THE ISLAMIC UNIVERSITY OF GAZA
DEANERY OF HIGHER STUDIES
FACULTY OF SCIENCE
DEPARTMENT OF MATHEMATICS

Some Congruences on prime factors of class number of algebraic extensions

PRESENTED BY

Yousef Atef M. Dabboor Asad

SUPERVISED BY

Prof. Dr. Jasser H. Sarsour

A THESIS SUBMITTED IN PARTIAL FULFILMENT OF THE REQUIREMENT FOR THE DEGREE OF MASTER OF MATHEMATICS

January 2010

Dedication

To my father...

To my mother

To my wife

To my son mohammed

To all knowledge seekers...

Acknowledgments

I would like to express my sincere thanks and gratitude to Almighty for his blessings.

I would like to express my sincere appreciation and thanks to my supervisor Prof. Dr. Jasser Sarsour for his ceaseless help and supervision during the preparation of this thesis.

I would like to express my sincere thanks to all the staff members of mathematics department and all my teachers who taught me to come to this stage of learning. Specially for Dr. Ahmad Al-Mabhouh for his great help.

I am extremely and sincerely thankful to my parents whose love, care and sacrifice enabled me to reach this level of learning.

Abstract

In this thesis, we study some congruences on the odd prime factors of the class number of the number fields.

We say that a finite Galois extension L/K is Galois solvable if the Galois group $Gal(L/K)$ is solvable.

The main result studied is:

Let L/Q be a finite algebraic extension with $[L : Q] = 2^{\alpha_0} \times N_1$, where $N_1 > 1$ is odd. Suppose that there exists a field $K \subset L$ with $[K : Q] = 2^{\alpha_0}$ and with L/K Galois solvable extension. Let $h(L)$ be the class number of L. Suppose that $h(L) > 1$. Let p be a prime dividing $h(L)$. Let r_p be the rank of the $p-$class group of L. If $p \times \prod_{i=1}^{r_p}(p^i - 1)$ and N_1 are coprime, then p divides the class number $h(K)$ of K.

Contents

Introduction

Algebraic number theory is a major branch of number theory which studies algebraic structures related to algebraic integers.

This is generally accomplished by considering a ring of algebraic integers O in an algebraic number field K/Q, and studying their algebraic properties such as factorization, the behavior of ideals, and field extensions.

The focus of algebraic number theory is to extend the properties of the natural numbers to more general number structures: algebraic number fields, and their rings of algebraic integers.

These structures have most of the standard properties that we associate with ordinary whole numbers, but some subtle properties sometimes fail to generalize. One particular property that fails to generalize and can be problematic is that of unique factorization.

The notion of prime in the regular whole numbers can be viewed as two different ideas. First is the notion of being irreducible in the sense that a prime has no factors other than 1 and itself. The second being that if p is a factor of a product ab then it must be a factor of either a or b.

It turns out that in certain number fields these ideas do not concide.

In an integral domain a prime is always irreducible but the reverse is not always true, as a result unique factorization into irreducibles breaks down.

The factorization of ideals in such rings turns out to be more satisfactory: every ideal is a unique product of prime ideals.

The extent to which factorization in these rings is not unique can be measured by the group of ideal classes (fractional ideals modulo principal ones). This group of ideal classes

is called the ***class group*** and its order: called the ***class number*** turns out to be of crucial importance in the theory of numbers and many deep and delicate results are related to its arithmetic properties.

For instance unique factorization holds in a ring of integers if and only if the class number is 1. In general the larger the class number the more non-unique the factorization !!.

Class field theory has deep roots in the history of mathematics, going back to Gauss, Kummer and Kronecker. The term "class field" was coined by Heinrich Weber in his book on elliptic functions and algebraic numbers [8] which appeared in 1891. It was Hilbert [3] who in 1898 proposed to establish class field theory as the theory of arbitrary abelian extensions of algebraic number fields. Although Hilbert himself discussed unramified abelian extensions only, i.e., what today is called the "Hilbert class field", it is evident from his introductory remarks that he clearly envisioned the possible generalization to the ramified case. And Takagi, giving class field theory a new turn, succeeded in completing Hilbert's program to its full extent [9],

The class number h_K of an algebraic number field K is a basic object in Class field theory, extensively studied since the 19th century. Yet, little is known of its values in general. As we said before, one may consider it to measure the failure of the unique factorization in the ring of integers.

There does not exist a practical method to compute h_K in general, but an efficient algorithm exists, for instance, for quadratic fields and for some other fields of very small degree.

The class number h_K can be computed for extensions with small degree and discriminant, however computations take a very long time for higher extensions.

In our thesis, we are going to give a survey on some congruences on prime factors of class number of algebraic extensions.

In the first chapter we give some preliminaries on basic topics and concepts in abstract algebra, especially on groups, rings and field extensions in order to remember some of most wanted definitions and theorems such as normality, separability, solvability, Galois extensions, and others.

The subject of class number is one of the most deep, difficult and advanced topics in class field theory, which is emerged from algebraic number theory, and in order to put the reader in the mood of this subject, and understand its terms we have given in the second, and the third chapters the basic and wanted definitions, theorems and results of algebraic number theory and class field theory briefly or detailed according to its importance and utilization in our thesis.

Finally we study a paper of Roland Queme on some congruences of prime factors of class number of finite algebraic extensions.

Chapter 1

Preliminaries

In this chapter we study some basic concepts in Abstract algebra. It consists of two sections, in the first one , we mention some basic definitions and theorems in Group, Ring and field theory, that are necessary needed for understanding this thesis.
In the second section we define extension fields, and give some important related theorems and results needed for our research.
The definitions and facts in this chapters are taken from "Thomas W. Hungerford, ALGEBRA, Graduate Texts in Mathematics." [17].

1.1 Groups, Rings, Modules and Fields

Definition 1.1.1. [17]

- A **semigroup** is a nonempty set G together with a binary operation on G which is

  1. associative: $a(bc) = (ab)c$ for all $a, b, c \in G$;

     a **monoid** is a semigroup G which contains a

  2. (two-sided) identity element $e \in G$ such that $ae = ea = a$ for all $a \in G$.

- A **group** is a monoid G such that

1. for every $a \in G$ there exists a (two-sided) inverse element $a^{-1} \in G$ such that $a^{-1}a = aa^{-1} = e$.

   A semigroup G is said to be **abelian** or **commutative** if its binary operation is

2. commutative: $ab = ba$ for all $a, b \in G$.

- A nonempty subset H of a group G that is closed under the operation in G is said to be a **subgroup** of G, and denoted by $H \leq G$ if H is itself a group under the operation in G.

Definition 1.1.2. [17] If $a,\ b\ \in G$, $N \leq G$, then

- a is **right congruent** to b modulo N ($a\ \equiv_r b\ mod\ N$) if $ab^{-1} \in N$.
- $Na\ =\ \{na\ :\ n\ \in\ N\}$ is called the **right cosset** of N in G.

Theorem 1.1.1. *If N is a subgroup of a group G, then the following conditions are equivalent.*

1. *Left and right congruence modulo N coincide (that is, define the same equivalence relation on G);*
2. *every left coset aN of N in G is a right coset Na of N in G;*
3. *$aN = Na$ for all $a \in G$;*
4. *for all $a \in G$, $aNa^{-1} \subset N$, where $aNa^{-1} = \{ana^{-1} | n \in N\}$;*
5. *for all $a \in G$, $aNa^{-1} = N$.*

Proof. See [17] page 41. □

Definition 1.1.3. [17]

- A subgroup N of a group G which satisfies the equivalent conditions of Theorem (1.1.1) is said to be **normal** in G (or a **normal subgroup** of G); we write $N \lhd G$ if N is normal in G.

Theorem 1.1.2. *If N is a normal subgroup of a group G and G/N is the set of all (left) cosets of N in G, then G/N is a group of order $[G : N]$ under the binary operation given by $(aN)(bN) = abN$.*

Proof. See [17] page 42. □

- If N is a normal subgroup of a group G, then the group G/N, in (Theorem (1.1.2)), is called the **quotient group** or **factor group** of G by N. If G is written additively, then the group operation in G/N is given by $(a + N) + (b + N) = (a + b) + N$.
- If $H \leq G$, then gHg^{-1} is a subgroup of G called the **conjugate subgroup** of H by g.

Definition 1.1.4. [17]

- Let G be a group. The subgroup of G generated by the set $\{aba^{-1}b^{-1} : \ a, b \in G\}$ is called the **commutator subgroup** of G, and it is denoted by G'.
- The elements $aba^{-1}b^{-1}$; $(a, b \in G)$ are called **commutators**.

Theorem 1.1.3. *If G is a group, then G' is normal subgroup of G and G/G' is abelian.*
Moreover, if N is a normal subgroup of G, then G/N is abelian if and only if N contains G'.

Proof. See [17] page 102. □

- Let G be a group and let $G^{(1)} = G'$, then for $i \geq 1$, define $G^{(i)}$ by $G^{(i)} = (G^{(i-1)})'$, $G^{(i)}$ is called the i^{th} **derived subgroup** of G. This gives a sequence of subgroups of G, each normal in the preceding one $G \trianglerighteq G^{(1)} \trianglerighteq G^{(2)} \trianglerighteq$ .....
Actually each $G^{(i)}$ is a normal subgroup of G.
- A group G is said to be **solvable** if $G^{(n)} = \langle e \rangle$ for some n.
i.e if G has a normal series $\langle e \rangle = G^{(n)} \trianglelefteq G^{(n-1)} \trianglelefteq$ ..... $\trianglelefteq G^{(0)} = G$.

Remark 1.1.1. Abelian group are solvable.

Proof. See [17] page 103. □

Definition 1.1.5. [17]

- Let G be a group and X a subset of G. Let $\{H_i : i \in I\}$ be the family of all subgroups of G which contain X. Then $\bigcap_{i\in I} H$ is called the **subgroup of G generated by the set** X and denoted by $\langle X\rangle$. The elements of X are the **generators** of the subgroup $\langle X\rangle$. If $X = \{a_1, ...a_n\}$, we write $\langle a_1, ..., a_n\rangle$ in place of $\langle X\rangle$. If $G = \langle a_1, ..., a_n\rangle$, $a_i \in G$, G is said to be **finitely generated**.

- If $a \in G$, the subgroup $\langle a\rangle$ is called the **cyclic (sub)group generated by** a.

- The **order** of an element a in a group G(denoted by $|a|$) is the least positive n such that $a^n = 1$, if no such n exists, $|a| = \infty$.

- Let p be a prime number, the group G is said to be a **p-group** if the order of each element of G is a power of p.

- If G is a finite group, then G is a $p-$group if and only if $\mid G \mid = p^r$ for some positive integer r.

- If $\mid G \mid = p^r m$ for some positive integer m, where $p \nmid m$, then a subgroup P of G of order p^r is called a **Sylow p-subgroup** of G.
  Thus P is a $p - subgroup$ of G of maximum order.

Definition 1.1.6. [17]

- Let $G_1, G_2, \ldots, G_n$ be a finite collection of groups. The **direct product** of $G_1, G_2, \ldots, G_n$ denoted by $G_1 \bigoplus G_2 \bigoplus \ldots \bigoplus G_n$ is the set of all n tuples for which the $i'th$ component is an element of G_i, and the operation is componentwise.

  Theorem 1.1.4. *Every finitely generated abelian group G is (isomorphic to) a finite direct sum of cyclic groups, each of which is either infinite or of order a power of a prime p.*

Proof. See [17] page 76. □

Definition 1.1.7. [17]

- A **ring** is a nonempty set R together with two binary operations (usually denoted as addition $(+)$ and multiplication) such that:

  1. $(R, +)$ is an abelian group;
  2. $(ab)c = a(bc)$ for all $a, b, c \in R$ (associative multiplication);
  3. $a(b + c) = ab + ac$ and $(a + b)c = ac + bc$ (left and right distributive laws).

  If in addition:

  4. $ab = ba$ for all $a, b \in R$, then R is said to be a **commutative ring**.

  If R contains an element 1_R such that

  5. $1_R a = a l_R = a$ for all $a \in R$, then R is said to be a **ring with unity**.

- Let R be a ring and S a nonempty subset of R that is closed under the operations of addition and multiplication in R.

  – If S is itself a ring under these operations, then S is called a **subring of** R.

  – A subring I of a ring R is a **left ideal** provided

  $$r \in R \quad \text{and} \quad x \in I \quad \text{implies} \quad rx \in I;$$

  – I is a **right ideal** provided

  $$r \in R \quad \text{and} \quad x \in I \quad \text{implies} \quad xr \in I;$$

  – **I is an ideal** if it is both a left and right ideal.

  Example 1.1.1. *For any ring R , $\{0\}$ and R are ideals of R.*

Definition 1.1.8. [17]

- A commutative ring R with unity $I_R \neq 0$ and no zero divisors is called an **integral domain**.

  A ring D with unity $I_D \neq 0$ in which every nonzero element is a unit is called a **division ring**.

- A **field** is a commutative division ring.

Definition 1.1.9. [17]

- Let X be a subset of a ring R. Let $\{A_i | i \in I\}$ be the family of all [left] ideals in R which contain X. Then $\bigcap_{i \in I} A_i$, is called the **[left] ideal generated by** X. This ideal is denoted (X). The elements of X are called **generators** of the ideal (X). If $X = \{x_1, x_2, \ldots, x_n\}$, then the ideal (X) is denoted by $(x_1, x_2, \ldots, x_n)$ and said to be **finitely generated**.

- An ideal (x) generated by a single element is called a **principal ideal**.

- A **principal ideal ring** is a ring in which every ideal is principal.

- A principal ideal ring which is an integral domain is called a **principal ideal domain**.

  Remark 1.1.2. [20] Let I and J be ideals of R, then

  1. $I + J = \{a + b : a \in I,\ b \in J\}$ is the smallest ideal containing both I and J.
  2. $I \cap J$ is an ideal.
  3. The set $\{ab :\ a \in I,\ b \in J\}$ is not in general an ideal of R.
  4. $IJ = \{a_1b_1 + a_2b_2 + ... + a_nb_n : a_1, ...a_n \in I, b_1, ...b_n \in J\}$ is an ideal of R.

Definition 1.1.10. [17]

- Let R be a ring, a **(left) R-module** is an additive abelian group A together with a function $R \times A \longrightarrow A$ (the image of (r, a) being denoted by (ra) such that for all $r, s \in R$ and $a, b \in A$:

  1. $r(a + b) = ra + rb$.
  2. $(r + s)a = ra + sa$.

3. $r(sa) = (rs)a$.

   If R has an unity element 1_R, and

4. $1_R a = a$ for all $a \in A$, then A is said to be a **unitary R-module**.

   If R is a division ring, then a unitary R-module is called a **(left) vector space**.

Example 1.1.2. *Every additive abelian group G is a unitary Z-module; see [17], page 169*

- Let R be a ring, A an R-module and B a nonempty subset of A. B is a **submodule** of A provided that B is an additive subgroup of A and $rb \in B$ for all $r \in R,\ b \in B$.

- If X is finite, and X generates the module B, then B is said to be **finitely generated**.

- If $X = \phi$, then X clearly generates the *zero* module.

- If X consists of a single element, $X = \{a\}$, then the submodule generated by X is called the **cyclic (sub)module generated by** a.

- Finally, if $\{B_i : i \in I\}$ is a family of submodules of A, then the submodule generated by $X = \bigcup_{i \in I} B_i$ is called the sum of the modules B_i.

- If the index set I is finite, then the sum of $B_1, \ldots, B_n$ is denoted $B_1 + B_2 + \ldots B_n$.

Definition 1.1.11. [17]

- Let S be an extension ring of a ring R and $s \in S$. If there exists a monic polynomial $f(x) \in R[x]$ such that s is a root of f (that is, $f(s) = 0$), then s is said to be **integral over** R.

  If every element of S is integral over R, then S is said to be an **integral extension** of R.

  Theorem 1.1.5. *Let S be an extension ring of R and let R' be the set of all elements of S that are integral over R. Then R' is an integral extension ring of R which contains every subring of S that is integral over R.*

Proof. See [17], page 397. □

- If S is an extension ring of R, then the ring R' of Theorem (1.1.5) is called the **integral closure** of R in S.
  If $R' = R$, then R is said to be **integrally closed** in S.

