim \mathfrak{p}_6^{-1}$ and we conclude that the ideal class is generated by the class containing $\mathfrak{p}_3$. Finally, we check the degree of $\mathfrak{p}_3$ using SageMath. It's clear that degree should be a multiple of 3.



```
sage: K.<a> = NumberField(x^3-19)
sage: I = K.fractional_ideal(3,1/3*a^2 + 1/3*a + 1/3)
sage: I*I*I
Fractional ideal (1/3*a^2 - 2/3*a + 4/3)
```

$$\mathfrak{p}_3^3 = \langle 3, \beta\rangle^3 = \langle 1 - \alpha + \beta\rangle$$

Hence it has three ideal classes (class number is 3).

Remark 32. In part (b), this course of action was motivated by the fact that we were not able to find elements $r, s \in \mathcal{O}_K$ having norm 3 and such that $\langle r, s\rangle = \mathcal{O}_K$. On the contrary if $m = 17 \equiv -1 \pmod 9$ then the corresponding cubic field have class number 1.

The standard way of proceeding is collecting many elements of small norm and forming quotients; if we have elements of norm 2 and 6 we can in general find an integer with norm 3. Note that the integer basis for this case is $1, \alpha, \beta = \frac{\alpha^2 \pm \alpha + 1}{3}$ for $m \equiv \pm 1 \pmod 9$. Now we look for elements of the form $a + b\alpha + c\beta$ with interesting norms and x, y, z small. A little inspection shows that

Element of $\mathcal{O}_K$	Norm for $m = 19$	Norm for $m = 17$
$-1 + \alpha$	$18 = 2 \cdot 3^2$	$16 = 2^4$
$1 + \alpha + \beta$	$27 = 3^3$	3
$1 + \beta$	$8 = 2^3$	$20 = 2^2 \cdot 5$
$-1 + \beta$	18	$6 = 2 \cdot 3$
$-2 + \beta$	$20 = 2^2 \cdot 5$	-2
$1 + \alpha$	20	18
$2 + \alpha + \beta$	$12 = 2^2 \cdot 3$	2
$4 + \alpha + \beta$	$30 = 2 \cdot 3 \cdot 5$	$48 = 2^4 \cdot 3$
$3 - \alpha$	8	$10 = 2 \cdot 5$
$1 - \alpha + \beta$	27	3

For $m = 17$ we have $|\mathcal{O}_K/\mathfrak{a}| \leq 9$, and $\alpha = \sqrt[3]{17}$

$$\begin{aligned}
\langle 2\rangle\mathcal{O}_K &= \mathfrak{p}_1\mathfrak{p}_2 = \langle 2, \alpha + 1\rangle \left\langle 2, \alpha^2 + \alpha + 1\right\rangle = \langle 2 + \alpha + \beta\rangle \langle 2 - \beta\rangle \\
\langle 3\rangle\mathcal{O}_K &= \mathfrak{p}_3^2\mathfrak{p}_4 = \langle 1 + \alpha + \beta\rangle \langle 1 - \alpha + \beta\rangle \\
\langle 5\rangle\mathcal{O}_K &= \mathfrak{p}_5\mathfrak{p}_6 = \langle 5, \alpha + 2\rangle \left\langle 5, \alpha^2 + 3\alpha - 1\right\rangle = \left\langle \frac{3 - \alpha}{2 + \alpha + \beta}\right\rangle \left\langle \frac{5(2 + \alpha + \beta)}{3 - \alpha}\right\rangle \\
\langle 7\rangle\mathcal{O}_K &= \mathfrak{p}_7
\end{aligned}$$

Hence the ring of integers of $\mathbb{Z}[\sqrt[3]{17}]$ is a principal ideal domain.

4.2 Group of Units

Theorem (Dirichlet's Units Theorem). *Let U be the group of units in $\mathcal{O}_K$. Let r and $2s$ be the number of real and non-real embeddings of K in $\mathbb{C}$. Then U is the direct product $W \times V$ where W is a finite cyclic group consisting of the roots of unity in K, and V is a free abelian group of rank $r + s - 1$.*

Definition 32 (Fundamental system of units). The free abelian group V of rank $r + s - 1$ consists of products of some $r + s - 1$ units $u_1, u_2, \dots, u_{r+s-1}$

$$u_1^{k_1} u_1^{k_1} \cdots u_{r+s-1}^{k_{r+s-1}}$$

where $k_i \in \mathbb{Z}$ are uniquely determined for a given element of V. This set of $r + s - 1$ units $\{u_1, u_2, \dots, u_{r+s-1}\}$ is called fundamental system of units in $\mathcal{O}_K$.

Definition 33 (Fundamental unit). A fundamental unit is a generator (modulo the roots of unity) for the unit group of the ring of integers of a number field, when the group has rank 1.

Remark 33. The unit group has fundamental unit iff free abelian group V has rank 1 and this is possible only when the number field is real quadratic field, cubic field or a totally imaginary quartic field.

(a) For real quadratic field $r = 2, s = 0$ therefore, $U = \{\pm u^k : k \in \mathbb{Z}\}$ where u is fundamental unit in $\mathcal{O}_K$.

(b) For pure cubic field $r = 1, s = 1$ therefore, $U = \{\pm u^k : k \in \mathbb{Z}\}$ where u is fundamental unit in $\mathcal{O}_K$.

