Lectures on
Topics in Algebraic Number Theory

Sudhir R. Ghorpade
Indian Institute of Technology Bombay

Mathematisches Seminar, Bereich II
Christian-Albrechts-Universität zu Kiel
Kiel, Germany
December 2000

© Sudhir R. Ghorpade
Department of Mathematics
Indian Institute of Technology Bombay
Powai, Mumbai 400 076, India
E-Mail: srg@math.iitb.ac.in
URL: http://www.math.iitb.ac.in/∼srg

Version 1.1, August 18, 2002
[Original Version (1.0): January 7, 2002]

Preface

During December 2000, I gave a course of ten lectures on Algebraic Number Theory at the University of Kiel in Germany. These lectures were aimed at giving a rapid introduction to some basic aspects of Algebraic Number Theory with as few prerequisites as possible. I had also hoped to cover some parts of Algebraic Geometry based on the idea, which goes back to Dedekind, that algebraic number fields and algebraic curves are analogous objects. But in the end, I had no time to discuss any Algebraic Geometry. However, I tried to be thorough in regard to the material discussed and most of the proofs were either explained fully or at least sketched during the lectures. These lecture notes are a belated fulfillment of the promise made to the participants of my course and the Kieler Graduiertenkolleg. I hope that they will still be of some use to the participants of my course and other students alike.

The first chapter is a brisk review of a number of basic notions and results which are usually covered in the courses on Field Theory or Galois Theory. A somewhat detailed discussion of the notion of norm, trace and discriminant is included here. The second chapter begins with a discussion of basic constructions concerning rings, and goes on to discuss rudiments of noetherian rings and integral extensions. Although both these chapters seem to belong to Algebra, they are mostly written with a view towards Number Theory. Chapters 3 and 4 discuss topics such as Dedekind domains, ramification of primes, class group and class number, which belong more properly to Algebraic Number Theory. Some motivation and historical remarks can be found at the beginning of Chapter 3. Several exercises are scattered throughout these notes. However, I have tried to avoid the temptation of relegating as exercises some messy steps in the proofs of the main theorems. A more extensive collection of exercises is available in the books cited in the bibliography, especially [4] and [13].

In preparing these notes, I have borrowed heavily from my notes on *Field Theory and Ramification Theory* for the Instructional School on Algebraic Number Theory (ISANT) held at Bombay University in December 1994 and to a lesser extent, from my notes on *Commutative Algebra* for the Instructional Conference on Combinatorial Topology and Algebra (ICCTA) held at IIT Bombay in December 1993. Nevertheless, these notes are neither a subset nor a superset of the ISANT Notes or the ICCTA notes. In order to make these notes self-contained, I have inserted two appendices in the end. The first appendix contains my *Notes on Galois Theory*, which have been in private circulation at least since October 1994. The second appendix reproduces my recent article in *Bona Mathematica* which gives a leisurely account of discriminants. There is a slight repetition of some of the material in earlier chapters but this article may be useful for a student who might like to see some connection between the discriminant in the context of field extensions and the classical discriminant such as that of a quadratic.

It is a pleasure to record my gratitude to the participants of my course, especially, Andreas Baltz, Hauke Klein and Prof. Maxim Skriganov for their interest, and to the Kiel graduate school "Efficient Algorithms and Multiscale Methods" of the German Research Foundation ("Deutsche Forschungsgemeinschaft") for its support. I am particularly grateful to Prof. Dr. Anand Srivastav for his keen interest and encouragement. Comments or suggestions concerning these notes are most welcome and may be communicated to me by e-mail. Corrections or future revisions to these notes will be posted on my web page at `http://www.math.iitb.ac.in/~srg/Lecnotes.html` and the other notes mentioned in the above paragraph will also be available here.

Mumbai, January 7, 2002 Sudhir Ghorpade

Contents

Chapter 1

Field Extensions

We begin with a quick review of the basic facts regarding field extensions. For more details, consult Appendix A or any of the standard texts such as Lang [11] or Jacobson [9].