Definition 1.1.12. [17]

- Let D be an integral domain. A polynomial $f(x)$ from $D[x]$ that is neither the zero polynomial nor a unit in $D[x]$ is said to be **irreducible over** D if, whenever $f(x)$ is expressed as a product $f(x) = g(x)h(x)$, with $g(x)$ and $h(x)$ from $D[x]$, then $g(x)$ or $h(x)$ is a unit in $D[x]$.

- A nonzero nonunit element of $D[x]$ that is not irreducible over D is called **reducible over** D.

- In the case that an integral domain is a field F it is equivalent and more convenient to define a nonconstant $f(x) \in F[x]$ to be irreducible if $f(x)$ cannot be expressed as a product of two polynomials of lower degree.

Definition 1.1.13. [17] Let R and S be rings then a function $f : R \longrightarrow S$ is

- **Homomorphism** of rings if

  1. $f(a + b) = f(a) + f(b)$.
  2. $f(ab) = f(a)f(b)$. for all $a,\ b \in R$.

- **Monomorphism** of rings if f is homomorphism injective.

- **Epimorphism** of rings if f is homomorphism surjective.

- **Isomorphism** of rings if f is homomorphism, injective and surjective.

- Monomorphism of rings $R \longrightarrow S$ is sometimes called an **embedding** of R in S.

- An Isomorphism $R \longrightarrow R$ is called an **automorphism** of R.

1.2 Extension Field

Definition 1.2.1. [17]

- A field F is said to be an **extension field** of K (or simply an **extension of** K) provided that K is a subfield of F, and we write E/F.
- Let F be an extension field of K.
  - An element u of F is said to be **algebraic over** K provided that u is a root of some nonzero polynomial $f \in K[x]$.
  - If F is an extension field of K, and $u \in F$ is algebraic over K, then the quotient field $K(u)$ is the field of rational functions in u over K; i.e. $K(u) = \{f/g\,;\ f,\ g \in K[u]\}$.
  - If u is not a root of any nonzero $f \in K[x]$, u is said to be **transcendental over** K.
  - F is called an **algebraic extension of** K if every element of F is algebraic over K.
  - F is called a **transcendental extension** if at least one element of F is transcendental over K.

    Example 1.2.1. *Let Q, R and C be the fields of rational, real, and complex numbers respectively. Then $i \in C$ is algebraic over Q and hence over R; in fact, $C = R(i)$.*
    It is a nontrivial fact that $\pi, e \in R$ are transcendental over Q; see, for instance, I. Her- stein [7], so R is transcendental extension of Q

Theorem 1.2.1. *[17] If F is an extension field of K, and $u \in F$ is algebraic over K, then $K(u) \cong K[x]/(f)$, where $f \in K[x]$ is an irreducible monic polynomial of degree $n > 1$ uniquely determined by the conditions that $f(u) = 0$ and $g(u) = 0$ $(g \in K[x])$ if and only if f divides g.*

Proof. See [17] page 234. □

Definition 1.2.2. [17]

- Let $u \in F$ be algebraic over K. The monic irreducible polynomial f of Theorem (1.2.1) is called the **irreducible (or minimal or minimum) polynomial** of u. The degree of u over K is $degf = [K(u) : K]$.

- A **quadratic field** is an algebraic number field K of degree *two* over Q.

- Let F be a field and $f \in F[x]$ a polynomial of positive degree, f is said to **split over** F (or to **split in** $F[x]$) if f can be written as a product of linear factors in $F[x]$; that is, $f(x) = u_o(x - u_1)(x - u_2)\dots(x - u_n)$ with $u_i \in F$.

- Let K be a field and $f \in K[x]$ a polynomial of positive degree. An extension field F of K is said to be a **splitting field over K of the polynomial** f if f splits in $F[x]$ and $F = K(u_1, \dots, u_n)$ where $u_1, \dots, u_n$ are the roots of f in F. i.e.: $K = F(u_1, \dots, u_n)$ which is the smallest field containing $F, u_1, \dots, u_n$.

  Example 1.2.2. *The only roots of* $x^2 - 2$ *over* Q *are* $\sqrt{2}$ *,*$-\sqrt{2}$ *and* $x^2 - 2 = (x - \sqrt{2})(x + \sqrt{2})$. *Therefore* $Q(\sqrt{2}) = Q(\sqrt{2}, -\sqrt{2})$ *is splitting field of* $x^2 - 2$ *over* Q.

- An algebraic extension field F of K is **normal over K (or a normal extension)** if every irreducible polynomial in $K[x]$ that has a root in F actually splits in $F[x]$.

Definition 1.2.3. [17]

- Let F be a field and $f \in F[x]$ be a polynomial, if c is a root of f with multiplicity 1, then it is said to be simple root. If c has multiplicity $m > 1$, c is called a **multiple root.**

- Let K be a field and $f \in F[x]$ an irreducible polynomial. The polynomial f **is said to be separable** if in some splitting field of f over K every root of f is a simple root.

- If F is an extension field of K and $u \in F$ is algebraic over K then u **is said to be separable over** K provided its irreducible polynomial is separable.

  Example 1.2.3. *$x^2 + 1 \in Q[x]$ is separable since $x^2 + 1 = (x + i)(x - i)$ in $C[x]$.*

- If F is an extension field of K and every element of F is separable over K, then F **is said to be a separable extension of** K.

Definition 1.2.4. [17] If E/F is an extension, then **the Galois group** $Gal(E/F)$ is the set of $F-$ automorphism of E where σ is $F-$ automorphism of E, if $\sigma : E \longrightarrow E$ is an automorphism such that $\sigma(x) = x \ \ \forall \ x \in F$.

Example 1.2.4. *Let C be the field of complex numbers, Q be the field of rational numbers, R be the field of real numbers, and F be any field. Then*

- *$Gal(F/F)$ is the trivial group that has a single element, namely the identity automorphism.*

- *$Gal(C/R)$ has two elements, the identity automorphism and the complex conjugation automorphism.*

Remark 1.2.1.

- It is a well-known property of fields that their only ideals are the zero ideal and the whole field itself. Therefore, the kernel is 0, so any embedding of fields is a monomorphism.

- Moreover, F is isomorphic to the subfield $\sigma(F)$ of E. This justifies the name embedding of fields.

Definition 1.2.5. [17] $Aut_K F$ is the group of all $K - automorphisms$ of F which is the Galois group of F over K

Definition 1.2.6. [17] Let F be an extension field of K such that the fixed field of the Galois group $Aut_K F$ is K itself. Then F is said to be a **Galois extension (field)** of K or to be **Galois over** K.

Example 1.2.5. *The field $K = Q(i)$, the rationales adjoined by the imaginary number i , over Q , is a Galois extension.*

Theorem 1.2.2. *[17] **(Fundamental Theorem of Galois Theory)** If F is a finite dimensional Galois extension of K, then there is a one-to-one correspondence between the set of all intermediate fields of the extension and the set of all subgroups of the Galois group $Aut_K F$ (given by $E \longmapsto E' = Aut_E F$) such that:*

1. *The relative dimension of two intermediate fields is equal to the relative index of the corresponding subgroups; in particular, $Aut_K F$ has order $[F : K]$;*

2. *F is Galois over every intermediate field E, but E is Galois over K if and only if the corresponding subgroup $E' = Aut_E F$ is normal in $G = Aut_K F$, in this case G/E' is (isomorphic to) the Galois group $Aut_K E$ of E over K.*

Proof. See [17] page 246. □

Chapter 2

Number Fields And Rings Of Algebraic Integers

This chapter is about fundamental concepts in Algebraic number theory.
It consists of two sections, in the first section, we define the number field,and give some related definitions and theorems, and some illustrative examples.
We have also defined the norm, the trace, and some examples and proprieties.
In the second section, we define the ideals of the ring of algebraic integers which plays a fundamental rule in algebraic number theory, we introduce some related theorems and results needed for the next chapters.

2.1 Number fields

Definition 2.1.1. [12]

- A **number field** $F = Q(\theta)$ is a finite (*and hence algebraic*) field extension of the field of rational numbers Q.
  Thus F is a field that contains Q and has finite dimension when considered as a vector space over Q.

- θ is called a **generator** of F

Example 2.1.1. *The smallest and most basic number field is the field Q of rational numbers.*

Example 2.1.2. *If $f(X) = 2X^2 - 3$, then it's irreducible over Q, and $\theta = \sqrt{\frac{3}{2}}$ is a root, so $\sqrt{\frac{3}{2}}$ is an algebraic number,*
$K = Q(\frac{\sqrt{3}}{2}) = \{\sum_{i=0}^{1} A_i(\frac{\sqrt{3}}{2})^i : A_i \in Q\} = \{A_0 + A_1(\frac{\sqrt{3}}{2}) : A_0, A_1 \in Q\}$ is a number field.

Definition 2.1.2. [12] A number α in a number field K/Q is called an **algebraic integer** if α is the root of a monic polynomial with coefficients in Z.

Remark 2.1.1. All algebraic integers are algebraic numbers. However the converse need not be true.

Proof. If $\alpha \in K/Q$ is an algebraic integer, then there exist a polynomial $f(x) = a_n x_n + \ldots + a_0$ such that $a_n, \ldots, a_0$, not all zero, are in Z and $f(\alpha) = 0$, so $a_n, \ldots, a_0$ not all zero, are in Q, that is α is an algebraic number.
For the converse, consider the following example.
Example: $\frac{\sqrt{2}}{3}$ is an algebraic number but not an algebraic integer.
Proof:
Consider the polynomial $f(x) = 9x^2$ - 2, which is in $Q[x]$. Since $f(\frac{\sqrt{2}}{3}) = 0$, then $\frac{\sqrt{2}}{3}$ is an algebraic number. Now assume that $\frac{\sqrt{2}}{3}$ is an algebraic integer. Then there exists a monic polynomial in $Z[x]$, say $g(x) = x_n + b_n x_{n-1} + \ldots + b_0$, which has $\alpha = \frac{\sqrt{2}}{3}$ as a root. So

$$g(\alpha) \;=\; g(\tfrac{\sqrt{2}}{3}) = (\tfrac{\sqrt{2}}{3})^n + b_{n-1}(\tfrac{\sqrt{2}}{3})^{n-1} + \ldots + b_0 \;=\; 0,$$

so

$$(\sqrt{2})^n + b_{n-1}(\sqrt{2})^{n-1}(3) + \ldots + b_0(3)^n \;=\; 0 \tag{2.1.1}$$

Now if i is odd, then $(\sqrt{2})^i = (\sqrt{2})^{2t+1} = \sqrt{2}(\sqrt{2})^{2t} = \sqrt{2}.2^t = \sqrt{2}/2^{\frac{i-1}{2}}$, for some $t \in Z$
and if i is even then $(\sqrt{2})^i = (\sqrt{2})^{2t} = 2^t = 2^{\frac{i}{2}}$, for some $t \in Z$.

So equation 2.1.1 becomes,

$$\sum_{i\ odd} b_i(\sqrt{2})^i 3^{n-i} + \sum_{i\ even} b_i(\sqrt{2})^i 3^{n-i} = 0$$
$$\sum_{i\ odd} b_i\sqrt{2}.2^{\frac{i-1}{2}}3^{n-i} + \sum_{i\ even} b_i 2.2^{\frac{i-2}{2}}.3^{n-i} = 0$$
$$\sqrt{2}\sum_{i\ odd} b_i.2^{\frac{i-1}{2}}3^{n-i} + 2\sum_{i\ even} b_i.2^{\frac{i-2}{2}}.3^{n-i} = 0$$
$$\sqrt{2}(x) + 2(y) = 0, \text{ where}$$
$$x = \sum_{i\ odd} b_i.2^{\frac{i-1}{2}}3^{n-i}, \quad y = \sum_{i\ even} b_i.2^{\frac{i-2}{2}}.3^{n-i} = 0$$
$$\text{So } x = 0 \text{ and } y = 0, \text{ but } 3 \mid 0, \text{ so } 3 \mid x \text{ and } 3 \mid y$$

Case(1)

If n is even , then $y = b_n 2^{\frac{i-1}{2}}.3^{n-n} + b_{n-2}2^{\frac{i-1}{2}}.3^2 + \ldots + b_0 2^{\frac{n}{2}}.3^n$, but $b_n = 1,\ \ 3^0 = 1$, so $y = 2^{\frac{n-2}{2}} + 3(b_{n-2}.2^{\frac{n-4}{2}}.3 + \ldots + b_0.2^{\frac{n}{2}}.3^{n-1})$, and since $3 \mid y$, and $3 \mid 3(b_{n-2}.2^{\frac{n-4}{2}}.3 + \ldots + b_0.2^{\frac{n}{2}}.3^{n-1})$, then $3 \mid 2^{\frac{n-2}{2}}$ which is impossible.

Case(2)

If n is odd then, $x = b_n 2^{\frac{n-1}{2}}.3^{n-n} + b_{n-2}2^{\frac{n-3}{2}}.3^2 + \ldots + b_1 2^0.3^{n-1}$, but $b_n = 1,\ 3^0 = 1$, so $x = 2^{\frac{n-1}{2}} + 3(b_{n-2}.2^{\frac{n-3}{2}}.3 + \ldots + b_1.3^{n-2})$, but $3 \mid x$, $3 \mid 3(b_{n-2}.2^{\frac{n-3}{2}}.3 + \ldots + b_1.3^{n-2})$. So $3 \mid 2^{\frac{n-1}{2}}$, which is impossible.

In either cases, we get contradiction and hence, we conclude that the algebraic number $\frac{\sqrt{2}}{3}$ is not an algebraic integer. □

Example 2.1.3. *The only algebraic integers in the field of rational numbers are the integers.*

Definition 2.1.3. [4]

- Let K/Q be a number field. If $\phi_1, \phi_2, \ldots, \phi_r$ are linearly independent over Q, and for any $\alpha \in K,\ \alpha = \Sigma_{i=1}^{r} A_i\phi_i$, then $\{\phi_i, i = 1, \ldots, r\}$ is said to form a **basis** for K over Q.

- Let K/Q be a number field with $[K : Q] = n$. Then, an **integral basis** of K is a set of algebraic integers $\phi_1, \phi_2, \ldots, \phi_n$ such that every algebraic integer α of O_K "***where O_K is the set of algebraic integers in K/Q***" has a unique representation of the form $\alpha = \Sigma_{j=1}^{n} a_j\phi_j,\ a_j \in \mathbb{Z}$, and so every integral basis is also a basis.

Definition 2.1.4. [20] Let a and b be elements of a group G. We say a and b are **conjugate** in G (and call b a conjugate of a) if $x^{-1}ax = b$ for some x in G.

Remark 2.1.2. [4]

- If θ is a generator of an algebraic number field K, and θ is of degree n, then K is said to be of degree n over Q, or in symbols, $[K : Q] = n$.
- In fact, K is an n-dimensional vector space over Q, with a basis $1, \theta, \theta^2, ..., \theta^{n-1}$.
- Every element of K is of the form $\alpha = f(\theta)$, $f \in Q[x]$, $degf \leq n-1$, and this representation is unique.
- If we replace θ successively by its conjugates, we obtain the n field conjugates $\alpha^{(j)} = f(\theta^{(j)})$ of α.

Lemma 2.1.1. *[2] Let R be a subring of a commutative ring S with unity and let $s \in S$. Then the following are equivalent :*

- *s is integral over R.*
- *$R[s]$ is a finitely generated R-module; where $R[s]$ is the ring of all $R-$linear combinations of powers of s.*

Proof. See [2] page 692. □

Proposition 2.1.2. *[10] Let K be an extension field of Q,then the set O_K of algebraic integers of K forms a ring.*

Proof. Since algebraic integers are the elements of a field K, then the commutative, associative in addition and product, left, and right distributive properties in definition (1.1.7) holds immediately for them. So, to prove that the set of algebraic integers form a ring, we need to establish the other properties for the set of algebraic integers.