(c) For quartic field with $r = 0, s = 2$ we have $U = \{\theta u^k : k \in \mathbb{Z}\}$ where θ is a root of unity and u is fundamental unit in $\mathcal{O}_K$.

Theorem 35 (Algorithm for determining fundamental units in a real quadratic field). *Let m be a square free positive integer.*

(a) $m \equiv 2, 3 \pmod 4)$

1. *Take the smallest positive b such that either $mb^2 + 1$ or $mb^2 - 1$ is a square, say a^2, $a > 0$*
2. *$a + b\sqrt{m}$ is the fundamental unit in $\mathbb{Z}[\sqrt{m}]$.*

(b) $m \equiv 1 \pmod 4$

1. *Take the smallest positive b such that either $mb^2 + 4$ or $mb^2 - 4$ is a square, say a^2, $a > 0$ with a having same parity as that of b.*
2. *$\frac{a+b\sqrt{m}}{2}$ is the fundamental unit in $\mathbb{Z}\left[\frac{1+\sqrt{m}}{2}\right]$.*

Proof. We will prove both cases separately.

(a) Note that $N_{\mathbb{Q}}^{K}(a + b\sqrt{m}) = a^2 - b^2 m = \pm 1$ for a unit $a + b\sqrt{m}$. Hence, we have to consider numbers of form $mb^2 \pm 1$, $b \in \mathbb{Z}$ such that it is a perfect square. Now, $a + b\sqrt{m}$ is a power of fundamental unit u (Remark 33). If $u^k = a + b\sqrt{m}$ for $k > 1$ then it will contradict the fact that a and b are the smallest possible positive integers such that $a + b\sqrt{m}$ is a unit.

(b) As noted in Remark 8, for $m \equiv 1 \pmod 4$ the elements of $\mathcal{O}_K$ are of form $\frac{a+b\sqrt{m}}{2}$ where a, b have same parity. Then, $N_{\mathbb{Q}}^{K}\left(\frac{a+b\sqrt{m}}{2}\right) = \frac{a^2-b^2m}{4} = \pm 1$ for a unit $\frac{a+b\sqrt{m}}{2}$. Then as in previous case, for least positive value of b and a satisfying these conditions, we get fundamental unit.

□

Remark 34. We can use continued fractions to find minimal positive solution for $m \equiv 2, 3 \pmod 4$ (see pp. 57 of [21])

Example 6. *Let $K = \mathbb{Q}[\sqrt{m}]$, determine the fundamental unit in $\mathcal{O}_K$ for $m = 2, 3, 5, 6, 13$ and 17.*

Solution. We will use above algorithm.

m	minimum solution	fundamental unit
2	$2(1)^2 - 1 = 1$	$1 + \sqrt{2}$
3	$3(1)^2 + 1 = 2^2$	$2 + \sqrt{3}$
5	$5(1)^2 - 4 = 1$	$\frac{1+\sqrt{5}}{2}$
6	$6(2)^2 + 1 = 5^2$	$5 + 2\sqrt{6}$
13	$13(1)^2 - 4 = 3^2$	$\frac{3+\sqrt{13}}{2}$
17	$17(2)^2 - 4 = 8^2$	$4 + \sqrt{17}$

Theorem 36 (Lower bound of fundamental unit for pure cubic field)**.** *Let K be a cubic extension of $\mathbb{Q}$ having only one embedding in $\mathbb{R}$. Let u be the fundamental unit in $\mathcal{O}_K$, then for $|\operatorname{disc}(\mathcal{O}_K)| \geq 33$*

$$\frac{|\operatorname{disc}(\mathcal{O}_K)| - 27}{4} < u^3$$

Proof. From Remark 33 it follows that $u > 1$ and all units in $\mathcal{O}_K$ are of form $\pm u^k$, $k \in \mathbb{Z}$.

Claim 1 Let $u, ae^{i\theta}$ and $ae^{-i\theta}$ be the conjugates of u. Then $u = a^{-2}$ and

$$\operatorname{disc}(u) = -4\sin^2(\theta)(a^3 + a^{-3} - 2\cos(\theta))^2$$

Since, $N_{\mathbb{Q}}^{K}(u) = 1 = ua^2$, we have $u = a^{-2}$. From Remark 5 we know that

$$\begin{aligned}
\operatorname{disc}(u) &= (ae^{i\theta} - ae^{-i\theta})^2(u - ae^{i\theta})^2(u - ae^{-i\theta})^2 \\
&= -4a^2\sin^2(\theta)\left(u^2 - (ae^{i\theta} + ae^{-i\theta})u + a^2\right)^2 \\
&= -4a^2\sin^2(\theta)\left(u^2 - 2au\cos(\theta) + a^2\right)^2 \\
&= -4\sin^2(\theta)\left(a^{-3} - 2\cos(\theta) + a^3\right)^2
\end{aligned}$$