1.1 Basic Facts

Suppose L/K is a field extension (which means that L is a field and K is a subfield of L). We call L/K to be *finite* if as a vector space over K, L is of finite dimension; the *degree* of L/K, denoted by $[L : K]$, is defined to be the vector space dimension of L over K. Given $\alpha_1, \ldots, \alpha_n \in L$, we denote by $K(\alpha_1, \ldots, \alpha_n)$ (resp: $K[\alpha_1, \ldots, \alpha_n]$) the smallest subfield (resp: subring) of L containing K and the elements $\alpha_1, \ldots, \alpha_n$. If there exist finitely many elements $\alpha_1, \ldots, \alpha_n \in L$ such that $L = K(\alpha_1, \ldots, \alpha_n)$, then L/K is said to be *finitely generated*. An element $\alpha \in L$ such that $L = K(\alpha)$ is called a *primitive element*, and if such an element exists, then L/K is said to be a *simple* extension. If L'/K is another extension, then a homomorphism $\sigma : L \to L'$ such that $\sigma(c) = c$ for all $c \in K$ is called a *K–homomorphism* of $L \to L'$. Note that a K–homomorphism is always injective and if $[L : K] = [L' : K]$, then it is surjective. Thus if $L = L'$, then such maps are called K–automorphisms of L. The set of all K–automorphisms of L is clearly a group where the group operation defined by composition of maps. This is called the *Galois group* of L/K and is denoted by $\mathrm{Gal}(L/K)$ or $G(L/K)$. Given any subgroup H of the group of automorphisms of L, we can associate a subfield L^H of L defined by $L^H = \{\alpha \in L : \sigma(\alpha) = \alpha \text{ for all } \sigma \in H\}$; this is called the *fixed field* of H.

An element $\alpha \in L$ is said to be *algebraic* over K if it satisfies a nonzero polynomial with coefficients in K. Suppose $\alpha \in L$ is algebraic over K. Then a nonzero polynomial of least possible degree satisfied by α is clearly irreducible and, moreover, it is unique if we require it to be monic; this monic irreducible polynomial will be denoted by $\mathrm{Irr}(\alpha, K)$, and called the *minimal polynomial* of α over K. The extension L/K is said to be *algebraic* if every $\alpha \in L$ is algebraic over K. If L/K is algebraic, then we call it *separable* if $\mathrm{Irr}(\alpha, K)$ has distinct roots (in some extension of K) for every $\alpha \in L$, and we call it *normal* if $\mathrm{Irr}(\alpha, K)$ has all its roots in L for every $\alpha \in L$. It may be noted that if L/K is algebraic, then it is normal if and only if any K–homomorphism of L into some extension L' of L maps L onto itself. We call L/K to be a *Galois extension* if it is finite, separable and normal.

To check separability, one generally uses the fact that an irreducible polynomial in $K[X]$ has

distinct roots iff (= if and only if) its derivative is a nonzero polynomial. This fact follows, in turn, from the elementary observation that a root α of a polynomial $f(X) \in K[X]$ is a multiple root iff $f'(\alpha) = 0$. The above fact can be used to show that K is perfect (which means either the characteristic of K is 0 or the characteristic of K is $p \neq 0$ and $K = K^p$, i.e., for any $x \in K$, there exists $y \in K$ such that $x = y^p$) iff every algebraic extension of K is separable. On the other hand, normality can be checked using the fact a finite extension of K is normal iff it is the "splitting field" of some polynomial in $K[X]$. Recall that given a nonconstant polynomial $f(X) \in K[X]$, we can find an extension E of K such that $f(X)$ splits into linear factors in $E[X]$, and E is generated over K by the roots of $f(X)$ in E. Such an extension is unique up to a K–isomorphism, and is called the *splitting field* of $f(X)$ over K. If $\deg f(X) = n$, then the degree of the splitting field of $f(X)$ over K is at most $n!$. Thus if $f(X)$ is a nonconstant polynomial in $K[X]$ having distinct roots, and L is its splitting field over K, then L/K is an example of a Galois extension. A K–automorphism of L permutes the roots of $f(X)$, and this permutation uniquely determines the automorphism. Thus $\mathrm{Gal}(L/K)$ may be thought of as a finite group of permutations. In this case, $\mathrm{Gal}(L/K)$ is also called the Galois group of the polynomial $f(X)$ or of the equation $f(X) = 0$.

Some basic results regarding field extensions are the following.