Proving that O_K is closed under addition, and multiplication :
Let s and t be an algebraic integers in O_K, then s and t are integral over $R = Z$. Thus,

by lemma (2.1.1) both $R[s]$ and $R[t]$ are finitely generated modules by $\{s, s^2, \ldots, s^n\}$, and $\{t, t^2, \ldots, t^m\}$ respectively, i.e

$R[s] = Rs + Rs^2 + \ldots + Rs^n$

$R[t] = Rt + Rt^2 + \ldots + Rt^m$

and so $R[s,t] = R_{st} + \ldots + Rs^i t^j + \ldots + Rs^n t^m$

But $1 \in R$, then $R[s,t]$ is a ring containing $s+t$, and st that is also a finitely generated R-module. Hence, whenever s, and t are integral over Z, then so are $s+t$, and st. Thus, $s+t$, and st belong to the set of algebraic integers O_K whenever s, and t belong to it.

Proving the existent, and uniqueness of additive identity:

Take a polynomial $P(x) = x^n + a_{n-1}x^{n-1} + a_{n-2}x^{n-2} + ... + a_2x^2 + a_1x \quad , \quad a_i's \ \in Z.$

Clearly, $P(x) \in Z[x]$, and $P(0) = 0$. Thus, $\alpha = 0$ is an algebraic integer.

Proving the existence, and uniqueness of additive inverse:

Let $\alpha \in K$ be an algebraic integer. So it is a zero for a monic polynomial $P(x) = x^n + a_{n-1}x^{n-1} + a_{n-2}x^{n-2} + ... + a_2x^2 + a_1x + a_0 \quad , \quad a_i's \ \in Z.$

Therefore, $P(\alpha) = \alpha^n + a_{n-1}\alpha^{n-1} + a_{n-2}\alpha^{n-2} + ... + a_2\alpha^2 + a_1\alpha + a_0 = 0$

- Case(1), when n is odd, take a polynomial
  $Q(x) = x^n + (-1)^n a_{n-1}x^{n-1} + (-1)^{n-1}a_{n-2}x^{n-2} + ... + (-1)^2 a_1 x + (-1)a_0$. So it is clear that $Q(x) \in Z[x]$.
  Now, $Q(-\alpha) = -\alpha^n - a_{n-1}\alpha^{n-1} - a_{n-2}\alpha^{n-2} - ..... - a_2\alpha^2 - a_1\alpha - a_0 = -P(\alpha) = 0.$

- Case(2), when n is even, take a polynomial
  $T(x) = x^n + (-1)^{n-1} a_{n-1}x^{n-1} + (-1)^{n-2}a_{n-2}x^{n-2} + ... + (-1)a_1 x + (-1)a_0$. So it is clear that $T(x) \in Z[x]$.
  Now, $T(-\alpha) = \alpha^n + a_{n-1}\alpha^{n-1} + a_{n-2}\alpha^{n-2} + ... + a_2\alpha^2 + a_1\alpha + a_0 = P(\alpha) = 0.$

So, in both cases, $(-\alpha)$ is a root of a monic polynomial with coefficients in Z. Thus $(-\alpha)$ is an algebraic integer. That is, for any algebraic integer α, there exists a corresponding algebraic integer $(-\alpha)$ such that $\alpha + (-\alpha) = (-\alpha) + \alpha = 0$.

So, we have proved all the properties of a ring (definition (1.1.7)), for the set of algebraic integers. Therefore, the set of algebraic integers O_K form a ring. $\square$

Theorem 2.1.3. *[15] Let $f(X) = X^n + A_1X^{n-1} + ... + A_n, (A_j \in Q)$ be an irreducible polynomial over Q. Then $f(X) = 0$ has n distinct roots in C.*

Proof. Suppose that α is a repeated root of $f(X) = 0$. Then $f(X) = (X-\alpha)^2 g(X)$ where $g(X) \in C[X]$. Thus $f'(X) = (X-\alpha)^2 g'(X) + 2(X-\alpha)g(X)$, and so $f(\alpha) = f'(\alpha) = 0$. Let h be the greatest common divisor of f and f'. Then $h = uf + vf'$ for some $u, v \in Q[X]$. Thus $h(\alpha) = u(\alpha)f(\alpha) + v(\alpha)f'(\alpha) = 0$. But since $h|f$ and f is irreducible, then $h = 1$ or $h = f$. Since $h(\alpha) = 0$, then $h = f$. But then $f|f'$ which is impossible since the leading term of f' is nx^{n-1}. Therefore f has no repeated roots as desired. □

Note [4] Let $f(x) = x^n + A_1x^{n-1} + ... + A_n, (A_j \in Q)$ be an irreducible polynomial over Q, then

- The $n-$roots of $f(x) = 0$ are all distinct and will be denoted by $\alpha = \alpha_1, \alpha_2, ..., \alpha_n$.
- The algebraic numbers α_j's "not necessarily integers" are called **conjugates of** α.

Example 2.1.4. *Consider $f(x) = x^3 - 1$, then the roots are $1, \ -\frac{1}{2} + \frac{\sqrt{3}}{2}i$ and $-\frac{1}{2} - \frac{\sqrt{3}}{2}i$. The later two roots are conjugate elements in the field $K = Q(\sqrt{-3})$.*

Definition 2.1.5. [18] Let $Q(\alpha)$ be an algebraic number field for some algebraic number α and let $\alpha_1, ..., \alpha_n$ be the conjugates of α, then the fields $Q(\alpha_j)'s, \ \ 1 \leq j \leq n$ are all isomorphic to $Q(\alpha)$ each being generated by an element with minimum polynomial f, via the isomorphism $\sigma_j : Q(\alpha) \to Q(\alpha_j)$ by setting $\sigma_j(g(\alpha)) = g(\alpha_j)$ where $g \in Q[x]$.

Now, if $\beta \in Q(\alpha)$, we define the **norm**

$$N(\beta) = \Pi_{j=1}^{n} \sigma_j(\beta) \quad ,$$

and the **Trace**

$$T(\beta) = \Sigma_{j=1}^{n} \sigma_j(\beta)$$

Remark 2.1.3. [18] Since the σ_j preserve addition,and multiplication, then the following properties are almost immediate:

- $N(\beta\gamma) = N(\beta)N(\gamma)$ for all $\beta, \gamma \in Q(\alpha)$.
- $N(c\beta) = c^n N(\beta)$ for all $c \in Q,\ \beta \in\ Q(\alpha)$.
- $T(\beta + \gamma) = T(\beta) + T(\gamma)$ for all $\beta, \gamma \in\ Q(\alpha)$.
- $T(c\beta) = cT(\beta)$ for all $c \in Q,\ \beta \in\ Q(\alpha)$.
- $N(0) = 0, N(1) = 1$.
- If $\beta \neq 0$ then $1 = N(1) = N(\beta).N(1/\beta)$ so that $N(\beta) \neq 0$.

Note 2.1.4. *The norm $N(\beta)$, and trace $T(\beta)$ depends on the field $Q(\alpha)$ as well as the number β.*
If we wish to be strict, we should use the notation $N_{Q(\alpha)/Q}(\beta)$, and $T_{Q(\alpha)/Q}(\beta)$ instead.

Proposition 2.1.5. *[18] Given a number field $K = Q(\alpha)$, If α is an algebraic number and $\beta \in O_K$ for $K = Q(\alpha)$, then we have $T(\beta), N(\beta) \in Z$.*

Proof. See [15], page 12. □

Example 2.1.5. *[15]"**How to find** O_K"*

Proof. Consider a quadratic field which is a number field of the form $Q(\sqrt{m})$, where $m \in Q$, but $\sqrt{m} \notin Q$.
Without lost of generality we may assume that m is a square free integer, " because $Q(\sqrt{r^2 m}) = Q(\sqrt{m})$ for any nonzero $r \in Q$.
So m is not divisible by the square of any prime number.
Now when $m > 0$, then $Q(\sqrt{m})$ is a real quadratic field, and when $m < 0$, then $Q(\sqrt{m})$ is an imaginary quadratic field.
We want to compute O_K whenever $K = Q(\sqrt{m})$ is a quadratic field.
Let $\beta = a + b\sqrt{m} \in K$ with $a, b\ \in Q$. Now, suppose that $\beta \in O_K$, then $N(\beta), T(\beta) \in Z$,

then

$$T(\beta) = 2a \in Z, N(\beta) = a^2 - mb^2 \in Z$$
$$\Rightarrow [T(\beta)]^2 - 4N(\beta) = m(2b)^2 \in Z.$$

So $2b \in Z$, otherwise $2b$ would have a power of prime $p \in P$ divides its denominator, which implies that $p^2 \mid m$ which is impossible because m is square free.
Thus, since $2a, 2b \in Z$, we can write $\beta = \frac{1}{2}(2a + 2b\sqrt{m})$, take $c = 2a, d = 2b$ to get that $\beta = \frac{1}{2}(c + d\sqrt{m}), c, d \in Z$ "where a, b need not belong to Z"
But $4N(\beta) = 4(a^2 - mb^2) = (2a)^2 - (2b)^2m = c^2 - d^2m$, so $c^2 - d^2m \equiv\ 0\ mod\ 4$ but

1. m is square free, so $m \not\equiv\ 0\ mod\ 4$
2. Odd squares are congruent to 1 mod 4
3. Even squares are congruent to 0 mod 4

So, by above we have either

1. c and d are both even
   so, $a, b \in Z$ that is $O_K = \{a + b\sqrt{m},\ a, b \in Z\} = Z[\sqrt{m}]$.
   or

2. c and d are both odd, $m \equiv\ 1\ (mod\ 4)$ and then $m = 4t+1$ but $c^2 - md^2 \equiv 0(mod\ 4)$ that is $c^2 - (4t + 1)d^2 \equiv 0(mod\ 4)$, which implies that $c^2 \equiv d^2(mod\ 4)$. Thus $c \equiv d\ (mod\ 2)$.
   And so $O_K = \{\frac{c+d\sqrt{m}}{2},\ c, d \in Z,\ c \equiv d\ (mod\ 2)\}$.
   Now, since $c \equiv d\ mod\ 2$, then
   $2 \mid c - d$,so $c - d = 2t, t \in Z$, that is $c = 2t + d$
   Thus $O_K = \{\frac{2t+d+d\sqrt{m}}{2},\ t, d \in Z\}$
   $= \{t + \frac{d(1+\sqrt{m})}{2}, t, d \in Z\}$
   $= \{t + b(\frac{1+\sqrt{m}}{2}), t, d \in Z\}\ =\ \{a + b(\frac{1+\sqrt{m}}{2}); a, b \in Z\}$
   Therefore we have

$$O_K = Z[\tfrac{1+\sqrt{m}}{2}]$$

□

For example *For instance, if* $K = Q[\sqrt{7}]$*, then the integers of* K *are given by* $O_K = Z[\sqrt{7}]$ *"since* $7 \not\equiv 1$ *mod* 4*". The maps* σ_j*'s are given by*

$$\sigma_1(p + q\sqrt{7}) = p + q\sqrt{7}$$

$$\sigma_2(p + q\sqrt{7}) = p - q\sqrt{7}$$

Hence

$$N(p + q\sqrt{7}) = p^2 - 7q^2$$

and

$$T(p + q\sqrt{7}) = 2p$$

Definition 2.1.6. [18] Suppose that K is a number field, and O_K is the ring of algebraic integers, then:

- A **unit** in O_K is an element $\beta \in O_K$ such that $\frac{1}{\beta} \in O_K$.
- The set of units of O_K is denoted by $\mu(O_K)$**.**

Proposition 2.1.6. *[18] The set* $\mu(O_K)$ *forms a group under multiplication.*

Proof. See [18] page 77. □

Theorem 2.1.7. *[18] Suppose that* K *is a number field, and let* $\beta \in O_K$*, then* $\beta \in \mu(O_K)$ *if and only if* $N(\beta) = \pm 1$*.*

Proof. Suppose that $\beta \in \mu(O_K)$, then there exist $u \in O_K$ such that $\beta u = 1$, so by remark (2.1.5) $N(\beta).N(u) = 1$, but $N(\beta),\ N(u) \in Z$ by proposition (2.1.3), so we have $N(\beta) = \pm 1$.
Conversely, if $N(\beta) = \pm 1$, then $N(\beta) = \Pi_{j=1}^{n}\sigma_j(\beta) = \pm 1$, where the $\sigma' s$ are the monomorphisms $K \to C$. One factor, say $\sigma_1(\beta)$, is equal to β, all the others are integers. Put $u = \pm\,\sigma_2(\beta)\ldots\sigma_n(\beta)$ which is an algebraic integer since each $\sigma_j(\beta)$ is an algebraic integers, therefore $\beta u = 1$. Hence β is a unit. □

Example 2.1.6.

1. *For $Z = O_Q$ the only units are ± 1.*

2. *If $\beta = 1 + \sqrt{2} \in K = Q(\sqrt{2})$, then*
   $N(\beta) = \Pi_{j=1}^{2} \sigma_j(\beta) = g(\alpha_1)g(\alpha_2) = (1 + \sqrt{2})(1 - \sqrt{2}) = -1.$

So β is a unit, but $\beta > 1$, so $\beta^m \to \infty$ as $m \to \infty$ and also if m is a positive integer, then $\beta^m \in \mu(O_K)$, so $\mu(O_K)$ is infinite.
Note $N(1 + \sqrt{2})^m = [N(1 + \sqrt{2})]^m = (-1)^m = \pm 1.$

2.2 Ideals Of Rings Of Algebraic Integers

Definition 2.2.1. [18] Suppose that K is a number field, and $\beta, \gamma \in O_K$, with $\beta \neq 0$ we say that $\beta \mid \gamma$, **(β divides γ or γ is divisible by β)** if $\frac{\gamma}{\beta} \in O_K$, otherwise, we say $\beta \nmid \gamma$.

Theorem 2.2.1. *[15] Suppose that K is a number field, and let $\gamma, \beta \in O_K$, if $\beta \mid \gamma$, then $N(\beta) \mid N(\gamma)$ as integers.*

Proof. Suppose that $\beta \mid \gamma$, then there exist $\delta \in O_K$ such that $\gamma = \beta\delta$, and so $N(\gamma) = N(\beta)N(\delta)$, but $N(\beta),\ N(\delta) \in Z$, thus $N(\beta)|N(\gamma)$. □

Definition 2.2.2. [18]

- suppose that K is a number field, and let γ, β, and $\delta \in O_K$, then we say that β is **irreducible** if:

  1. $\beta \neq 0$
  2. β is not a unit, and
  3. if $\beta = \gamma\delta$, with $\gamma, \delta \in O_K$, then either γ or δ is a unit "we say here that β **associate to** δ and γ".

  Remark 2.2.1.

  1. For $\beta \in O_K$, if $N(\beta)$ is a prime number, then β is irreducible.

Proof. If $N(\beta) = p$, then

(a) $\beta \neq 0$.

(b) β is not a unit because $N(u) = \pm 1$ for any $u \in \mu(K)$.

(c) If $\beta = \gamma.\delta$, then $N(\beta) = N(\gamma)N(\delta)$,
but so $N(\gamma)N(\delta) = P \Rightarrow$ either $N(\gamma)$ or $N(\delta)$ equal to 1, that is either γ or δ is a unit, thus β is irreducible.

□

2. But if β is irreducible, then $N(\beta)$ needn't be prime.

Example 2.2.1.
For $K = Q(i)$, $O_K = Z[i]$, *so 3 is irreducible in* O_K, *but*
$N(3) = \sigma_1(\beta)\sigma_2(\beta) = (3 + 0.i).(3 + 0(-i)) = 3.3 = 9$
"since the conjugate of $3 + 0.i$ *in* $Q(i)$ *is* $3 + 0(-i)$*." So* $N(3) = 9$ *is not prime.*

- suppose that K is a number field, and let γ, β, and $\delta \in O_K$, then we say that β is a **prime** if:

  1. $\beta \neq 0$
  2. β is not a unit.
  3. If $\beta \mid \gamma\delta$, with $\gamma, \delta \in O_K$, then either $\beta \mid \gamma$ or $\beta \mid \delta$.