Claim 2 $|\operatorname{disc}(u)| < 4(u^3 + u^{-3} + 6)$

Let $x = a^3 + a^{-3}$ and $c = \cos(\theta)$, so from previous claim we have, $f(x) = -4(1 - c^2)(x - 2c)^2$, now we will find the minimum value of

$$g(x) = \frac{-f(x)}{4} - x^2 = (1 - c^2)(x - 2c)^2 - x^2 = -c^2x^2 + 4c(c^2 - 1)x - 4c^4$$

$$\Rightarrow g'(x) = -2c^2x + 4c(c^2 - 1) = 0$$

$$\Rightarrow x = \frac{2(c^2-1)}{c}$$

$$\Rightarrow g(x) \le g\left(\frac{2(c^2-1)}{c}\right) = 4(1-2c^2) \le 4$$

since minimum value of $c^2 = \cos^2(\theta) = 0$. From this we conclude that

$$|f(x)| = |-4(g(x)+x^2)| \le 4(4+x^2) = 4(u^3+u^{-3}+6)$$

From this claim we conclude that

$$u^3 + u^{-3} > \frac{|\operatorname{disc}(u)|}{4} - 6$$

As given in box of Theorem 13 we have

$$u^3 + u^{-3} > \frac{|\operatorname{disc}(\mathcal{O}_K)|}{4} - 6$$

$$\Rightarrow u^3 > \frac{|\operatorname{disc}(\mathcal{O}_K)|}{4} - 6 - u^{-3}$$

Since $u > 1$ we have

$$u^3 > \frac{|\operatorname{disc}(\mathcal{O}_K)|}{4} - 7 = \frac{|\operatorname{disc}(\mathcal{O}_K)| - 28}{4}$$

For $\operatorname{disc}(\mathcal{O}_K)| \ge 33$, we have

$$u^3 > \frac{|\operatorname{disc}(\mathcal{O}_K)| - 27}{4}$$

□

Example 7. *Let $K = \mathbb{Q}[\sqrt[3]{2}]$, prove that $\frac{1}{\sqrt[3]{2}-1}$ is the fundamental unit of $\mathcal{O}_K$.*

Solution. Let $\alpha = \sqrt[3]{2}$, $\mathbb{O}_K = \mathbb{Z}[\alpha]$ and $\operatorname{disc}(\alpha) = \operatorname{disc}(\mathcal{O}_K) = -108 > 33$. If u is the fundamental unit, then from the theorem above, $u^3 > 20.25 > 20$. Therefore, $u > 2.72$ and $u^2 > 7.39$. Now,

$$\beta = \frac{1}{\alpha - 1} = \alpha^2 + \alpha + 1$$

is unit in $\mathcal{O}_K$ since $N_{\mathbb{Q}}^K(\alpha-1) = 2-1 = 1$ (see Example 1). We can see that ($\sqrt[3]{2} \approx 1.26$)

$$1 < \beta < 4 \qquad \Rightarrow 1 < \beta < u^2$$

and β is a power of u, hence $\beta = u$.

Remark 35. There is no known formula for calculating fundamental unit but is intimately related to a unit c, called *circular unit*, in ring of algebraic integers and satisfies: $c = u^h$ where h is the class number for that ring[11].

4.3 Solving Diophantine Equations

In Example 6 we saw that $1+\sqrt{2}$ is the fundamental unit in $\mathbb{Z}[\sqrt{2}]$, but clearly it's not a root of unity. We can use powers of $1+\sqrt{2}$ to generate infinitely many solutions to the Diophantine equation $x^2-2y^2=\pm 1$ (pp. 20, [21]). Just as quadratic fields enabled us to solve Diophantine equations of form $x^2-dy^2=\pm 1, 4$ (pp. 55 [5]) and $x^2+x+b=y^3$ (pp. 26, [21]), pure cubic fields enable us to solve Diophantine equations of form $ax^3+by^3=c$. Though we have already proved that such equations have finitely many solutions (pp. 64, [22]), but for some special cases we can tell the exact value of maximum possible number of solutions.

Theorem 37 (Delaunay[1]-Nagell[2] Theorem). *The equation $x^3+dy^3=1$ has at most one solution in integers x, y different from zero. If x_1, y_1 is a solution, the number $x_1+y_1\sqrt[3]{d}$ is either the fundamental unit of $K=\mathbb{Q}[\sqrt[3]{d}]$ or its square; the latter can happen for only finitely many values of d.*

Proof. If $d=\pm 1$ then the given equation has only trivial solutions. If d contains a cube larger than 1, it can be absorbed into the factor y^3. Hence we can assume that d is cubefree and larger than 1. From Example 1 we know that $N_{\mathbb{Q}}^{K}(a+b\sqrt[3]{d})=a^3+db^3$ therefore, if

$$N_{\mathbb{Q}}^{K}(x_1+y_1\sqrt[3]{d})=x_1^3+dy_1^3=1, \qquad y_1\neq 0$$

then $x_1+y_1\sqrt[3]{d}$ is a positive unit of K, and a such is a positive power of the fundamental unit u mentioned in Remark 33. It therefore suffices to show that no power of a positive unit smaller than 1, with exponent larger than 2, is of the special form $x+y\sqrt[3]{d}$ and to show that the square of a unit is of this form in only finitely many cases. We divide the proof in four parts. I won't give details of the proof of these parts since they involve lengthy arguments and details can be found on pp. 113-119 of [5]. Let $d=ab^2$ where a, b are coprime and squarefree, also $\alpha=\sqrt[3]{ab^2}$, $\beta=\sqrt[3]{a^2b}$ and $X, Y\in\mathbb{Q}$.

Claim 1. The square of an irrational unit of K of the form $v=x+y\alpha+z\beta$, with $x,y,z\in\mathbb{Z}$ is itself of the form $X+Y\alpha$ only if $v=1+\sqrt[3]{20}-\sqrt[3]{50}$. The square of a unit of K of the form $v=\dfrac{x+y\alpha+z\beta}{3}$ with $3\nmid xyz$ (if such exists) is itself of the form $X+Y\alpha$ for only finitely many values of d.