(i) L/K is finite $\iff$ L/K is algebraic and finitely generated.

(ii) Given any $\alpha \in L$, we have:

$$\alpha \text{ is algebraic over } K \;\Leftrightarrow\; K(\alpha)/K \text{ is finite } \;\Leftrightarrow\; K(\alpha) = K[\alpha].$$

Moreover, if α is algebraic over K and $\deg \mathrm{Irr}(\alpha, K) = n$, then $\{1, \alpha, \alpha^2, \ldots, \alpha^{n-1}\}$ forms a K–basis of $K(\alpha)$.

(iii) If $\alpha_1, \ldots, \alpha_n \in L$ are algebraic, then $K(\alpha_1, \ldots, \alpha_n)$ is an algebraic extension of K. Further, if $\alpha_1, \ldots, \alpha_n$ are separable over K, then it is also a separable extension. In particular, the elements of L which are algebraic over K form a subfield of L and among these, those which are separable form a smaller subfield.

(iv) Finiteness, algebraicity and separability are "transitive" properties. That is, if E is a subfield of L containing K, then L/K is finite (resp: algebraic, separable) iff both L/E and E/K are finite (resp: algebraic, separable). Moreover, if L/K is finite, then $[L : K] = [L : E][E : K]$. In case of normality, all we can say in general is that L/K is normal implies that L/E is normal[1]. Thus, a fortiori, the same thing holds for Galois extensions.

(v) (Primitive Element Theorem). If L/K is finite and separable, then it is simple, i.e., there exists $\alpha \in L$ such that $L = K(\alpha)$.

In Number Theory, one has to usually deal with algebraic extensions of $\mathbb{Q}$, the field of rationals, or of $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$, the finite field with p elements. Since $\mathbb{Q}$ and $\mathbb{F}_p$ are clearly perfect fields, every such extension is separable and thus saying that it is Galois amounts to saying that it is finite and normal.

[1] Find examples to show that the other two possible implications are not true.

Now we come to the central result in Galois Theory. Suppose L/K is a Galois extension. Then $\mathrm{Gal}(L/K)$ is a finite group of order $[L:K]$ and its fixed field is K. In fact, we have an inclusion–reversing one–to–one correspondence between the subgroups of the Galois group of L/K and the intermediate fields between K and L. This correspondence is given as follows. Given an intermediate field E (i.e., a subfield of L containing K), the corresponding subgroup of $\mathrm{Gal}(L/K)$ is $\mathrm{Gal}(L/E)$. And given a subgroup H of $\mathrm{Gal}(L/K)$, the corresponding intermediate field is the fixed field L^H of H. Moreover, given a subfield E of L containing K, the "bottom part" E/K is Galois iff $\mathrm{Gal}(L/E)$ is a normal subgroup of $\mathrm{Gal}(L/K)$, and if this is the case, then $\mathrm{Gal}(E/K)$ is isomorphic to the factor group $\mathrm{Gal}(L/K)/\mathrm{Gal}(L/E)$. The above result is usually called the Fundamental Theorem of Galois Theory.

Adjectives applicable to a group are generally inherited by a Galois extension. Thus a Galois extension is said to be *abelian* if its Galois group is abelian, and it is said to be *cyclic* if its Galois group is cyclic.

Before ending this section, we make some remarks about the important notion of compositum (or composite) of fields, which is very useful in Algebraic Number Theory. Let E and F be subfields of the field L. The *compositum* (or the *composite*) of E and F (in L), denoted by EF, is defined to be the smallest subfield of L containing both E and F. The compositum of an arbitrary family of subfields of L is defined in a similar fashion; we use an obvious analogue of the above notation in case of a finite family of subfields. Now suppose K is a subfield of both E and F, i.e., a subfield of the field $E \cap F$. We list below some elementary facts concerning compositum of fields, which the reader may prove as exercises.

(i) If E/K is finitely generated (resp: finite, algebraic, separable, normal, Galois, abelian), then so is EF/F.

(ii) If both E/K and F/K are finitely generated (resp: finite, algebraic, separable, normal, Galois, abelian), then so is EF/K.