Theorem 2.2.2. *[18] Let* K *be a number field, if* β *is a prime element of* O_K*, then* β *is irreducible in* O_K.

Proof. Let β be a prime element of O_K, and suppose that $\beta = \gamma\delta$ with $\gamma, \delta \in O_K$. Then $\beta \mid \gamma\delta$, and sine β is prime, then $\beta \mid \gamma$, or $\beta \mid \delta$, say that $\beta \mid \gamma$, so $\delta = \beta/\gamma$ is a unit. Therefore β is irreducible. □

Remark 2.2.2. In general integral domains, it's not necessary that every irreducible is prime e.g.

In $Z[\sqrt{-3}]$, we have 2 as an irreducible element, because

$$N(2) = (2 + 0\sqrt{-3})(2 + 0\sqrt{-3}) = 4$$

so if $2 = x.y$, $x, y \in Z[\sqrt{-3}]$, neither x nor y is a unit, then $N(2) = N(x).N(y) \Rightarrow 4 = N(x).N(y)$.

So $N(x) = 2$, $N(y) = 2$ otherwise one of them say $N(x) = 2$, which means that there exist $a, b \in Z$ s.t $a^2 + 3b^2 = 2$ which is impossible.

So if $2 = x.y$, then either x or y is a unit that is 2 is irreducible

But 2 is not prime, because $2 = (1+\sqrt{-3})(1-\sqrt{-3})$ but $2 \nmid (1+\sqrt{-3})$ and $2 \nmid (1-\sqrt{-3})$, other wise $2 = (1 + \sqrt{-3})(a + b\sqrt{-3}) = (a - 3b) + (a + b)\sqrt{-3} \Rightarrow a - 3b = 2$ and $a + b = 0$ which is impossible in Z or $2 = (1 - \sqrt{-3})(a + b\sqrt{-3}) = (a + 3b) + (a - b)\sqrt{-3} \Rightarrow a + 3b = 2$ and $a - b = 0$ which is impossible in Z.

Then 2 is irreducible but not prime in $Z[\sqrt{-3}]$ which is O_K for $K = Q(\sqrt{-3})$.

Definition 2.2.3. [4]

- Let O_K be the ring of algebraic integers in some number field K of degree n over Q, and let $\alpha_j \in O_K (1 \leq j \leq k)$. The set $a = \{\lambda_1\alpha_1 + ... + \lambda_k\alpha_k\}$ obtained when the $\lambda_j' s$ range independently over O_K is said to be an **ideal of** O_K.
- The set of elements $\{\alpha_1, \alpha_2, ..., \alpha_k\}$ of O_K above are called **generators** of the ideal a, in symbols, $a = (\alpha_1, \alpha_2, ..., \alpha_k)$.

Definition 2.2.4. [4] Two ideals $\mathfrak{a}$ and $\mathfrak{b}$ of O_K are said to be **identical** "i.e $\mathfrak{a} = \mathfrak{b}$", if they consist of the same set of generators.

Remark 2.2.3. [4]

- The set $\{0\}$ consisting of the only element zero is an ideal. It will be denoted by $\mathfrak{o}$, but unless specific mention is made to the contrary, we shall always assume tacitly that any ideal $\mathfrak{a}$ under consideration is not $\mathfrak{o}$.

Also the whole ring O_K is clearly an ideal. For uniformity of notation we shall denote it by $\mathfrak{i}$ when we want to consider it as an ideal.

- The generators of a given ideal are by no means unique. In particular, one may suppress among them or add to them any integer α_0, where α_0 is not "linearly independent" of the others, that is which can be represented as a sum $\alpha_0 = \Sigma_i \lambda_i \alpha_i$ with α_i generators of $\mathfrak{a}, \lambda_i \in O_K$. Also without changing the ideal one may add or subtract from any generator products of any other generator by integers of the ring.

Theorem 2.2.3. *[4]Let O_K be the ring of algebraic integers in some number field K over Q, and let $\mathfrak{a}$ and $\mathfrak{b}$ be ideals of O_K, if the ideals $\mathfrak{a} = (\alpha)$ and $\mathfrak{b} = (\beta)$ are principal, then they are equal if and only if the generators α and β are associates,* i.e. their ratio is a unit in O_K.

Proof. See [4] page 220. □

Definition 2.2.5. [4] Let O_K be the ring of algebraic integers in some number field K over Q, and let $\mathfrak{a}$ and $\mathfrak{b}$ be ideals of O_K, if the ideals $\mathfrak{a} = (\alpha_1, \alpha_2, \ldots, \alpha_m)$ and $\mathfrak{b} = (\beta_1, \beta_2, \ldots, \beta_k)$ we call **product of $\mathfrak{a}$ and $\mathfrak{b}$** the ideal $\mathfrak{c}$ generated by all products $\alpha_i \beta_j$.

Example 2.2.2. $(1 - \sqrt{-5}) * (2, 1 + \sqrt{-5}) = (2(1 - \sqrt{-5}), 6)$ *in* $Q(\sqrt{-5})$.

Theorem 2.2.4. *[4] The multiplication of ideals is commutative and associative.*

Proof. See [4] page 220. □

Note 2.2.5. *We shall denote product of ideals by themselves as powers.*
For instance, $\mathfrak{a}.\mathfrak{a} = \mathfrak{a}^2, \mathfrak{a} \ldots \mathfrak{a} = \mathfrak{a}^m,\ \mathfrak{a}^0 = (1) = \mathfrak{i} = O_K$.

Definition 2.2.6. [4] Let O_K be the ring of algebraic integers in some number field K over Q, and let $\mathfrak{a}$, $\mathfrak{b}$, and $\mathfrak{c}$ be ideals of O_K, if $\mathfrak{a} = \mathfrak{b}.\mathfrak{c}$, we say that $\mathfrak{a}$ has the **factors** $\mathfrak{b}$ and $\mathfrak{c}$, and that $\mathfrak{b}$ and $\mathfrak{c}$ **divide** $\mathfrak{a}$; in symbols, $\mathfrak{b} \mid \mathfrak{a},\ \mathfrak{c} \mid \mathfrak{a}$.

Example 2.2.3. *In* $O_{Q(\sqrt{-5})}$, $(1 - \sqrt{-5}) * (2, 1 + \sqrt{-5}) = (2(1 - \sqrt{-5}), 6)$, *so we have*

- *The ideal* $(2(1-\sqrt{-5}),6)$ *has the factors* $(1-\sqrt{-5})$, *and* $(2,1+\sqrt{-5})$.
- *And so* $(1-\sqrt{-5})$, *and* $(2,1+\sqrt{-5})$ *divide* $(2(1-\sqrt{-5}),6)$.

Theorem 2.2.6. *[4] If* K *is algebraic number field,* $\mathfrak{a}=(\alpha)$ *and* $\mathfrak{b}=(\beta)$ *are principle ideals in* O_K, *then*

1. $\mathfrak{b} \mid \mathfrak{a} \Leftrightarrow \beta \mid \alpha$;
   and for all ideals $\mathfrak{a},\mathfrak{b},\mathfrak{c}$, *and* $\mathfrak{d}$ *we have.*
2. $\mathfrak{a} \mid \mathfrak{b},\ \mathfrak{b} \mid \mathfrak{c} \Rightarrow \mathfrak{a} \mid \mathfrak{c}$;
3. $\mathfrak{a} \mid \mathfrak{b} \Rightarrow \mathfrak{a}\mathfrak{d} \mid \mathfrak{b}\mathfrak{d}$;
4. $\mathfrak{i} \mid \mathfrak{a}$;
5. $\mathfrak{a} \mid \mathfrak{a}$

Proof. See [4] page 221. □

Definition 2.2.7. [4] We say that an algebraic integer α is **divisible by an ideal** $\mathfrak{a}$ if and only if the principle ideal (α) is divisible by $\mathfrak{a}$, that is , if and only if $\mathfrak{a} \mid (\alpha)$.

Theorem 2.2.7. *[4] Let* O_K *be the ring of algebraic integers in some number field* K *over* Q, *and let* $\mathfrak{a}=(\alpha_1,\alpha_2,.....,\alpha_m)$ *and* $\mathfrak{b}=(\beta_1,\beta_2,.....,\beta_k)$ *be ideals of* O_K, *If* $\mathfrak{a} \mid \mathfrak{b}$ *then* $\mathfrak{a} \supset \mathfrak{b}$ *(that is, each integer of* $\mathfrak{b}$ *belong to* $\mathfrak{a}$*).*

Proof. Suppose that $\mathfrak{a} \mid \mathfrak{b}$ for the ideals $\mathfrak{a}$ and $\mathfrak{b}$ of O_K, then there exist an ideal $\mathfrak{c}=(\gamma_1,\gamma_2,.....,\gamma_r)$ such that $\mathfrak{b}=\mathfrak{a}\mathfrak{c}$, and so if $\beta \in \mathfrak{b}$, then

$$\beta \ = \ \textstyle\sum_{i,t} \lambda_{it}\alpha_i\gamma_t \ = \ \sum_{i=1}^{m} \alpha_i(\sum_{t=1}^{r} \lambda_t\gamma_t); \text{ for } \lambda' s \in O_K;$$

and thus $\beta \in \mathfrak{a}$. Therefore $\mathfrak{a} \supset \mathfrak{b}$. □

Corollary 2.2.8. *[4]Let* O_K *be the ring of algebraic integers in some number field* K *over* Q, *and let* $\mathfrak{a}$ *be an ideal of* O_K, *then* $\mathfrak{a} \mid \mathfrak{i} \Rightarrow \mathfrak{a}=\mathfrak{i}$.

Proof. Suppose that $\mathfrak{a} \mid \mathfrak{i}$, then by Theorem (2.2.7) $\mathfrak{a} \supseteq \mathfrak{i}$, but $\mathfrak{a} \subseteq \mathfrak{i}$ for any ideal $\mathfrak{a}$ in O_K. Therefore, $\mathfrak{a} = \mathfrak{i}$. □

Definition 2.2.8. [4] An ideal $\mathfrak{p} \neq \mathfrak{i}$ in the ring of algebraic integers O_K is said to be a **prime ideal** if it has no other factors except $\mathfrak{p}$ itself and $\mathfrak{i}$.

Theorem 2.2.9. *[4] Every ideal $\mathfrak{a}(\neq 0)$ in the ring of algebraic integers O_K has a basis.*

Proof. See [4] page 221. □

Theorem 2.2.10. *[4] There exist only finitely many ideals containing a given integer $a \in Z$.*

Proof. Let $\mathfrak{a} = (\alpha_1, \alpha_2, \ldots, \alpha_m)$ be an ideal containing $a \in Z$. Then by Remark (2.2.3), $\mathfrak{a} = (\alpha_1, \alpha_2, \ldots, \alpha_m, a)$.
If $(\phi_1, \phi_2, \ldots, \phi_n)$ is an integral basis, then $\alpha_j = a_{j1}\phi_1 + a_{j2}\phi_2 + \ldots + a_{jn}\phi_n$; $(a_{jk} \in Z)$.
And by division algorithm, there exist $q_{jk} \in Z$, $r_{jk} \in Z$ such that $a_{jk} = aq_{jk} + r_{jk}$ with $0 \leq r_{jk} < a$.
Hence if we set $\sum_{k=1}^{n} r_{jk}\phi_k = \beta_j$, then by Remark (2.2.3) we obtain that $\mathfrak{a} = (\beta_1, \beta_2, \ldots, \beta_m, a)$, in which a is fixed and each β_j may take only finitely many values, namely those of the sums $\sum_{k=1}^{n} r_{jk}\phi_k$, with $0 \leq r_{jk} < a$.
Also by Remark (2.2.3), we need to keep only the independent elements as generators, and it follows that there can exist at most n such elements if the degree of the field is n. Hence $m \leq n$ and the total number of ideals $\mathfrak{a} = (\beta_1, \beta_2, \ldots, \beta_m, a)$ that may contain $a \in Z$ is indeed finite. □

Theorem 2.2.11. *[4] An ideal $\mathfrak{a}$ in the ring of algebraic integers O_K has only a finite number of factors.*

Proof. Let $\mathfrak{a}$ be an ideal, $\alpha \in \mathfrak{a}$, and let $\lambda \in O_K$ be the product of all conjugates of α, then we have $\lambda\alpha \in \mathfrak{a}$, and $N\alpha = \lambda\alpha$, that is $N\alpha \in \mathfrak{a}$; hence if $\mathfrak{b} \mid \mathfrak{a}$, then $N\alpha = a(\in Z)$ belongs also to $\mathfrak{b}$.
However, by Theorem (2.2.10), the number of ideals containing a given $(a \in Z)$ is finite. Therefore, the number of factors of $\mathfrak{a}$ is finite as desired. □

Theorem 2.2.12. *[5] For each ideal $\mathfrak{a}$ there is an ideal $\mathfrak{b}$ different from $\mathfrak{o}$ such that $\mathfrak{ab}$ is a principal ideal.*

Proof. See [5] page 80. □

Theorem 2.2.13. *[4] Let O_K be the ring of algebraic integers in some number field K over Q, and let $\mathfrak{a}$ and $\mathfrak{b}$ be ideals of O_K. For $\gamma \in O_K$, if (γ) is a principle ideal, and $(\gamma)\mathfrak{a} = (\gamma)\mathfrak{b}$ then $\mathfrak{a} = \mathfrak{b}$.*

Proof. Suppose that (γ) is a principle ideal, and $(\gamma)\mathfrak{a} = (\gamma)\mathfrak{b}$, then for every $\alpha \in \mathfrak{a}$, $\gamma\alpha = \gamma\beta$ for some $\beta \in \mathfrak{b}$, i.e. for any integer $\alpha \in \mathfrak{a}$, there corresponds an integer $\beta \in \mathfrak{b}$ such that $\alpha = \beta$. Thus $\mathfrak{a} \subseteq \mathfrak{b}$.
Similarly we get that $\mathfrak{b} \subseteq \mathfrak{a}$. Therefore $\mathfrak{a} = \mathfrak{b}$. □

Theorem 2.2.14. *[4] **(Cancelation law)** Let O_K be the ring of algebraic integers in some number field K over Q, and let $\mathfrak{a}$, $\mathfrak{b}$ and $\mathfrak{c}$ be ideals of O_K not equal to $\mathfrak{o}$, then $\mathfrak{ca} = \mathfrak{cb}$ implies that $\mathfrak{a} = \mathfrak{b}$.*

Proof. By Theorem (2.2.12), we can find an ideal $\mathfrak{d}$ such that $\mathfrak{dc} = (c)$. Hence $\mathfrak{ca} = \mathfrak{cb}$ implies that $\mathfrak{dca} = \mathfrak{dcb}$ that is $(c)\mathfrak{a} = (c)\mathfrak{b}$, therefore by Theorem (2.2.13), we get that $\mathfrak{a} = \mathfrak{b}$ as desired. □

Theorem 2.2.15. *[4] Let O_K be the ring of algebraic integers in some number field K over Q, and let $\mathfrak{a}$ and $\mathfrak{b}$ be ideals of O_K, if $\mathfrak{a} \supset \mathfrak{b}$, then $\mathfrak{a} \mid \mathfrak{b}$.*

Proof. Suppose that $\mathfrak{a} \supset \mathfrak{b}$, then $\mathfrak{ca} \supset \mathfrak{cb}$ for any ideal $\mathfrak{c}$. Choose $\mathfrak{c}$ so that $\mathfrak{ca} = (d)$ which exist by Theorem (2.2.12). Then each element of $\mathfrak{cb}$ is a multiple of d, and so $\mathfrak{cb} = (d)(\gamma_1, \gamma_2, \ldots, \gamma_r) = \mathfrak{ca}(\gamma_1, \gamma_2, \ldots, \gamma_r)$. Thus by Theorem (2.2.14), we get that $\mathfrak{b} = \mathfrak{a}(\gamma_1, \gamma_2, \ldots, \gamma_r)$, which implies that $\mathfrak{a} \mid \mathfrak{b}$ as desired. □

Remark 2.2.4. [4]

1. The Theorem (2.2.15) is the converse of Theorem (2.2.7).

2. In more general situation it is convenient to make a distinction between the concept of maximal ideal, prime ideal and irreducible ideal; but these objects coincide in the present setting. The three conceptually distinct properties which an ideal may have:

   (a) To have no factors, except i and itself(irreducibility);

   (b) To divide at least one factor if it divides a product of two integer of O_K(primarily); or

   (c) Not to be contained properly in any other ideal except i (maximality), go together for ideals in algebraic number fields. Either an ideal has all three, or none of them. This is the reason why we did not define formally irreducible, prime and maximal ideals, but only prime ideals, which we characterized by property (a).