To prove this we will need FLT for $n=3$ (pp. Theorem 2.4.3, pp. 75, [21]); $(\pm 5, 3)$ are the only solution of $x^2+2=y^3$ (Example 1.7.3, pp. 26, [21]) and following result by Louis Joel Mordell[3] is a very weak consequence of a result by Kurt Mahler[4] (uses p-adic version of Roth's Theorem, see pp. 68 of [22])

> Suppose that $m\geq 2, n\geq 3, ab\neq 0, \gcd(x,y)=1$. Then as $\max(|x|,|y|)\to\infty$, the greatest prime factor of ax^m+by^n tends to infinity (pp. 155, [5]).

Claim 2. The fourth power of a positive irrational unit of K is never of the form $X+Y\alpha$.

This follows from previous claim.

[1] Announced in French Academy of Sciences in three parts in 1916, 1920 and 1921; for the part reported in 1921 see: http://gallica.bnf.fr/ark:/12148/bpt6k31239

[2] "Solution complète de quelques équations cubiques à deux indeterminées." *Journal de Mathématiques Pures et Appliquées* 9, no. 4 (1925), 209–270. http://sites.mathdoc.fr/JMPA/afficher_notice.php?id=JMPA_1925_9_4_A6_0

[3] "The Integer Solutions of the Equation $y^2=ax^n+bx^{n-1}+\ldots+k$." *Journal of the London Mathematical Society* 1, no. 2 (1926): 66–68. http://dx.doi.org/10.1112/jlms/s1-1.2.66

[4] "On the greatest prime factor of ax^m+by^n." *Nieuw Archief voor Wiskunde* 3, no. 1 (1953): 113–122.

Claim 3. The cube of a positive irrational unit of K is never of the form $X + Y\alpha$

Claim 4. If $p > 3$ is a prime and $v = \dfrac{x + y\alpha + z\beta}{3}$ is a positive unit smaller than 1, then v^p is not of the form $X + Y\alpha$

Along with Theorem 13, we need to use following result

> Suppose x and y are integers such that $\gcd(x, dy) = 1$, such that
>
> $$(x + y\sqrt[3]{d})^n = X + Y\sqrt[3]{d} + Z\sqrt[3]{d^2}$$
>
> where X, Y and Z are rational and $n > 1$. Then $XYZ \neq 0$ except in two instances: $(\sqrt[3]{10} - 1)^5 = 99 - 45\sqrt[3]{10}$ and $(\sqrt[3]{4} - 1)^4 = -15 + 12\sqrt[3]{2}$ (pp. 110, [5]).

From second, third and fourth claim it follows that any non-zero solution of $x^3 + dy^3 = 1$ must correspond either to the fundamental unit of K, or to its square. Not both of these numbers can lead to solutions, thus completing the proof.

□

Conclusion

The proof of second case of FLT for *regular primes* is direct application of Kummer's higher reciprocity laws and was his main achievement, for complete proof refer [9]. Hence combining both cases, Kummer proved:

Theorem (Kummer, 1847[5]). *The equation $x^p + y^p = z^p$ has no solution in integers if the exponent p is a regular prime.*

Kummer found a criterion in terms of *Bernoulli numbers* $B_0 = 1, B_1 = -\frac{1}{2}, B_2 = \frac{1}{6}, B_3 = B_5 = \ldots = B_{odd>1} = 0, B_4 = \frac{-1}{30}, \ldots$, that could be checked reasonably conveniently, at least for primes less than 100.

Theorem. *Let h_+ be the class number of $\mathbb{Z}[\zeta + \zeta^{-1}]$ and h be the class number $\mathbb{Z}[\zeta]$ where $\zeta = e^{\frac{2\pi i}{p}}$ and p is a prime integer. Then*

(a) If $p|h_+$ then $p|h_*$ where $h_* = \frac{h}{h_+}$

(b) $p|h_*$ if and only if there is some integer k with $1 \leq k \leq \frac{p-3}{2}$, such that p^2 divides the sum $\sum_{j=1}^{p-1} j^{2k}$.

(c) If $p|h_*$ then p divides the numerator of a Bernoulli number B_{2k} with $2 \leq 2k \leq p-3$.

(d) p is regular if and only if it does not evenly divide the numerator of any of the first $p-3$ numbers in the series of fractions of the Bernoulli Numbers B_n.

Using this theorem Kummer proved FLT for prime exponents less than 100 except 37, 59 and 67. These three are the only irregular primes less than 100, since 37 divides the numerator of B_{32}, 59 divides the numerator of B_{44} and 67 divides the numerator of B_{58}. Actually this is checked using following congruences relation derived by Kummer between 1850-1857, for its proof refer pp. 44, of Neal Koblitz's book[6].

Theorem. *Let $n, m, p, r \in \mathbb{N}$ where n, m are even numbers and p is prime number with $p - 1 \not| n$, then*

$$\left(1 - p^{n-1}\right) \frac{B_n}{n} \equiv \left(1 - p^{m-1}\right) \frac{B_m}{m} \pmod{p^r}$$

when $n \equiv m \pmod{\varphi(p^r)}$, where φ is Euler's totient function.