(iii) If E/K is Galois, then the map $\sigma \to \sigma|_E$ defines an isomorphism of $\mathrm{Gal}(EF/F)$ with the subgroup $\mathrm{Gal}(E/E \cap F)$ of $\mathrm{Gal}(E/K)$. If both E/K and F/K are Galois, then the map $\sigma \to (\sigma|_E, \sigma|_F)$ defines an isomorphism of $\mathrm{Gal}(EF/K)$ with the subgroup $\mathrm{Gal}(E/E\cap F) \times \mathrm{Gal}(F/E\cap F)$ of $\mathrm{Gal}(E/K) \times \mathrm{Gal}(F/K)$. In particular, if $E \cap F = K$, then we have natural isomorphisms $\mathrm{Gal}(EF/F) \simeq \mathrm{Gal}(E/K)$ and $\mathrm{Gal}(EF/K) \simeq \mathrm{Gal}(E/K) \times \mathrm{Gal}(F/K)$.

Observe that in view of the above properties, we can define the *maximal abelian extension of* K in L (as the compositum of all abelian extensions of K contained in L).

Exercise 1.1. Suppose L/K is a Galois extension. Let H_1 and H_2 be subgroups of $\mathrm{Gal}(L/K)$, and E_1 and E_2 be their fixed fields respectively. Show that the fixed field of $H_1 \cap H_2$ is the compositum E_1E_2 whereas the fixed field of the smallest subgroup H of $\mathrm{Gal}(L/K)$ containing H_1 and H_2 (note that if either H_1 or H_2 is normal, then $H = H_1H_2$) is $E_1 \cap E_2$.

Exercise 1.2. Let $L_1, \ldots, L_r$ be Galois extensions of K with Galois groups $G_1, \ldots, G_r$ respectively. Suppose for $1 \leq i < r$ we have $L_{i+1} \cap (L_1L_2 \ldots L_i) = K$. Then show that the Galois group of $L_1L_2 \ldots L_r$ is isomorphic to $G_1 \times G_2 \times \cdots \times G_r$.

Exercise 1.3. Suppose L/K is Galois and $\mathrm{Gal}(L/K)$ can be written as a direct product $G_1 \times \cdots \times G_r$. Let L_i be the fixed field of the subgroup $G_1 \times \ldots G_{i-1} \times \{1\} \times G_{i+1} \times \cdots \times G_r$

of G. Show that L_i/K is Galois with $\mathrm{Gal}(L_i/K) \simeq G_i$, and $L_{i+1} \cap (L_1 L_2 \dots L_i) = K$, and $L_1 L_2 \dots L_r = L$.

1.2 Basic Examples

In this section, we will discuss some examples of Galois extensions, which are quite important in Number Theory and Algebra.

Example 1: Quadratic Extensions.

An extension of degree 2 is called a *quadratic extension*. Let L/K be a quadratic extension. Suppose $\alpha \in L$ is any element such that $\alpha \notin K$. Then $[K(\alpha) : K]$ must be > 1 and it must divide $[L : K] = 2$. Therefore $L = K(\alpha)$ and α satisfies an irreducible quadratic, say $X^2 + bX + c$, with coefficients in K. The other root, say β, of this quadratic must satisfy $\alpha + \beta = -b$, and hence it is also in L. So L/K is normal. Also if $\mathrm{char}\, K \neq 2$, then clearly $\beta \neq \alpha$ and so L/K is separable as well. Thus a quadratic extension is always a Galois extension except possibly in characteristic two. Now assume that $\mathrm{char}\, K \neq 2$. Then $\mathrm{Gal}(L/K)$ is a group of order 2, and the nonidentity element in it is the automorphism of L which maps α to β. Using the (Shreedharacharya's) formula for roots of quadratic polynomial, we can replace α by $\sqrt{a}$ so that $L = K(\sqrt{a})$, where a is some element of K and $\sqrt{a}$ denotes an element of L whose square is a. With this, we can write $L = \{r + s\sqrt{a} : r, s \in K\}$ and $\mathrm{Gal}(L/K) = \{\mathrm{id}, \sigma\}$, where id denotes the identity automorphism of L and σ is the K–automorphism defined by $\sigma(r + s\sqrt{a}) = r - s\sqrt{a}$.