Proof. See [4] page 225. □

Chapter 3

Factorization Of Ideals And The Class Number

There are infinitely many algebraic number fields in which the uniqueness of factorization of integers fails.
We will prove here two fundamental theorems of ideal theory in number fields: every non-zero proper ideal in the ring of integers of a number field admits unique factorization into a product of non-zero prime ideals. And the number if ideal classes in each field of algebraic numbers is finite.

3.1 Unique Factorization Of Ideals In Algebraic Number Fields

Definition 3.1.1. [17]

- A **partially ordered set** is a nonempty set A together with a relation R on $A \times A$ (called a **partial ordering of** A) which is reflexive, transitive and antisymmetric. If R is a partial ordering of A, then we usually write $a \leq b$ in place of $(a, b) \in R$.
- Let $(A, \leq)$ be a partially ordered set; an element $a \in A$ is **maximal** in A if for every $c \in A, a \leq c \Longrightarrow a = c$.

Lemma 3.1.1. *[6] A ring R is Noetherian if and only if every non-empty set of ideals has a maximal element with respect to inclusion.*

Proof. See [6] page 5. □

Definition 3.1.2. [17]

- A ring R is **left [resp. right] Noetherian** if R satisfies the ascending chain condition (ACC) on left [resp. right] ideals; that is for every chain $\mathfrak{a}_1 \subseteq \mathfrak{a}_2 \subseteq \mathfrak{a}_2 \subseteq \ldots$ of left [resp. right] ideals of R, there is an integer n such that $\mathfrak{a}_i = \mathfrak{a}_n$ for all $i \geq n$.
- R is said to be **Noetherian** if R is both left and right Noetherian.

Definition 3.1.3. [17]A **Dedekind domain** is an integral domain R in which every ideal ($\neq R$) is the product of a finite number of prime ideals.

Remark 3.1.1. Every P.I.D. is Dedekind domain, but the converse need not be true. "e.g $Z[\sqrt{10}]$ is a Dedekind domain which is not a P.I.D."

Proof. See [17] page 407. □

Definition 3.1.4. [11] Let A be an integral domain, there is a field $K \supset A$, called the **field of fractions of** A, with the property that every $c \in K$ can be written in the form $c = ab^{-1}$ with $a,\ b \in A$ and $b \neq 0$.

Example 3.1.1. *The field of fraction of the ring of integers is the field of rationales.*

Definition 3.1.5. [17] Let R be an integral domain with fractional field K, and let I be $R-$submodule of K. We say that I is a **fractional ideal** of R if $rI \subset R$ for some nonzero $r \in R$. We call r a **denominator** of I.

Note 3.1.2.

- *Every ordinary nonzero ideal I in an integral domain R is an $R-$submodule of R, and of course $rI \subset I \subset R$, and hence a fractional ideal of R.*

- *Conversely, every fractional ideal of R that is contained in R is an ordinary ideal of R*

- $\frac{1}{2}Z$ *is not contained in* Z,
  $\frac{1}{2}Z$ *is* $Z-$*submodule of* Q,
  $2(\frac{1}{2}Z) = Z \subset Z$ *or* $4(\frac{1}{2}Z) = 2Z \subset Z$.
  Therefore the collection $\frac{1}{2}Z$ *of rational numbers is a fractional ideal but not an ideal in* Z.

Theorem 3.1.3. *[17] If R is Noetherian with K its quotient field, and I is a fractional ideal of R, then I is a finitely generated R-submodule of K.*

Proof. See [16] page 157. □

Theorem 3.1.4. *[17] The following conditions on an integral domain R are equivalent:*

1. *R is a Dedekind domain;*

2. *every proper ideal in R is uniquely a product of a finite number of prime ideals;*

3. *the set of all fractional ideals of R is a group under multiplication;*

4. *R is Noetherian, integrally closed and every nonzero prime ideal is maximal.*

Proof. See [17] page 406. □

Note 3.1.5.

- *If $I_1, \ldots, I_n$ are ideals of a ring R, the product $\prod_{i=1}^{n} I_i$ is the set of all finite sums $\sum_{i}^{\infty} a_{1_i}\ a_{2_i} \ldots a_{k_i}$ where $a_{k_i} \in I_k,\ k = 1, 2, \ldots, n$.*

- *The product $\prod_{i=1}^{n} I_i$ is an ideal in R contained in each I_j.*

Theorem 3.1.6. *[17] If p is an ideal in a ring R, such that $p \neq R$ and for, all $a,\ b\ \in\ R$, $ab\ \in\ p\ \Rightarrow\ a\ \in\ p$, or $b\ \in\ p$, then p is a prime ideal.*
Conversely, if p is a prime ideal, and R is commutative, then p satisfies that for all $a,\ b\ \in\ R$, and $ab\ \in\ p$, then $a\ \in\ p$ or $b\ \in\ p$.

Proof. See [17]. □

Proposition 3.1.7. *[6] If $\mathfrak{p}, \mathfrak{p}_i$ are all prime ideals in O_K and*

$$\prod_{i=1}^{n} \mathfrak{p}_i \subseteq \mathfrak{p} \tag{3.1.1}$$

then there is a $k \leq n$ such that $\mathfrak{p}_k \subseteq \mathfrak{p}$.

Proof. Assume that for each i, $\mathfrak{p}_i \nsubseteq \mathfrak{p}$. Then for each i, there is a $p_i \in \mathfrak{p}_i \setminus \mathfrak{p}$, so

$$\textstyle\prod_{i=1}^{n} p_i\ \in \prod_{i=1}^{n} \mathfrak{p}_i \subseteq \mathfrak{p}$$

But $\mathfrak{p}$ is prime and O_K is a commutative ring, so there is a $k \leq n$ such that $p_k \in \mathfrak{p}$, contradicting the method by which the p_i were selected. Therefore, there is a $k \leq n$ such that $\mathfrak{p}_k \subseteq \mathfrak{p}$. □

Lemma 3.1.8. *[16] Let $\mathfrak{p}$ be a nonzero prime ideal of the Dedekind domain R, and let*

$$\mathfrak{p}^{-1} = \{k \in K | k\mathfrak{p} \subseteq R\}, \text{ where } K \text{ is the field of fractions of } R$$

Then $R\ \subset \mathfrak{p}^{-1}$.

Proof. See [16] page 157. □

Lemma 3.1.9. *[6] Let $\mathfrak{p}$ be a nonzero prime ideal of the Dedekind domain R, then $\mathfrak{p}^{-1}$ is a fractional ideal and $\mathfrak{p}\mathfrak{p}^{-1} = R$.*

Proof. From definition of $\mathfrak{p}^{-1}$, we get that $\mathfrak{p}^{-1}$ is an R-submodule of K.
Now let r be a nonzero element of $\mathfrak{p}$, and $x \in \mathfrak{p}^{-1}$, then $rx \in R$, and so

$$r\mathfrak{p}^{-1}\ \subseteq\ R\ \text{.....}(*)$$

Thus $\mathfrak{p}^{-1}$ is a fractional ideal.

Now by $(*)$, $\mathfrak{p}\mathfrak{p}^{-1} \subseteq R$, so $\mathfrak{p}\mathfrak{p}^{-1}$ is an integral ideal of R.

By Lemma (3.1.8) $R \subset \mathfrak{p}^{-1}$, so $\mathfrak{p}R \subset \mathfrak{p}\mathfrak{p}^{-1}$, but also $\mathfrak{p}R = \mathfrak{p}$, and $\mathfrak{p}\mathfrak{p}^{-1} \subseteq R$, so we have $\mathfrak{p} \subseteq \mathfrak{p}\mathfrak{p}^{-1} \subseteq R$. But $\mathfrak{p}$ is prime ideal and R is a Dedekind domain, so by Theorem (3.1.4) $\mathfrak{p}$ is a maximal ideal which implies that $\mathfrak{p}\mathfrak{p}^{-1} = \mathfrak{p}$ or $\mathfrak{p}\mathfrak{p}^{-1} = R$. If $\mathfrak{p}\mathfrak{p}^{-1} = R$, we have done.

So assume that $\mathfrak{p}\mathfrak{p}^{-1} = \mathfrak{p}$, and let $x \in \mathfrak{p}^{-1}$, then $x\mathfrak{p} \subseteq \mathfrak{p}\mathfrak{p}^{-1} = \mathfrak{p}$. Now by induction, we get that $x^n\mathfrak{p} \subseteq \mathfrak{p}$ for all $n = 1, 2, \ldots$

So for any nonzero element r of $\mathfrak{p}$, we have $rx^n \in x^n\mathfrak{p} \subseteq \mathfrak{p} \subseteq R$, so $R[x]$ is a fractional ideal. But R is a Dedekind domain, so by Theorem (3.1.4) it is Noetherian which implies by Theorem (3.1.3) that $R[x]$ is a finitely generated R-submodule of K, so by Lemma (2.1.1), x is integral over R, and since R is a Dedekind domain then by Theorem (3.1.4), R is integrally closed, which implies that $x \in R$. Therefore $\mathfrak{p}^{-1} \subseteq R$ which contradicts Lemma (3.1.8). Therefore $\mathfrak{p}\mathfrak{p}^{-1} = R$. □

Theorem 3.1.10. *[1] In a commutative ring with unity, any proper ideal is contained in a maximal ideal.*

Proof. See [1] page 382. □

Lemma 3.1.11. *[1] Let R be a Noetherian commutative ring, and let $\mathfrak{a}$ and $\mathfrak{p}$ be ideals in R with $\mathfrak{p}$ prime. If $\mathfrak{a}\mathfrak{p} = \mathfrak{a}$, then $\mathfrak{a} = 0$.*

Proof. See [1] page 433. □

We come now to the fundamental theorem of ideal theory in number fields.

Proposition 3.1.12. *[6] Every nonzero, proper ideal of a Dedekind domain can be uniquely factored into nonzero prime ideals, and this factorization is unique except for order.*

Proof. Let I be the set of nonzero proper ideals of the Dedekind domain D that do not factor into prime ideals.

Assume I is non-empty, then by Lemma (3.1.1), there is a maximal element $\mathfrak{m} \in I$, which is contained by Theorem (3.1.10) in a maximal ideal $\mathfrak{p}$ in D, so $\mathfrak{m} \subseteq \mathfrak{p}, \implies \mathfrak{m}\mathfrak{p}^{-1} \subseteq \mathfrak{p}\mathfrak{p}^{-1}$, but $\mathfrak{m} \subseteq \mathfrak{m}\mathfrak{p}^{-1}$.

So, and by Lemma (3.1.8), and (3.1.9) $\mathfrak{m} \subseteq \mathfrak{m}\mathfrak{p}^{-1} \subseteq \mathfrak{p}\mathfrak{p}^{-1} = D$, so $\mathfrak{m}\mathfrak{p}^{-1}$ is an ideal of D. By Lemma (3.1.11), $\mathfrak{m} \subsetneq \mathfrak{m}\mathfrak{p}^{-1}$, but $\mathfrak{p}$ is maximal, hence prime by Proposition (2.2.4), but $\mathfrak{m}$ cannot be prime, so $\mathfrak{m} \subsetneq \mathfrak{p}$, so $\mathfrak{m}\mathfrak{p}^{-1} \subsetneq \mathfrak{p}\mathfrak{p}^{-1}$, so $\mathfrak{m}\mathfrak{p}^{-1}$ is a proper ideal containing $\mathfrak{m}$. Since $\mathfrak{m}$ is a maximal element of I, $\mathfrak{m}\mathfrak{p}^{-1}$ has a prime factorization. But $\mathfrak{m} = \mathfrak{m}\mathfrak{p}^{-1}\mathfrak{p}$, so $\mathfrak{m}$ also has prime factorization, so I is necessarily empty.

Therefore, all ideals in a Dedekind domain can be factored into primes.

Let the following be two prime factorizations of the same ideal:

$$\mathfrak{a} = \prod_{i=1}^{m} \mathfrak{p}_i = \prod_{j=1}^{n} \mathfrak{p'}_j \tag{3.1.2}$$

Since $\mathfrak{p}_m$ is prime, then by proposition (3.1.7) there must be a $j' \geq 1$ such that $\mathfrak{p}_m \supseteq \mathfrak{p'}_{j'}$, but prime ideals are maximal in a Dedekind domain, so $\mathfrak{p}_m = \mathfrak{p'}_{j'}$. Assume without lost of generality that $j' = n$. Since $\mathfrak{p}\mathfrak{p}^{-1} = D$, by multiplying by $\mathfrak{p}_m^{-1}$, we find that

$$\prod_{i=1}^{m-1} \mathfrak{p}_i = \prod_{j=1}^{n-1} \mathfrak{p'}_j \tag{3.1.3}$$

Using this recursive process, and remembering that the ideals are prime, we find that $m = n$ and pair up all $m = n$ pairs of equal prime ideals. Thus, the factorization of ideals in a Dedekind domain into prime ideals is unique. □

Theorem 3.1.13. *[21] The ring of algebraic integers in a number field is a Dedekind domain.*

Proof. See [21] page 22. □

Remark 3.1.2. It is not necessary that O_K is a U.F.D., for example in $Z[\sqrt{-5}]$ which is $O_{Q(\sqrt{-5})} : 6 = 2.3 = (1 + \sqrt{-5})(1 - \sqrt{-5})$.

Proposition 3.1.14. *[4]The ideals of a ring of algebraic integers O_K of some number field K over Q, factor into prime ideals and this factorization is unique except for order.*

Proof. It is a consequence of Theorem (3.1.13) and proposition (3.1.12). □

Example 3.1.2. *[18] Consider the ideal* $< 18 >$ *generated by* 18 *in the ring of algebraic integers* $Z[\sqrt{-17}]$ *in the number field* $Q[\sqrt{-17}]$.

Let $\mathfrak{p}_1 = < 2, 1 + \sqrt{-17},$

$\mathfrak{p}_2 = < 3, 1 + \sqrt{-17},$

$\mathfrak{p}_3, 1 - \sqrt{-17}.$

It shown in page 131 in ([18]) that.

$< 18 > = (\mathfrak{p}_1^2)(\mathfrak{p}_2\mathfrak{p}_3)^2 = < 2 >< 3 >^2$

$= (\mathfrak{p}_1\mathfrak{p}_2^2)(\mathfrak{p}_1\mathfrak{p}_3^2) = < 1 + \sqrt{-17} >< 1 - \sqrt{-17} >$

which is unique factorization of $< 18 >$ *except for order since* $(\mathfrak{p}_1^2)(\mathfrak{p}_2\mathfrak{p}_3)^2 = (\mathfrak{p}_1\mathfrak{p}_2^2)(\mathfrak{p}_1\mathfrak{p}_3^2) = \mathfrak{p}_1^2\mathfrak{p}_2^2\mathfrak{p}_3^2$.

3.2 Ideal Classes And The Class Number

Definition 3.2.1. [4]Let O_K be the ring of algebraic integers in some number field K over Q, then any two integers α and β in O_K are said to be **congruent modulo an ideal** $\mathfrak{a}$ in symbols : $\alpha \equiv \beta(mod\ \mathfrak{a})$, if $\mathfrak{a} \mid \alpha - \beta$ or equivalently, if $\mathfrak{a} \mid (\alpha - \beta)$.