In 1915, Kaj Løchte Jensen[7] proved that there are infinitely many *irregular primes*, for proof see §7.2 in Chapter 5 of Borevich-Safarevich[8]. We still don't know that whether there are infinite or finite number of regular primes. Hence, we face the similar dilemma as faced by Germain in 1823 (see Corollary 1) but now have a better understanding of algebraic numbers.

[5] "Beweis des Fermat'schen Satzes der Unmöglichkeit von $x^\lambda + y^\lambda = z^\lambda$ für eine unendliche Anzahl Primzahlen λ." Lejeune Dirichlet communicated to the Königlichen Preußischen Akademie der Wissenschaften zu Berlin in 1847. The proof was given in modern form, using Dedekind's notion of ideals, by David Hilbert in 1894.

[6] *p-adic Numbers, p-adic Analysis, and Zeta - Functions.* New York: Springer-Verlag, 1984. http://dx.doi.org/10.1007/978-1-4612-1112-9

[7] "Om talteoretiske Egenskaber ved de Bernoulliske tal." *Nyt tidsskrift for matematik* 26 (1915): 73-83. http://www.jstor.org/stable/24532219

[8] *Number Theory.* New York and London: Academic Press, 1966

Appendix A

Lattice

Within mathematics, the term *lattice* has different meanings in different contexts. While studying *number fields* we came across this term *lattice* in three different contexts, which I will discuss here (in the order of their occurrence in this report). I will be deliberately avoiding discussion of properties of sublattices.

A.1 Module

Let R be an Dedekind domain and F be the corresponding *field of fractions*.

> *$R-$lattice is a finitely generated $R-$torsion-free module*[1].

Each $R-$lattice M is a $R-$submodule of a finite dimensional vector space V over F, namely $V = FM$. We call M a *full* $R-$lattice in V, the adjective indicting that M contains a $F-$basis of V. Let M and N be a pair of full $R-$lattices in a $F-$space V. Since N contains a $F-$basis for V, for each $x \in M$ there is a non-zero $a \in R$ such that $ax \in N$. But M is finitely generated as $R-$module. Therefore we can choose $a \in R, a \neq 0$, such that $aM \subset N$.

We define dual and double dual $R-$modules corresponding to the $R-$lattice M:

$$M^* = \mathrm{Hom}_R(M, R), \qquad M^{**} = \mathrm{Hom}_R(M^*, R)$$

where, for example, the set of all module homomorphisms[2] from M to R is denoted by $\mathrm{Hom}_R(M, R)$. Also, the evaluation map[3] $\varphi : M \to M^{**}$ is given by

$$\{\varphi(m)\}f = f(m), \quad f \in M^*$$

Clearly $\varphi = 0$ if and only if $M^* = 0$. Then every $R-$lattice is reflexive[4], that is, $M \cong M^{**}$. Then define dual spaces

$$V^* = \mathrm{Hom}_F(V, F), \quad V^{**} = \mathrm{Hom}_F(V^*, F)$$

The evaluation map gives a $F-$isomorphism $V \cong V^{**}$. Since R is noetherian, M^* and M^{**} are also $R-$lattices, and there are embeddings $M^* \subset V^*$ and $M^{**} \subset V^{**}$. Explicitly we have

$$M^{**} = \{v \in V : f(v) \in R \quad \text{for all} \quad f \in M^*\}$$

For a more general discussion, than given earlier, of *different ideal* refer pp. 60 of [6].

[1] A torsion-free module is a module over a ring such that 0 is the only element annihilated by a regular element (non zero-divisor) of the ring.

[2] This set is an abelian group and also a module since R is commutative.

[3] Let S, T be sets, and let S^T be the set of all mappings from T to S. The evaluation mapping for S^T is the mapping $\varphi : S^T \times T \to S$ defined by $\varphi(f, t) = f(t)$

[4] We call M reflexive if φ is an isomorphism.

For the case where M is a $\mathbb{Z}-$module[a] embedded in a vector space V over the field $\mathbb{R}$, and the Euclidean metric is used to describe the lattice structure, we get *lattice-group* as a special case of *lattice-module*. Since the motivation behind study of each of them is different, I have discussed them separately.

[a] A free abelian group or free $\mathbb{Z}-$module is an abelian group with a basis.

A.2 Partially Ordered Set

A lattice is a partially ordered set in which for every two elements a and b the least upper bound (called join, denoted $a \vee b$) and the greatest lower bound (called meet, denoted $a \wedge b$) exist.

According to their properties, lattices are divided into various types. The most basic ones being distributive, modular and complemented lattices[10].
The elements of a distributive lattice satisfy the distributive law:

$$a \vee (b \wedge c) = (a \wedge b) \vee (a \wedge c)$$

The elements of a modular lattice satisfy the modular law:

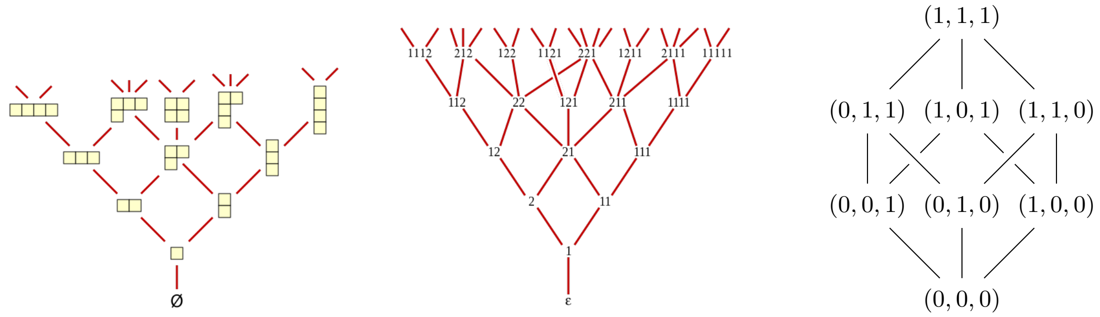
$$a \leq c \Rightarrow a \vee (b \wedge c) = (a \vee b) \wedge c$$