If $K = \mathbb{Q}$ and L is a subfield of $\mathbb{C}$ such that $[L : \mathbb{Q}] = 2$, then it is called a *quadratic field*. In general, a subfield of $\mathbb{C}$ which is of finite degree over $\mathbb{Q}$ is known as an *algebraic number field* or simply, a *number field*. In view of the above discussion, we easily see that if L is a quadratic field, then there exists a unique squarefree integer m, with $m \neq 0, 1$, such that $L = \mathbb{Q}(\sqrt{m})$. We say that L is a *real quadratic field* or *imaginary quadratic field* according as $m > 0$ or $m < 0$.

Exercise 1.4. Suppose L/K is a *biquadratic extension*, i.e., $L = K(\alpha, \beta)$ where α, β are elements of L which are not in K but whose squares are distinct elements of K. Assume that $\mathrm{char}\, K \neq 2$. Show that L/K is a Galois extension and compute its Galois group.

Example 2: Cyclotomic Extensions.

Let k be a field and n be a positive integer. An element $\omega \in k$ such that $\omega^n = 1$ is called an n^{th} root of unity (in k). Let $\mu_n = \mu_n(k)$ denote the set of all n^{th} roots of unity in k. Then μ_n is a finite subgroup of the multiplicative group k^* of nonzero elements of k, and therefore it is cyclic. Any generator of μ_n is called a *primitive* n^{th} *root of unity* in k. For example, if $k = \mathbb{C}$, then $\zeta = \zeta_n = e^{2\pi i/n}$ is a primitive n^{th} root of unity, and $\mu_n(\mathbb{C})$ consists of the n elements $1, \zeta, \zeta^2, \dots, \zeta^{n-1}$; among these the elements ζ^j where $(j, n) = 1$, are precisely the primitive n^{th} roots of unity (verify!). The subfield $\mathbb{Q}(\zeta)$ of $\mathbb{C}$ generated by ζ over $\mathbb{Q}$ is called the n^{th} *cyclotomic field*, and the extension $\mathbb{Q}(\zeta)/\mathbb{Q}$ is called a *cyclotomic extension*. Since the polynomial $X^n - 1$ splits into distinct linear factors in $\mathbb{Q}(\zeta)[X]$ as

$$X^n - 1 = \prod_{i=0}^{n-1} (X - \zeta^i)$$

we see that $\mathbb{Q}(\zeta)/Q$ is a Galois extension whose degree is at most n. Suppose $G = \mathrm{Gal}(\mathbb{Q}(\zeta)/\mathbb{Q})$ and $\sigma \in G$. Then $\sigma(\zeta)$ must also be a root of $X^n - 1$, and therefore $\sigma(\zeta) = \zeta^j$ for some integer $j = j(\sigma)$. It is clear that σ uniquely determines $j(\sigma)$ modulo n. Hence the map $\sigma \to j(\sigma)$ is injective. Moreover, if $\sigma, \tau \in G$, then we have $j(\sigma\tau) = j(\sigma)j(\tau)(\mathrm{mod}\ n)$. Since G is a group, we see that $j(\sigma)(\mathrm{mod}\ n)$ is a unit in $\mathbb{Z}/n\mathbb{Z}$, and $\sigma \to j(\sigma)$ defines an injective homomorphism of G into $(\mathbb{Z}/n\mathbb{Z})^\times$, the multiplicative group of units[2] in $\mathbb{Z}/n\mathbb{Z}$. It follows that G is abelian and its order is at most $\varphi(n)$, where φ is the Euler totient function defined by

$$\varphi(n) = \text{ the number of positive integers } \leq n \text{ and relatively prime to } n.$$

We will now show that the order of G, i.e., $[\mathbb{Q}(\zeta) : \mathbb{Q}]$, is exactly equal to $\varphi(n)$, which will imply that the Galois group of $\mathbb{Q}(\zeta)/Q$ is naturally isomorphic to $(\mathbb{Z}/n\mathbb{Z})^\times$. For this, we need the following elementary fact which will be proved later in Section 2.4.