Theorem 3.2.1. *[4]If* O_K *is the ring of algebraic integers in some number field* K *over* Q*, then the congruence modulo an ideal* $\mathfrak{a}$ *in* O_K *is an equivalence relation.*

Proof. See [4] page 226. □

Theorem 3.2.2. *[4] Let* O_K *be the ring of algebraic integers in some number field* K *over* Q*, and let* α *and* β *be two integers in* O_K*, and* $\mathfrak{a}$, $\mathfrak{c}$ *be two ideals of* O_K*. If* $\alpha \equiv \beta(mod\ \mathfrak{a})$ *and* $\mathfrak{c} \mid \mathfrak{a}$*, then* $\alpha \equiv \beta(mod\ \mathfrak{c})$.

Proof. See [4] page 226. □

Corollary 3.2.3. *[4] Let* O_K *be the ring of algebraic integers in some number field* K *over* Q*, and let* $\alpha, \beta, \gamma, \delta, \lambda \in O_K$ *and let* $\mathfrak{a}$ *be an ideal in* O_K.

If $\alpha \equiv \beta(mod\ \mathfrak{a})$, $\gamma \equiv \delta(mod\ \mathfrak{a})$ *then* $\alpha \pm \gamma \equiv \beta \pm \delta(mod\ \mathfrak{a})$, $\alpha\gamma \equiv \beta\delta(mod\ \mathfrak{a})$ *and* $\lambda\alpha \equiv \lambda\beta(mod\ \mathfrak{a})$.

Proof. See [4] page 226. □

Theorem 3.2.4. *[4]The set of residue classes modulo an ideal is finite.*

Proof. Let $\mathfrak{a}$ be an ideal in K, then by Theorem (2.2.12), we can find an ideal $\mathfrak{b}$ such that $\mathfrak{ab} = (c),\ c > 0$. Now let $\phi_1,\ \phi_2,\ \cdots,\ \phi_n$ be an integral bases, then every $\alpha \in O_K$ has a unique representation $\alpha = a_1\phi_1 + a_2\phi_2 + \cdots + a_n\phi_n,\ (a_j \in Z)$. If we first consider the number of residue classes of α modulo c, we get that each coefficient a_j may belong to only at most c residue classes "when c is prime"; consequently, α can belong to at most c^n residue classes $(mod\ c)$. This is also the number of residue classes $(mod(c))$. By Theorem (3.2.2), it follows that there are at most c^n residue classes mod $\mathfrak{a}$. □

Definition 3.2.2. [4] The number of residue classes of integers of O_K modulo an ideal $\mathfrak{a}$ is called the **norm** of $\mathfrak{a}$, in symbols; $N(\mathfrak{a})$ or $N\mathfrak{a}$.

Note 3.2.5. *In the case of principal ideals we write $N((\alpha))$ to avoid confusion with $N\alpha = N(\alpha)$*

Theorem 3.2.6. *[4] Let O_K be the ring of algebraic integers in some number field K over Q, if $\alpha \in O_K$, then $N((\alpha)) =\mid N(\alpha) \mid$.*

Proof. See [4] page 226. □

Remark 3.2.1. If $\mathfrak{a}$ is an ideal of the ring of algebraic integers O_K, then $N\mathfrak{a} = 1$ implies that $\mathfrak{a} = i$.

Proof. Now, $N\mathfrak{a} = 1$ means that all integer are congruent to each other, hence to $0(\in \mathfrak{a})$ so that all belong to $\mathfrak{a}$. □

Theorem 3.2.7. *[4] Let O_K be the ring of algebraic integers in some number field K over Q, and let $\mathfrak{a}$ be an ideal and $\mathfrak{p}$ be a prime ideal of O_K, then $N\mathfrak{a}.N\mathfrak{p} = N(\mathfrak{ap})$.*

Proof. See [4] page 227. □

Theorem 3.2.8. *[4] Let O_K be the ring of algebraic integers in some number field K over Q, and let $\mathfrak{a}, \mathfrak{b}$, and $\mathfrak{c}$ be ideals in O_K; then $\mathfrak{a}.\mathfrak{b} = \mathfrak{c} \Rightarrow N\mathfrak{a}.N\mathfrak{b} = N\mathfrak{c}$.*

Proof. The proof is by induction on the number of factors of $\mathfrak{b}$. If $\mathfrak{b} = \mathfrak{p}$ then by Theorem (3.2.7), $N\mathfrak{a}.N\mathfrak{p} = N(\mathfrak{a}\mathfrak{p})$

Suppose that our claim hold for $\mathfrak{b}$ containing $k-1$ prime ideals factors, then it also hold for $\mathfrak{b} = \mathfrak{p}_1 \cdots \mathfrak{p}_{k-1}\mathfrak{p}$ as follows;

Let $\mathfrak{b} = \mathfrak{b}_1\mathfrak{p}$, then by Theorem (3.2.7), $N(\mathfrak{a}.\mathfrak{b}) = N(\mathfrak{a}.\mathfrak{b}_1.\mathfrak{p}) = N(\mathfrak{a}\mathfrak{b}_1).N(\mathfrak{p})$.

Also by induction assumption, $N(\mathfrak{a}\mathfrak{b}_1) = N\mathfrak{a}.N\mathfrak{b}_1$, hence by Theorem (3.2.7),

$N(\mathfrak{a}.\mathfrak{b}) = N\mathfrak{a}.N\mathfrak{b}_1.N\mathfrak{p} = N\mathfrak{a}.N(\mathfrak{b}_1.\mathfrak{p})$.

Finally, by replacing $\mathfrak{b}_1.\mathfrak{p}$ by $\mathfrak{b}$, we get the result. □

Theorem 3.2.9. *[4] Let O_K be the ring of algebraic integers in some number field K over Q, and let $\mathfrak{a}$ be an ideal of O_K, then $\mathfrak{a} \mid N\mathfrak{a}$ (i.e $\mathfrak{a} \mid (N(\mathfrak{a}))$.*

Proof. Let $\mathfrak{a}$ be an ideal of K, select an element α_j from each residue class from the $N\mathfrak{a}$ residue classes mod $\mathfrak{a}$ to get a maximal set of integers $\{\alpha_1, \alpha_2, \ldots, \alpha_{N\mathfrak{a}}\}$ whose elements are incongruent *mod* $\mathfrak{a}$.

Then also the set $\{\alpha_1 + 1, \alpha_2 + 1, \ldots, \alpha_{N\mathfrak{a}} + 1\}$ is a maximal set of integers whose elements are incongruent *mod* $\mathfrak{a}$; consequently $\alpha_1 + \alpha_2 + \ldots + \alpha_{N\mathfrak{a}} \equiv (\alpha_1 + 1) + (\alpha_2 + 1) + \ldots + (\alpha_{N\mathfrak{a}} + 1)$ (*mod* $\mathfrak{a}$), so that $0 \equiv 1 + 1 + \ldots + 1 = N\mathfrak{a}$ (*mod* $\mathfrak{a}$), as desired. □

Theorem 3.2.10. *[4] Let O_K be the ring of algebraic integers in some number field K over Q, then for every $m \in Z^+$, there exist only finitely many ideals $\mathfrak{a}$ such that $N\mathfrak{a} = m$.*

Proof. Let $m \in Z^+$, then for any ideal $\mathfrak{a}$ with $N\mathfrak{a} = m$, we have by Theorem (3.2.9) that $\mathfrak{a} \mid m$; and by Theorem (2.2.10), there exist only finitely many such ideals $\mathfrak{a}$ for which $\mathfrak{a} \mid m$ for any given $m \in Z^+$. Thus we have done. □

Definition 3.2.3. [4] Let O_K be the ring of algebraic integers in some number field K over Q, then two ideals $\mathfrak{a}$ and $\mathfrak{b}$ of O_K are said to be **equivalent** in symbols $\mathfrak{a} \sim \mathfrak{b}$, if there exist algebraic integers $\alpha, \beta \in O_K$ such that $(\alpha)\mathfrak{a} = (\beta)\mathfrak{b}$.

Example 3.2.1. *In $Q(\sqrt{-5})$ $(2, (1+\sqrt{-5})) \sim ((1-\sqrt{-5}), 3)$, because $(1-\sqrt{-5}) * (2, (1+\sqrt{-5})) = (2(1-\sqrt{-5}), 6) = (2) * ((1-\sqrt{-5}), 3)$.*

Theorem 3.2.11. *[4]The equivalence of ideals is an equivalence relation.*

Proof. 1. $\mathfrak{a} \sim \mathfrak{a}$ because $(1)\mathfrak{a} = (1)\mathfrak{a}$.

2. $\mathfrak{a} \sim \mathfrak{b}$ means that $(\alpha)\mathfrak{a} = (\beta)\mathfrak{b}$ for some $\alpha, \beta \in O_K$, so that $(\beta)\mathfrak{b} = (\alpha)\mathfrak{a}$, and so $\mathfrak{b} \sim \mathfrak{a}$.

3. $\mathfrak{a} \sim \mathfrak{b}$, and $\mathfrak{b} \sim \mathfrak{c}$ if and only if $(\alpha)\mathfrak{a} = (\beta_1)\mathfrak{b}$, $(\beta_2)\mathfrak{b} = (\gamma)\mathfrak{c}$ if and only if $(\beta_2)(\alpha)\mathfrak{a} = (\beta_2)(\beta_1)\mathfrak{b} = (\beta_1)(\gamma)\mathfrak{c}$ if and only if $(\beta_2\alpha)\mathfrak{a} = (\beta_1\gamma)\mathfrak{c}$, with α, β_1, β_2, and $\gamma \in O_K$, and so $\mathfrak{a} \sim \mathfrak{c}$.

□

Theorem 3.2.12. *[22]*

Let K be a number field, and let $Cl(K)$ be the set of ideal classes of K, then $Cl(K)$ form an abelian group.

Proof. Let K be a number field, and let $Cl(K)$ be the set of ideal classes of K, with multiplication $\cdot$ defined by

$$[\mathfrak{a}] \cdot [\mathfrak{b}] = [\mathfrak{ab}]$$

where $\mathfrak{a}, \mathfrak{b}$ are ideals of O_K.

We shall check the group properties:

1. Associativity: $[\mathfrak{a}] \cdot ([\mathfrak{b}] \cdot [\mathfrak{c}]) = [\mathfrak{a}] \cdot [\mathfrak{bc}] = [\mathfrak{a}(\mathfrak{bc})] = [\mathfrak{abc}] = [(\mathfrak{ab})\mathfrak{c}] = [\mathfrak{ab}] \cdot [\mathfrak{c}] = ([\mathfrak{a}] \cdot [\mathfrak{b}]) \cdot [\mathfrak{c}]$

2. Identity element: $[\mathcal{O}_K] \cdot [\mathfrak{b}] = [\mathfrak{b}] = [\mathfrak{b}] \cdot [O_K]$.

3. Inverses: Consider $[\mathfrak{b}]$. Let b be an integer in $\mathfrak{b}$. Then $\mathfrak{b} \supseteq (b)$, so there exists $\mathfrak{c}$ such that $\mathfrak{bc} = (b)$.
   Then the ideal class $[\mathfrak{b}] \cdot [\mathfrak{c}] = [(b)] = [O_K]$.

Then $Cl(K)$ is a group under the operation $\cdot$.

It is abelian since $[\mathfrak{a}][\mathfrak{b}] = [\mathfrak{ab}] = [\mathfrak{ba}] = [\mathfrak{b}][\mathfrak{a}]$.

□

Definition 3.2.4. [4] The classes induced by the equivalence relation $\sim$ among ideals of O_K are called **ideal classes**, the set of ideal classes is called **class group** of K, and is denoted by $Cl(K)$.

Remark 3.2.2. The principle ideals are equivalent to each other (and to $\mathfrak{i} = (1)$); hence, they form one of the classes, sometimes called the **principle class**.

We come now to one of the fundamental results of the theory of ideals, and to the main theorem in this section.
But we will give three lemmas before our theorem.

Lemma 3.2.13. *[4] Let O_K be the ring of algebraic integers in some number field K over Q, and let $\mathfrak{a}, \mathfrak{b}, \mathfrak{c}$, and $\mathfrak{d}$ be ideals in O_K; then $\mathfrak{a} \sim \mathfrak{b}, \mathfrak{c} \sim \mathfrak{d}$ implies that $\mathfrak{ac} \sim \mathfrak{bd}$.*

Proof. By definition (3.2.3), $\exists\ \alpha,\ \beta,\ \gamma$, and $\delta \in O_K$ such that $(\alpha)\mathfrak{a} = (\beta)\mathfrak{b}$, and $(\gamma)\mathfrak{c} = (\delta)\mathfrak{d}$, so $(\alpha\gamma)\mathfrak{ac} = (\beta\delta)\mathfrak{bd}$, so that $\mathfrak{ac} \sim \mathfrak{bd}$. □

Lemma 3.2.14. *[4] For every field K of algebraic numbers, there exists a positive integer $m = m(K)$ with the property that in every ideal $\mathfrak{a}$ of O_K, there exists an integer $\alpha \in \mathfrak{a}$ such that $\mid N\alpha \mid \ \leq\ m.N\mathfrak{a}$.*

Proof. Let $\phi_1\ ,\ \phi_2\ ,\ \cdots\ ,\ \phi_n$ be an integral bases for K, then by remark (2.1.2), each ϕ_j is uniquely represented by a polynomial $\phi_j = g_j(\theta)$ in the generator θ of K.
Now, if $\theta^{(1)}\ ,\ \theta^{(2)}\ ,\ \cdots\ ,\ \theta^{(n)}$ are the conjugates of θ, then the conjugates of ϕ_j are $\phi_j^{(k)} = g_j(\theta^{(k)}),\ 1 \leq j, k \leq n$. Let

$$M = \prod_{k=1}^{n} \{ \sum_{j=1}^{n} \mid g_j(\theta^{(k)}) \mid \}. \tag{3.2.1}$$

then M has the required property, and we may take $m = [M] + 1$.
Indead, for every ideal $\mathfrak{a}$, we can determine an integer r such that $r^n \leq N\mathfrak{a} < (r+1)^n$.
Now consider the set of integers of O_K represented by $a_1\phi_1 + a_2\phi_2 + \cdots + a_n\phi_n$ with $0 \leq a_j \leq r$, so each a_j may take $r+1$ distinct values because each $a_j \in Z$; hence we obtain $(r+1)^n$ different integers of O_K.

But there exist only $N\mathfrak{a}$ residue classes mod $\mathfrak{a}$, and we have $N\mathfrak{a} < (r+1)^n$, so those integers can not all be incongruent mod $\mathfrak{a}$.

Hence among these $(r+1)^n$ integers, there are at least two integers $\alpha = a_1\phi_1 + a_2\phi_2 + \cdots + a_n\phi_n$, and $\beta = b_1\phi_1 + b_2\phi_2 + \cdots + b_n\phi_n$, such that $\alpha \neq \beta$, but $\alpha \equiv \beta \ (mod\ \mathfrak{a})$, where $o \leq a_j \leq r$, $o \leq b_j \leq r$.

So $0 \neq \gamma = \alpha - \beta \equiv 0 \ (mod\ \mathfrak{a})$, that is $\gamma \in \mathfrak{a}$.Thus

$$| N\gamma | = | \prod_{k=1}^{n} \gamma^{(k)} |; \tag{3.2.2}$$

However;

$$| \gamma^{(k)} | = | \sum_{j=1}^{n} (a_j - b_j)\phi_j^{(k)} | \leq \sum_{j=1}^{n} r \ | \phi_j^{(k)} | = r. \sum_{j=1}^{n} | \phi_j^{(k)} |; \tag{3.2.3}$$

So that

$$| N\gamma | = \prod_{k=1}^{n} | \gamma^{(k)} | \leq r^n \prod_{k=1}^{n} \{ \sum_{j=1}^{n} | \phi_j^{(k)} | \} = r^n M \leq N\mathfrak{a}.M; \tag{3.2.4}$$

and $\gamma \in \mathfrak{a}$ has $| N\gamma | \leq M.N\mathfrak{a}$ as claimed. □

Lemma 3.2.15. *[4] Let $m = m(k)$ be defined as in lemma (3.2.14); then in each class of ideals there exists an ideal $\mathfrak{a}$ such that $N\mathfrak{a} \leq m$.*

Proof. Let $\mathfrak{U}$ be any class of ideals in K; and let $\mathfrak{b}$ be an arbitrary ideal in $\mathfrak{U}$. By Theorem (2.2.12), there exists an ideal $\mathfrak{c}$ in K such that $\mathfrak{cb}$ is principal.