Every distributive lattice is modular.
If a lattice has the greatest and the least elements and to each of its elements such an element exists that their join is the greatest element and their meet is the least element, it is called complemented. In other words, a lattice is said to be complemented if for each element a there exist an element b satisfying:

$$a \vee b = 1 \quad \text{and} \quad a \wedge b = 0$$

A complemented distributive lattice is called *Boolean algebra*.

To represent finite lattices we use Hasse diagram. It is a type of mathematical diagram used to represent a partially ordered set with all elements of the same rank shown at the same height above the bottom.



(a) Distributive Lattice: Young's lattice representing integer partitions
[By David Eppstein (Public domain), via Wikimedia Commons]

(b) Modular Lattice: Young-Fibonacci lattice representing the digit sequences of 1 and 2
[By David Eppstein (Public domain), via Wikimedia Commons]

(c) Complemented Lattice: It is representing the boolean algebra of subsets of a three element set

Figure A.1: Three examples of lattice-orders

A.3 Group

Let $\mathbf{a_1}, \mathbf{a_2}, \ldots, \mathbf{a_n}$ be *linearly independent* real vectors in $n-$dimensional real euclidean space $\mathbb{R}^n$ over $\mathbb{R}$. Then the lattice Λ is defined as

$$\Lambda = \{\mathbf{x} \in \mathbb{R}^n : \mathbf{x} = u_1\mathbf{a_1} + \ldots + u_n\mathbf{a_n}, u_i \in \mathbb{Z}\}$$

Since the basis $\mathbf{a_1}, \mathbf{a_2}, \ldots, \mathbf{a_n}$ is linearly independent, the expression of any vector $\mathbf{x}$ as defined above for real u_i is unique. Moreover, the basis is not uniquely determined by the lattice. If $\mathbf{a_1}, \mathbf{a_2}, \ldots, \mathbf{a_n}$ and $\mathbf{a'_1}, \mathbf{a'_2}, \ldots, \mathbf{a'_n}$ are bases of the same lattice, then

$$\mathbf{a'_i} = \sum_{j=1}^{n} v_{ij}\mathbf{a_j}$$

where v_{ij} are any integers with $\det(v_{ij}) = \pm 1$, then we have

$$\det(\mathbf{a'_1}, \ldots, \mathbf{a'_n}) = \det(v_{ij}) \det(\mathbf{a_1}, \ldots, \mathbf{a_n}) = \pm \det(\mathbf{a_1}, \ldots, \mathbf{a_n})$$

where, for example, $\det(\mathbf{a_1}, \ldots, \mathbf{a_n})$ denotes the determinant of the $n \times n$ matrix whose j^{th} row is the vector $\mathbf{a_j}$. Hence,

$$\mathrm{d}(\Lambda) = |\det(\mathbf{a_1}, \ldots, \mathbf{a_n})|$$

is independent of the particular choice of the basis of Λ. Note that if $\mathbf{x} \in \Lambda$ then $-\mathbf{x} \in \Lambda$; and if $\mathbf{x}, \mathbf{y} \in \Lambda$ then $\mathbf{x} \pm \mathbf{y} \in \Lambda$.

The vectors of a lattice Λ form a group under addition.

Moreover, by generalising Minkowski's convex body theorem as on pp. 73 of [4], a lattice is the most general group of vectors in $n-$dimensional space which contains n linearly independent vectors and which satisfies the further property that there is some sphere about the origin $\mathbf{o}$ which contains no other vector of the group except $\mathbf{o}$.

We denote the scalar product of two $n-$dimensional vectors $\mathbf{x} = (x_1, x_2, \ldots, x_n)$ and $\mathbf{y} = (y_1, y_2, \ldots, y_n)$ by

$$\mathbf{xy} = x_1y_1 + x_2y_2 + \ldots + x_ny_n$$

Let $\mathbf{b_1}, \ldots, \mathbf{b_n}$ be a basis of a lattice Λ. Since the $\mathbf{b_j}$ are linearly independent, there exist vectors $\mathbf{b_j^*}$ such that

$$\mathbf{b_j^*}\mathbf{b_i} = \begin{cases} 1 & \text{if} \quad i = j \\ 0 & \text{if} \quad i \neq j \end{cases}$$