By Lemma (3.2.14), we may select in $\mathfrak{c}$ an integer γ such that $| N\gamma | \leq m \ . \ N\mathfrak{c}$.

Since $\gamma \in \mathfrak{c}$, we have $(\gamma) \subset \mathfrak{c}$, thus, by Theorem (2.2.15), we get that $c \mid (\gamma)$; hence there exists an ideal $\mathfrak{a}$ in K such that $\mathfrak{ca} = (\gamma)$.

Now, since both $\mathfrak{ca}$, and $\mathfrak{cb}$ are principle, then $\mathfrak{ca} \sim \mathfrak{cb}$ which implies that $\mathfrak{a} \sim \mathfrak{b}$, hence $\mathfrak{a} \in \mathfrak{U}$.

And by Theorem (3.2.8), Theorem (3.2.6), and Lemma (3.2.14) it follows that

$$\mathfrak{ca} = (\gamma) \ \textit{implies that} \ N\mathfrak{c}.N\mathfrak{a} = N((\gamma)) = | N\gamma | \leq m.N\mathfrak{c}, \tag{3.2.5}$$

so that $N\mathfrak{a} \leq m$ and thus our lemma has been proven. □

Theorem 3.2.16. *[4] In every field K of algebraic numbers, the number of ideal classes is finite.*

Proof. By Theorem (3.2.10), there exist only finitely many ideals of a given norm, and so only finitely many ideals whose norm does not exceed any given bound.
Suppose that there are t ideals of norm $\leq m$, but by Lemma (3.2.15), there exist at least one ideal of norm $\leq m$ in each class, so there exist at most t classes of ideals. □

Definition 3.2.5. [4] The (finite) number of classes of ideals in an algebraic number field K is called the **class number** of K and is denoted by $h = h(K)$.

Theorem 3.2.17. *[4] If h is the class number of an algebraic number field K, then for every ideal $\mathfrak{a}$ of K, $\mathfrak{a}^h$ is a principal ideal.*

Proof. Select an ideal $\mathfrak{a}_j$ from each class from the h ideal classes to get the set $\{\mathfrak{a}_1, \mathfrak{a}_2, \ldots, \mathfrak{a}_h\}$ of inequivalent ideals in K.
If $\mathfrak{a}$ is any ideal of K, then by Theorem (2.2.12) and Lemma (3.2.13), we get that $\mathfrak{a}\mathfrak{a}_j \sim \mathfrak{a}\mathfrak{a}_k$ implies that $\mathfrak{b}\mathfrak{a}\mathfrak{a}_j \sim \mathfrak{b}\mathfrak{a}\mathfrak{a}_k$ if and only if $(\mathfrak{c})\mathfrak{a}_j \sim (\mathfrak{c})\mathfrak{a}_k$ if and only if $\mathfrak{a}_j \sim \mathfrak{a}_k$.
Thus, $\{\mathfrak{a}\mathfrak{a}_1, \mathfrak{a}\mathfrak{a}_2, \ldots, \mathfrak{a}\mathfrak{a}_h\}$ is also a set of h inequivalent ideals.
Consequently, in the set $\{\mathfrak{a}\mathfrak{a}_j : 1 \leq j \leq h\}$ there is again exactly one ideal from each of the h classes.
But we get by Lemma (3.2.13) that $\mathfrak{a}_1\mathfrak{a}_2 \ldots \mathfrak{a}_h \sim \mathfrak{a}\mathfrak{a}_1.\mathfrak{a}\mathfrak{a}_2 \ldots \mathfrak{a}\mathfrak{a}_h = \mathfrak{a}^h\mathfrak{a}_1 \ldots \mathfrak{a}_h$. Again, using Theorem (2.2.12), and Lemma (3.2.13) we get that $(1) \sim \mathfrak{a}^h$, as desired. □

Theorem 3.2.18. *[4] If h is the class number of an algebraic number field K, then for every ideal $\mathfrak{a}$ of K, if p is a prime, and $p \nmid h$, then $\mathfrak{a}^p \sim \mathfrak{b}^p$ implies that $\mathfrak{a} \sim \mathfrak{b}$.*

Proof. Now, since $g.c.d(h, p) = 1$, so there exist positive integers m, k such that $kp - mh = 1$, so $pk = mh + 1$.
But by Lemma (3.2.13), $\mathfrak{a}^p \sim \mathfrak{b}^p$ implies that $\mathfrak{a}^{kp} \sim \mathfrak{b}^{pk}$, and by Theorem (3.2.17), $\mathfrak{a}^h = (1)$, so $\mathfrak{a}^{pk} = \mathfrak{a}^{mh+1} = \mathfrak{a}^{mh}.\mathfrak{a} \sim \mathfrak{a}$; Similarly, $\mathfrak{b}^{kp} \sim \mathfrak{b}$, and thus we have done. □

Corollary 3.2.19. *[4] If $p \nmid h$, and $\mathfrak{a}^p$ is principal in K, then so is $\mathfrak{a}$.*

Proof. Take $\mathfrak{b} = 1$ in Theorem (3.2.18). □

Chapter 4

Some congruences on prime factors of class number of finite algebraic extensions K/Q

This chapter is based on analytic study of a paper for Dr. Roland Queme[14], and some related theorems and subjects from related papers such as Masely[19], and Bordelles[13]. We give a contribution to the description of congruences on the odd prime factors of the class number of the number field.

We also give a connection with Geometry of Numbers point of view. With an explicit geometric upper bound H_F of the class number $h(F)$ for any field F which is given in this chapter.

4.1 Ramification, And The p-Rank

Theorem 4.1.1. *[11] Let A be a Dedekind domain with field of fractions K, and let B be the integral closure of A in a finite separable extension L of K. Then B is a Dedekind domain.*

Proof. See [11] page 47. □

Definition 4.1.1. [11] Consider a Dedekind domain A with fraction field K, L is a finite separable extension of K of degree n and B is the integral closure of A in L and let $\mathfrak{p}$ be a nonzero prime ideal of A, then the **lifting(also called the extension**) of $\mathfrak{p}$ to B is the ideal $\mathfrak{p}B$.

Remark 4.1.1. Although $\mathfrak{p}B$ need not be a prime ideal of B, we can use the fact that B is a Dedekind domain and the unique factorization theorem to get that $\mathfrak{p}B = \prod_{i=1}^{g} \mathfrak{B}_i^{e_i}$, where $\mathfrak{B}_i's$ are distinct prime ideals of B and e_i are positive integers.

Definition 4.1.2. [12] Consider a Dedekind domain A, with fraction field K, and let L be a finite separable extension of K of degree n, and let $\mathfrak{p}$ be a nonzero prime ideal of A, and B is the integral closure of A in L.

1. If we lift $\mathfrak{p}$ to B and factor $\mathfrak{p}B$ as $\prod_{i=1}^{g} \mathfrak{B}_i^{e_i}$, the positive integer e_i is called the **ramification index** of $\mathfrak{B}_i$ over $\mathfrak{p}$ (or over A).

2. The prime ideals $\mathfrak{B}_j's$ are said to lie above $\mathfrak{p}$.

3. We say that $\mathfrak{p}$ **ramifies in** B (or in L), if $e_i > 1$ for at least one i.

4. If $e_i = 1$ for each $\mathfrak{B}_i$, then we say that $\mathfrak{p}$ **is unramified** in L.

5. The **extension** L/K itself is called **unramified** if all prime ideals $\mathfrak{p}$ of K are unramified in L.

Example 4.1.1. *[23] In $Z[i]$;*

- *The prime 2 of Z ramifies in $Z[i]$ because $(2) = (1+i)^2$, and the ramification index is $e = 2$.*

- *Any prime $p \equiv 1(mod\ 4)$ splits into two distinct prime ideals in $Z[i]$; for example $(13) = (2+3i)(2-3i)$.*

- *Any prime $p \equiv 3(mod\ 4)$ does not split in $Z[i]$; for example (7) remains prime in $Z[i]$.*

Definition 4.1.3. [14] A **cyclic extension** is a Galois extension whose Galois group is cyclic.

Theorem 4.1.2. *[17] Every finite dimensional extension of a finite field is a cyclic extension.*

Proof. See Hangerford[17], Theorem 5.10 □

Definition 4.1.4. [14] Let K/Q be a finite algebraic extension, let L/K be a finite Galois extension, we say that L/K is a **cyclic tower extension** if there is a tower of fields $K = L_0 \subset L_1 \subset ..... \subset L_n \subset L_{n+1} = L$, where L_{j+1}/L_j is a cyclic extension for $j = 0, 1, \ldots, n$.

Definition 4.1.5. [14] We say that a finite Galois extension L/K is **Galois solvable** if the Galois group $Gal(L/K)$ is solvable.

Definition 4.1.6. [14] We say that a finite extension L/K is **solvable extension** if the smallest Galois extension M of K containing L is Galois solvable.

Theorem 4.1.3. *[20]* ***Fundamental Theorem of Finite Abelian groups***
Every finite abelian group is a direct product of cyclic groups of prime order.
Moreover, the number of terms in the product and the orders of the cyclic groups are uniquely determined by the group.

Proof. See [20] page 177. □

Definition 4.1.7. [14] Let the class group of a field F, $Cl(F)$ be an abelian group, and let p be a prime dividing $h(L) = |Cl(F)|$, i.e. $h(L) = p^r m$ for some positive integer r, and $p \nmid m$. The $p-$subgroup C_p of C is an abelian group, direct sum of r_p cyclic groups whose order are power of p. This number r_p is the $p-$**rank** of the $p-$subgroup of C.

Example 4.1.2. *Let* $C = Z/20 \oplus Z/8$*, then by Theorem (4.1.3) we get that* $C \approx Z_5 \oplus Z_4 \oplus Z_8$*. Now any* $2-$*subgroup of* C *is isomorphic to a subgroup of* $Z_5 \oplus Z_{2^2} \oplus Z_{2^3}$*, so* $r_2 = 2,\ r_5 = 1$.

Note 4.1.4. *The notation $p^r \| k$, means that r is the greatest power of p letting $p^r | k$, i.e. $p^{r+1} \nmid k$.*

Remark 4.1.2. Let the class group of a field F, $Cl(F)$ be an abelian group, and let p be a prime dividing $h(L) = |Cl(F)|$, i.e. $h(L) = p^r m$ for some positive integer r, and $p \nmid m$. Now if r_p is the $p-$**rank** of the $p-$subgroup of $Cl(F)$, and $p^{e_p} \| h(L)$, for some integer e_p, then $r_p \leq e_p$.

Proof. Since $h(L) = p^r.m$ then $p^{r_p} | h(L)$, otherwise $r_p$the number of factors in the group decomposition is more than r, which is impossible by the fundamental theorem of finite abelain groups, so $r_p \leq e_p$. □

4.2 On congruences on prime factors of class number of Galois extensions K/Q

Theorem 4.2.1. *[19]* ***(Pushing up)*** *Let E/F be an extension of number fields. Then $|H(F) : H(F) \cap E|$ divides $h(E)$ and $h(F)$ divides $|E : F|h(E)$. In particular, if for any unramified abelian extension H of F we have $E \cap H = F$, then $h(F)$ divides $h(E)$.*

Proof. See [19] page 5. □

Theorem 4.2.2. *[19]****(Rank Theorem)*** *Suppose M/P is a cyclic extension of degree m. Let p be a prime which does not divide $h(E)$, the class number of E for any field E with $P \subset E \subset M$, $E \neq M$, and which does not divide m. If $p|h(M)$ class number of M then the rank r_p of $p-$class group of M is a multiple of f, the order of p mod m.*
In this subsection we use this theorem to get some congruences on prime factors of class number of some Galois extension K/Q.

Proof. See [19] page 9. □

Lemma 4.2.3. *[14] For any field extension L/L_t, the set of fractional ideals $I(L_t)$ is embedded in $I(L)$.*

Proof. Define the map $\phi : I(L_t) \longrightarrow I(L)$ via $\phi(a) = a.O_L$ which is an ideal of O_L for any ideal a in O_{L_t}.
Then ϕ is :

- Homomorphism, since $\phi(a_1)\phi(a_2) = a_1O_La_2O_L = a_1a_2O_L = \phi(a_1a_2)$.
- ϕ is one-to-one, to see this, let $x = \Sigma_{i=1}^{k} t_io_i \in a_1O_L \bigcap O_{L_t}$ where $t_i \in a_1, o_i \in O_L \forall\ 1 \leq i \leq k$, then $o_i \in O_{L_t}\ \forall\ 1 \leq i \leq k$, otherwise there exist j such that $o_j \in O_L/O_{L_t}$ which means that
  - there exist $f \in Z[x]$, such that $f(o_j) = 0$ since $o_j \in O_L$.
  - $(o_j \notin L_t.....(*))$, otherwise $o_j \in O_{L_t}$ because of the existence of f in $Z[X]$ for which $f(o_j) = 0$.

  But $t,\ o_j \in O_{L_t}$, which means that $t_jo_j \in L_t$ which is a field, so $t_j^{-1}.t_j.o_j \in L_t$, thus $o_j \in L_t$ which contradicts $(*)$. Thus $o_i \in O_{L_t}$ for all $1 \leq i \leq k$. But $t_i \in a_1\ \forall\ 1 \leq i \leq k$, and a_1 is an ideal of O_{L_t} so $t_io_i \in a_1 \forall\ 1 \leq i \leq k$. Thus $x \in a_1$ so

$$a_1O_L \bigcap O_{L_t} \subseteq a_1 \tag{4.2.1}$$

Also let $t \in a_1$ then $t \in O_{L_t}$ and $t \in a_1O_L$, so $t \in a_1O_L \bigcap O_{L_t}$, that is

$$a_1 \subseteq a_1O_L \bigcap O_{L_t} \tag{4.2.2}$$

Thus by (4.2.1) and (4.2.2) we have

$$a_1 = a_1O_L \bigcap O_{L_t} \tag{4.2.3}$$

So if $\phi(a_1) = \phi(a_2)$, then

$a_1O_L = a_2O_L$, so

$$a_1 O_L \bigcap O_{L_t} = a_2 O_L \bigcap O_{L_t},$$

thus by (4.2.3),

$$a_1 = a_2$$

Therefore ϕ is an embedding from $I(L_t)$ to $I(L)$.

□

Lemma 4.2.4. *[14] For any field extension L/L_t, the set of ideal classes $Cl(L_t)$ is embedded in $Cl(L)$*

Proof. Define $\phi : Cl(L_t) \rightarrow Cl(L)$ by $\phi[\mathfrak{a}] = [\mathfrak{a}O_L]$, then

- $\phi[\mathfrak{a}_1.\mathfrak{a}_2] = [\mathfrak{a}_1\mathfrak{a}_2 O_L] = [\mathfrak{a}_1 O_L.\mathfrak{a}_2 O_L] = \phi[\mathfrak{a}_1].\phi[\mathfrak{a}_2]$
- If $\phi[\mathfrak{a}_1] = \phi[\mathfrak{a}_2]$, then $[\mathfrak{a}_1 O_L] = [\mathfrak{a}_2 O_L]$, so $[\mathfrak{a}_1 O_L \cap O_{L_t}] = [\mathfrak{a}_2 O_L \cap O_{L_t}]$, thus $[\mathfrak{a}_1] = [\mathfrak{a}_2]$.

Therefore $Cl(L_t)$ is embedded in $Cl(L)$. □

Theorem 4.2.5. *[14] Let L/Q be a finite algebraic extension with $[L : Q] = 2^{\alpha_0} \times N_1$, where $N_1 > 1$ is odd. Suppose that there exists a field $K \subset L$ with $[K : Q] = 2^{\alpha_0}$ and with L/K Galois solvable extension. Let $h(L)$ be the class number of L. Suppose that $h(L) > 1$. Let p be a prime dividing $h(L)$. Let r_p be the rank of the $p-$class group of L. If $p \times \prod_{i=1}^{r_p}(p^i - 1)$ and N_1 are coprime, then p divides the class number $h(K)$ of K.*

Proof. Since L/K is Galois solvable, then $G = Gal(L/K)$ is solvable, that is G has a normal series with abelian factors, $G_r \trianglerighteq G_{r-1}..... \trianglerighteq G_1 \trianglerighteq G_0 = G$, and since $[L : K]$ is finite, then G is finite, that is G_{i+1}/G_i is cyclic of prime order, then by the Fundamental Galois Theory, there is a correspondence between subgroup of G and the intermediate fields between K, L, that is there exist a tower of fields $K \subset L_1 \subset L_2 \subset ..... \subset L_j \subset L_{j+1} \subset ..... \subset L_t \subset L$.
but G_{i+1}/G_i is cyclic, so $\mathrm{Gal}(L_{j+1}/L_j)$ is cyclic $\forall j$, that is L_{j+1}/L_j is cyclic extension, and W.L.O.G by the correspondence above, we may assume that $[L_{j+1} : L_j] = q_j$, q_j is prime,

otherwise the number of intermediate fields will be more than the number of groups in the normal series.

Since $Q \subset K \subset L, [L:Q] = 2^{\alpha_0} \times N_1, [K:Q] = 2^{\alpha_0}$, then $[L:K] = N_1$ since degree is multiplicative.

$$So \;\; L/L_t \;\; is \;\; cyclic \;\; with \;\; [L:L_t] = q_t, \;\; q_t \mid N_1 \tag{4.2.4}$$

$$Now \;\; suppose \;\; that \;\; P \nmid h(L_t) \tag{4.2.5}$$

1. $P \nmid N_1$, $q_t | N_1$ "by hypotheses and equation (4.2.4)".
   so $P \nmid q_t = [L:L_t]$.

2. $L|L_t$ is cyclic.

3. With $h(L) \equiv \; (0 \; mod \; P)$, i.e. $p|h(L)$.

4. $P \nmid h(E)$ for any $L_t \subset E \subsetneq L$

because there is no E with $L_t \subset E \subset L$ except L_t, otherwise $[E:L_t]|[L:L_t] = q_t$.

Thus the hypotheses of Rank theorem are satisfied, so if f is the order of $P \; mod \; q_t$, then $f|r_p$, where r_p is the $p-$rank of $C_p(L)$, and so $P^{r_p} \equiv (\; 1 \; mod \; q_t)$ but by (4.2.4) $q_t|N_1$ which is a contradiction because $(p \times \prod_{i=1}^{r_p}(p^i - 1), \; N_1) = 1$, therefore $P|h(L_t)$.

Now, let r'_p be the $p-$rank of the class group $Cl(L_t)$, but by pushing up theorem (4.2.1) we have $h(L_t)|q_t \times h(L)$, and also we have $p|h(L_t)$, so $h(L_t)|h(L)$, otherwise $(p, q_t) \neq 1$, which contradict the hypothesis that $(p \times \prod_{i=1}^{r_p}(p^i - 1), \; N_1) = 1$ because $q_t|N_1$, but we have by lemma (4.2.4) that the $p-$class group $C_p(L_t)$ of L_t and $C_p(L)$ of L verify that $C_p(L_t)$ is embedded in $C_p(L)$, that is $r'_p \leq r_p$.

Finally, consider $N' = \frac{N}{q_t} = [L_t : K]$, we can pursuer the same algorithm with the same theorems (4.2.1) and (4.2.2) applied to extension L_t/K in place of L/K, and N' in place of N with $r'_p \leq r_p$ in place of r_p up to find a prime divisor $q_j, \; 1 \leq j \leq t$ of N such that $q_j | p \times \prod_{i=1}^{r_p}(p^i - 1)$, or to get the subfield K of L with $[L:Q] = 2^{\alpha_0}$, and $p|h(K)$. $\square$

Remark 4.2.1. Let L/K be a finite extension and let M/K be the smallest Galois extension of K containing L, let q_M be the greatest prime devisor of $[M:K]$, then $q_M|[L:K]!$.

Proof. If $[L : K] = n$, then there exist $\alpha_1 \in L, L = K(\alpha_1)$ and $p(t) \in K[t]$, with degree n and $p(\alpha_1) = 0$.

Now write $p(t) = (t - \alpha_1)p_1(t)$, where $p_1(t) \in L[t]$, so also there exist $\alpha_2 \in L_1$ such that $p_1(t) = (t-\alpha_2)p_2(t)$, $p_2(t) \in L_2(t)$, $L_2 = K(\alpha_1\alpha_2)$, and $p(\alpha_2) = 0$, so $[L_2 : L_1] \leq (n-1) = deg\ p_1(t)$.

Proceeding in this process, we can factorize $p(t) = (t - \alpha_1).....(t - \alpha_n)$, where $p(t) \in L_n(t), L_n = K(\alpha_1, ..., \alpha_n)$.

Now, since M is the smallest Galois extension of K containing L, then $M = K(\alpha_1, ..., \alpha_n)$, so $[M : K] = [L_n : L_{n-1}].....[L_1 : K]$, but $[L_j : L_{j-1}] \leq n$ for all $1 \leq j \leq n$, so if $q_M|[M : K]$, then $q_M|[L_i : L_{i-1}]$ for some $1 \leq i \leq n$, so $q_M \leq n$, therefore $q_M|[L : K]!$. □

In the following corollary, we generalize the result obtained for L/K Galois solvable extension to the case where L/K is solvable extension.

Corollary 4.2.6. *[14] Let L/Q be a finite algebraic extension with $[L : Q] = 2^{\alpha_0} \times N_1$, $N_1 > 1$ is odd. Suppose that there exists a field $K \subset L$ with $[K : Q] = 2^{\alpha_0}$, and with L/K solvable extension. Let M/K be the Galois solvable extension containing L/K. Let $h(L)$ be the class number of L. Suppose that $h(L) > 1$. Let p be a prime dividing $h(L)$ such that $p > [L : K]$. Let $r_p(M)$ be the rank of the $p-$class group of M. If $\Pi_{i=1}^{r_p(M)}(p^i - 1)$ and N_1 are coprime, then p divides the class number $h(K)$ of K.*

Proof. Since L/K is solvable extension, then the smallest *Galois extension* M of K containing L is *Galois solvable extension* , so M is an extension of L. Thus, by pushing up theorem (4.2.1), we have that $h(L)|[M : L] \times h(M)$.

Now, let q_M be the greatest prime divisor of $[M : K]$. Since M/K is the smallest Galois extension of K containing L, then by Remark (4.2.1) we have $q_M|[L : K]!$. That is; $q_M \leq [L : K]$. So, if $p|[M : L]$, then $p|[M : K]$; That is, $p \leq q_M$. So, $p \leq [L : K]$ which contradicts the hypothesis that $p > [L : K]$. But, so $p|h(L), h(L)|[M : L] \times h(M)$, and $p \nmid [M : L]$. Thus, $p|h(M)$. Therefore, by Theorem (4.2.5), we have $p|h(K)$.

□

Corollary 4.2.7. *[14] Let L/Q be a Galois solvable extension with $[L:Q]=N$, where $N>1$ is odd, let $h(L)$ be the class number of L. Suppose that $h(L)>1$. Let p be a prime divides $h(L)$. Let r_p be the $p-$rank of the $p-$class group of L. Then, $p\times\Pi_{i=1}^{r_p}(p^i-1)$ and N are not coprime. i.e. $(p\times\Pi_{i=1}^{r_p}(p^i-1),N)=1$.*

Proof. Since $O_Q=Z$, which is a principal ideal domain, then $h(Q)=1$. Hence $p\nmid h(Q)$. Then by Theorem (4.2.5), we get that $(p\times\Pi_{i=1}^{r_p}(p^i-1),N)=1$. □

Remark 4.2.2. All the previous results on which L/K is Galois solvable extension, can be applied to all abelian extensions L/K with $[K:Q]=2^{\alpha_0}$, and $[L:K]$ is odd because if L/K is abelian extension, then L/K is Galois solvable extension.

Definition 4.2.1. [13] Let K/Q be a number field with $[K:Q]=n$. Let $\{\phi_1,\phi_2,\ldots,\phi_n\}$ be an integral basis of K, and let $\{\sigma_1,\ldots,\sigma_n\}$ be the set of embedding of K in C, then we define the **discriminate of the field** K by

$$d_K=\begin{vmatrix}\sigma_1(\phi_1) & \sigma_1(\phi_2) & \ldots & \sigma_1(\phi_n)\\ \sigma_2(\phi_1) & \sigma_2(\phi_2) & \ldots & \sigma_2(\phi_n)\\ \vdots & \vdots & & \vdots\\ \sigma_n(\phi_1) & \sigma_n(\phi_1) & \ldots & \sigma_n(\phi_n)\end{vmatrix}$$

Theorem 4.2.8. *[13] Let K be a number field of degree n, with discriminant $d(K)$ and class number $h(K)$. Then:*

$$h(K)\leq\frac{2^{n-1}}{(n-1)!}|d(K)|^{\frac{1}{2}}(\log|d(K)|)^{n-1}.$$

More generally, if $a>0$ is satisfying $a\geq 2(n-1)/(\log|d(K)|)$, then

$$h(K)\leq(\frac{a+1}{2})^{n-1}\ \frac{|d(K)|^{\frac{1}{2}}}{(n-1)!}(\log|d(K)|)^{n-1}.$$

Proof. See [13] page 4. □

From Bordelles Theorem (4.2.8), if L/Q is a finite algebraic extension, and there exists a subfield F of L such that L/F is a cyclic extension with $[L:Q] = N, [L:F] = q$ where q is an odd prime, then

$$H_F = \frac{2^{m-1}}{(m-1)!} \times \sqrt{|d_F|} \times (\log(|D_F|))^{m-1}, \tag{4.2.6}$$

where d_F is the discriminant of F, $m = \frac{N}{q}$, H_F is geometry upper bound of class number of F, **i.e.** $h(F) \leq H_F$.
Thus, if p is a prime verifies that $p > H_F$, then $P \nmid h(F)$ .....(4.3.7).

Theorem 4.2.9. *[14] Let L/Q be a finite algebraic extension. Let $h(L)$ be the class number of L. Suppose that $h(L) > 1$. Suppose that there exists a cyclic extension L/F, where $q = [L:F]$ is an odd prime. Let H_F be a geometric upper bound of class number of F given by relation (4.2.6). Suppose that $p > H_F$ is a prime dividing $h(L)$. Let r_p be the rank of the $p-$class group of L. Then,*

$$p \times (p^{r_p} - 1) \equiv 0 \ mod \ q.$$

Proof. Applying Brodles Theorem (4.2.8) hypothesis, which are:

1. L/Q is a finite algebraic extension,
2. F is a subfield of L such that L/F is a cyclic extension, with $[L:F] = q$, where q is an odd prime.

We get that $p \nmid h(F)$.
Now applying rank theorem hypothesis,

1. L/F is cyclic extension, with $[L:F] = q$,
2. If p is a prime number such that $p \neq q$, then $p \nmid q = [L:F]$,
3. $p|h(L)$ from the hypothesis of the theorem,

4. We have verified that $p \nmid h(F)$, and $p \nmid h(E)$ for any $F \subset E \subsetneq L$, because there is no E with $F \subset E \subset L$ except F, otherwise $[L : E].[E : F] = q$, which is impossible because q is a prime.

Thus the hypotheses of Rank theorem are satisfied, so if f is the order of $P \ mod \ q$, then $f|r_p$, and so $P^{r_p} \equiv \ 1 \ mod \ q$, so that $P^{r_p} - 1 \equiv \ 0 \ mod \ q$.
Therefore $p \times (P^{r_p} - 1) \equiv \ 0 \ mod \ q$ as desired. □

Corollary 4.2.10. *[14] Let $L/\mathbb{Q}$ be a finite Galois extension with $[L : \mathbb{Q}] = N$. Let $h(L)$ be the class number of L. Suppose that $h(L) > 1$. Suppose that N has odd prime divisors. Let q be an odd prime divisor of N. Then, there exists a cyclic extension L/F with $q = [L : F]$. Let H_F be a geometric upper bound of class number of F given by relation (1). Suppose that $p > H_F$ is a prime dividing $h(L)$. Let r_p be the rank of the $p-$class group of L. Then,*

$$p \times (p^{r_p} - 1) \equiv 0 \ mod \ q.$$

Proof. Immediate consequence of Theorem (4.2.9) taking in consideration the existence of L/F with $[L : F] = q$ by Galois theory because L/Q is a finite Galois extension with $[L : Q] = N$, and $q|N$. □

Bibliography

[1] Anthony W. Knapp; Basic Algebra Along with a companion volume Advanced Algebra, 2006, ISBN: 978-0-8176-3248-9.

[2] Dummit and Foote, Abstract Algebra - Third Edition, 2004, John Wiley and Sons, Inc.

[3] D. Hilbert, Uber die Theorie der relativ-Abelschen Zahlkorper. Nachr. der K. Ges. der Wiss. Gottingen 377-399 (1898) = Acta Mathematica 26 (1902) 99-132.

[4] Emil Grosswald, Topics From The Theory Of Numbers, Birkhauser Boston, 1984 .

[5] Erich Heeke, Lectures on the Theory of Algebraic Numbers, 1981 by Springer-Verlag New York Inc.

[6] GRANT LARSEN, GENERALIZED FACTORIZATION. http://www.math.uchicago.edu/ may/VIGRE/VIGRE2007/REUPapers/FINALFULL/Larsen.pdf

[7] Herstein, I., Topics in Algebra. Waltham, Mass.: Blaisdell Publishing Company, 1964.

[8] H. Weber, Elliptische Funktionen und algebraische Zahlen (Braunschweig 1891).

[9] K. Takagi, Uber eine Theorie des relativ abelschen Zahlkorpers. J. College of Science, Imp. Univ. of Tokyo 41 (1920) 1-133.

[10] Michael E. Pohst, Computational Algebraic Number Theory, 1993 Birkhauser Verlag, P.O. Box 133, CH-4010 Basel, Switzerland .

[11] Millin, Algebraic Number Theory.
http://www.jmilne.org/math/CourseNotes/ANT.pdf

[12] Neukirch, Jrgen (1999), Algebraic number theory, Grundlehren der Mathematischen Wissenschaften, 322, Berlin, New York: Springer-Verlag.

[13] O. Bordell'es, Explicit upper bounds for the average order of dn(m) and application to class number, Journal of Inequalities in Pure and Applied Mathematics, vol 3, issue 3, article 38, 2002.

[14] Roland Queme, Some congruences on prime factors of class number of finite algebraic extensions K/Q, eprint arXiv:math/0304405, (April 2003).

[15] Robin Chapman, Algebraic Number Theory summary of notes May 3, 2000, School of Engineering Computer Science and Mathematics, University of Exeter.

[16] Robert B Ash , Basic Abstract Algebra: For Graduate Students and Advanced Undergraduates , Dover Publications, 2006-12-31 .

[17] Thomas W. Hungerford , Abstract Algebra, 1974 Springer-Verlag New York, Inc.

[18] Ian Stewart and David Tall, Algebraic Number Theory and Fermafs Last Theorem Third Edition, 2002 by A K Peters, Ltd.

[19] J.M. Masley, Class number of real cyclic number fields with small conductor, Compositio Mathematica, 37, 3., 1978, pp 297-319.

[20] Joseph A. Gallian, Contemporary Abstract Algebra SECOND EDITION, 1990 by D. C. Heath and Company.

[21] Jonathan Rosenberg, Algebraic K-Theory and Its Applications (Graduate Texts in Mathematics), 1994 Springer-Verlag New York, Inc.

[22] http://planetmath.org/encyclopedia/IdealClassesFormAnAbelianGroup.html.

[23] http://en.wikipedia.org/wiki/Splitting_of_prime_ideals_in_Galois_extensions.

Conclusion

In this thesis we have made a survey on one of the most important topics in algebraic number theory which is the class number and some congruences on its prime factors, and we have studied the theoretical side; I will continuo in this topic and I will study some applications on it.

Finally I hope for every one reading this work to have the usefulness.