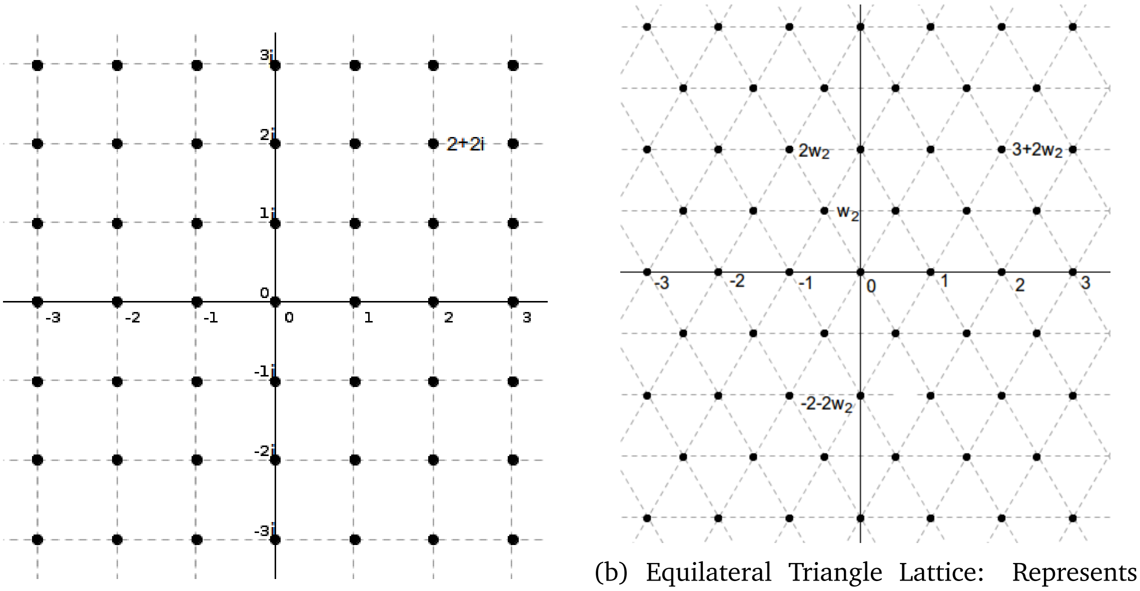
The lattice Λ^* with the basis $\mathbf{b_j^*}$ is called the *dual* (or *polar* or *reciprocal*) lattice of Λ, and $\mathbf{b_j^*}$ is the *dual* (or *polar* or *reciprocal*) basis to $\mathbf{b_j}$. The dual lattice Λ^* of Λ is independent of the choice of the particular basis, since

$$\mathrm{d}(\Lambda)\mathrm{d}(\Lambda^*) = 1$$

for proof refer pp. 24 of [4].

`Example`: Consider pair of complex numbers $w_1, w_2 \in \mathbb{C}$ such that their ratio $\frac{w_1}{w_2}$ is not real. In other words, considered as vectors in $\mathbb{R}^2$, the two are not collinear. The lattice generated by w_1 and w_2 is called *period lattice*. Thus

$$\Lambda = \{mw_1 + nw_2 : m, n \in \mathbb{Z}\}$$



(a) Square Lattice: Represents Gaussian integers when $w_1 = 1$ and $w_2 = \sqrt{-1} = i$

(b) Equilateral Triangle Lattice: Represents Eisenstein integers when $w_1 = 1$ and $w_2 = \frac{-1+\sqrt{-3}}{2}$

Figure A.2: *Examples of period lattices drawn on complex plane using GeoGebra v4.0.34.0 and Pinta v1.3*

Normally we are concerned with lattices over the rational integers, but we can extend this notion of lattice to general *number fields* as in [14].
Let K be an algebraic extension of the $\mathbb{Q}$ of degree m. We regard K as an algebra over $\mathbb{Q}$, which we can extend to an algebra K^* over $\mathbb{R}$. It is well known that K^* is commutative and semi-simple[a], and the integers of K^* are just those of K. Then we can define the $n-$dimensional space K^n over K as being the set of ordered $n-$tuples of elements in K^*. Thus if $\beta \in K^n$ then $\beta = (\beta_1, \ldots, \beta_n)$ where each $\beta_i \in K^*$ is of form

$$\beta_i = x_{i1}\alpha_1 + x_{i2}\alpha_2 + \ldots + x_{im}\alpha_m$$

where $x_i \in \mathbb{R}$ and $\alpha_1, \ldots, \alpha_m$ is an *integral basis* for K. Hence there is a natural map from K^n onto $\mathbb{R}^{mn}$ in which each component β_i of $\beta \in K^n$ is mapped onto m of the components of the point in $\mathbb{R}^{mn}$, namely $x_{i1}, \ldots, x_{im}$. A transformation in K^n of matrix A and determinant $\delta \neq 0$ induce a transformation in $\mathbb{R}^{mn}$ of matrix $P^{-1}BP$, where

$$P = \begin{bmatrix} \alpha_1^{(1)} I_n & \alpha_2^{(1)} I_n & \ldots & \alpha_m^{(1)} I_n \\ \alpha_1^{(2)} I_n & \alpha_2^{(2)} I_n & \ldots & \alpha_m^{(2)} I_n \\ \vdots & \vdots & \ddots & \vdots \\ \alpha_1^{(m)} I_n & \alpha_2^{(m)} I_n & \ldots & \alpha_m^{(m)} I_n \end{bmatrix} \quad \text{and} \quad B = \begin{bmatrix} A^{(1)} & 0 & \ldots & 0 \\ 0 & A^{(2)} & \ldots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \ldots & A^{(m)} \end{bmatrix}$$

with $\alpha_j^{(1)}, \ldots, \alpha_j^{(m)}$ to be conjugates of α_j, I_n to be $n \times n$ identity matrix and $A^{(1)}, \ldots, A^{(m)}$ be the conjugates of A. We can also extend the norm $\mathcal{N}$ from K to K^*, thus the transformation in $\mathbb{R}^{mn}$ has determinant $\mathcal{N}(\delta)$. Finally, we define a *lattice* in K^n to be any linear transformation of determinant δ of the set of points in K^n all of whose coordinates are integers, such that $\mathcal{N}(\delta) \neq 0$.

[a] K^* is isomorphic to direct sum of r copies of $\mathbb{R}$ and s copies of $\mathbb{C}$, where r and $2s$ are the number of real and complex conjugates of K.

Bibliography

[1] Marcus, D. A. *Number Fields*. New York: Springer-Verlag, 1977. http://dx.doi.org/10.1007/978-1-4684-9356-6

[2] Stewart, I. and Tall, D. O. *Algebraic Number Theory*. London and New York: Chapman and Hall, 1987

[3] van der Poorten, A. J. *Notes on Fermat's Last Theorem*. New York: John Wiley & Sons, 1996

[4] Cassels, J. W. S. *An Introduction to the Geometry of Numbers*. Berlin and Heidelberg: Springer-Verlag, 1997. http://dx.doi.org/10.1007/978-3-642-62035-5

[5] LeVeque, W. J. *Topics in Number Theory, Volumes I and II*. Mineola: Dover Publications, 2002

[6] Reiner, I. *Maximal Orders*. Oxford: Clarendon Press, 2003

[7] Ribenboim, P. "The Work of Kummer on Fermat's Last Theorem." in *Number Theory Related to Fermat's Last Theorem*, edited by Neal Koblitz, 1–29. Boston: Birkhäuser, 1982. http://dx.doi.org/doi:10.1007/978-1-4899-6699-5_1

[8] Stark, H. M. "Galois Theory, Algebraic Number Theory and Zeta Functions." in *From Number Theory to Physics*, edited by Michel Waldschmidt, Pierre Moussa, Jean-Marc Luck and Claude Itzykson, 313–393. Berlin and Heidelberg: Springer-Verlag, 1992. http://dx.doi.org/10.1007/978-3-662-02838-4_6

[9] Thakur, D. "Fermat's last theorem for regular primes." in *Cyclotomic Fields and Related Topics*, edited by Sukumar Das Adhikari, Shashikant Anant Katre and Dinesh Thakur, 165–173. Pune: Bhaskaracharya Pratishthana, 2000. http://www.bprim.org/cyclotomicfieldbook/d3f.pdf

[10] Bilová, Š. "Lattice Theory - its birth and life." in *Mathematics throughout the ages*, edited by Eduard Fuchs, 250–257. Praha: Prometheus, 2001. http://dml.cz/dmlcz/401261

[11] Mazur, B. "Algebraic Numbers." in *The Princeton Companion for Mathematics*, edited by Timothy Gowers, June Barrow-Green and Imre Leader, 315–332. Princeton and Oxford: Princeton University Press, 2008. http://www.math.harvard.edu/~mazur/preprints/algebraic.numbers.April.30.pdf

[12] Dickson, L. E. "Fermat's Last Theorem and the Origin and Nature of the Theory of Algebraic Numbers." *Annals of Mathematics*, Second Series 18, no. 4 (1917): 161–187. http://dx.doi.org/10.2307/2007234

[13] Vandiver, H. S. "Fermat's Last Theorem: Its History and the Nature of the Known Results Concerning It." *The American Mathematical Monthly* 53, no. 10 (1946): 555–578. http://dx.doi.org/10.2307/2305236

[14] Rogers, K. and Swinnerton-Dyer, H. P. F. “The Geometry of Numbers over Algebraic Number Fields.” *Transactions of the American Mathematical Society* 88, no. 1 (1958): 227–242. http:dx.doi.org/10.1090/s0002-9947-1958-0095160-9

[15] Edwards, H. M. “Fermat’s Last Theorem.” *Scientific American* 239, no. 4 (1978), 104–122. http://dx.doi.org/10.1038/scientificamerican1078-104

[16] Lenstra, H. W. “Euclidean Number Fields 1.” *The Mathematical Intelligencer* 2, no. 1 (1979): 6–15. http://dx.doi.org/10.1007/bf03024378 [Translated from Dutch to English by Alf van der Poorten]

[17] Lenstra, H. W. “Euclidean Number Fields 2.” *The Mathematical Intelligencer* 2, no. 2 (1980): 73–77. http://dx.doi.org/10.1007/bf03023376 [Translated from Dutch to English by Alf van der Poorten]

[18] Nakahata, N. “On Units of Galois Extensions over $\mathbb{Q}$.” *Proceedings of the Faculty of Science of Tokai University* 15 (1980): 23–27. http://ci.nii.ac.jp/naid/110000010754/en/

[19] Kleiner, I. “The Roots of Commutative Algebra in Algebraic Number Theory.” *Mathematics Magazine* 68, no. 1 (1995): 3–15. http://dx.doi.org//10.2307/2691370.

[20] Daileda, R. C. “Algebraic Integers on the Unit Circle” *Journal of Number Theory* 118, no. 2 (2006): 189-191. http://dx.doi.org/10.1016/j.jnt.2005.09.002

[21] Korpal, G. “Diophantine Equations.” *Summer Internship Project Report*, guided by Prof. S. A. Katre (18 May 2015 – 16 June 2015)

[22] Korpal, G. “Diophantine Approximations.” *Winter Internship Project Report*, guided by Dr. R. Thangadurai (13 December 2015 – 8 January 2016)