FACT: *If a monic polynomial with integer coefficients factors as $f(X)g(X)$, where $f(X)$ and $g(X)$ are monic polynomials with rational coefficients, then the coefficients of $f(X)$ and $g(X)$ must be integers.*

To prove the earlier assertion, let $\Phi_n(X)$ denote the minimal polynomial of $\zeta = \zeta_n$ over $\mathbb{Q}$. Then it must divide $X^n - 1$ in $\mathbb{Q}[X]$. Hence by the FACT above, $\Phi_n(X)$ must have integer coefficients and $X^n - 1 = \Phi_n(X)g(X)$, for some monic polynomial $g(X) \in \mathbb{Z}[X]$. Now let p be a prime number which doesn't divide n and α be a root of $\Phi_n(X)$. We claim that α^p must also be a root of $\Phi_n(X)$. To prove the claim, assume the contrary. Then α^p is a root of $g(X)$ and hence α is a root of $g(X^p)$. Thus $g(X^p) = \Phi_n(X)h(X)$ for some $h(X) \in \mathbb{Z}[X]$ (using the FACT once again!). Now reduce (mod p), i.e., consider the polynomials $\bar{g}(X), \bar{h}(X)$, etc obtained by reducing the coefficients of $g(X), h(X)$, etc., (mod p). Then (by Fermat's little theorem!), we find that $(\bar{g}(X))^p = \bar{g}(X^p) = \bar{\Phi}_n(X)\bar{h}(X)$. This implies that $\bar{g}(X)$ and $\bar{\Phi}_n(X)$ have a common root, and therefore the polynomial $X^n - \bar{1}$ in $\mathbb{Z}/p\mathbb{Z}[X]$ has a multiple root. But the latter is impossible since the derivative of $X^n - \bar{1}$ is $\bar{n}X^{n-1}$, which has zero as its only root since n is not divisible by p. This proves our claim, and, as a consequence, it follows that ζ^j is a root of $\Phi_n(X)$ for all integers j such that $(j, n) = 1$. Hence we find that $|G| = [\mathbb{Q}(\zeta) : \mathbb{Q}] = \deg \Phi_n(X)$ is $\geq \varphi(n)$. This together with the previous argument proves the equality. We also find that

$$\mathrm{Irr}(\zeta, \mathbb{Q}) = \Phi_n(X) = \prod_{\substack{0 \leq j \leq n-1 \\ (j,n)=1}} (X - \zeta^j).$$

The above polynomial is called the n^{th} *cyclotomic polynomial*. As noted above, it has integer coefficients and its degree is $\varphi(n)$. Collating the terms suitably in the product representation of $X^n - 1$, we readily see that

$$X^n - 1 = \prod_{d|n} \Phi_d(X)$$

[2]The structure of this group is well–known from Elementary Number Theory. To begin with, if $n = p_1^{e_1} \ldots p_g^{e_g}$ is the factorization of n as a product of powers of distinct primes, then by Chinese Remainder Theorem [see, for example. Prop. 2.3 in the next chapter], we have $(\mathbb{Z}/n\mathbb{Z})^\times \simeq (\mathbb{Z}/p_1^{e_1}\mathbb{Z})^\times \times \cdots \times (\mathbb{Z}/p_g^{e_g}\mathbb{Z})^\times$. If p is a prime and e a positive integer, then $(\mathbb{Z}/p^e\mathbb{Z})^\times$ is cyclic if p is odd or $p = 2$ and $e \leq 2$. If $e > 2$, then $(\mathbb{Z}/2^e\mathbb{Z})^\times$ is the direct product of $\mathbb{Z}/2\mathbb{Z}$ and $\mathbb{Z}/2^{e-2}\mathbb{Z}$. In particular, $(\mathbb{Z}/n\mathbb{Z})^\times$ is cyclic, i.e., primitive roots (mod n) exist iff $n = 2, 4, p^e$ or $2p^e$ where p is an odd prime. See, for example, [2] or [8] for details.

and so, in particular $n = \sum_{d|n} \varphi(d)$. The above formula, in fact, gives an efficient way to compute $\Phi_n(X)$ in a recursive manner.

Let m and n be relatively prime positive integers. We know from Elementary Number Theory, that φ is a multiplicative function, and thus $\varphi(mn) = \varphi(m)\varphi(n)$. This implies that $[\mathbb{Q}(\zeta_{mn}) : \mathbb{Q}] = [\mathbb{Q}(\zeta_m) : \mathbb{Q}][\mathbb{Q}(\zeta_n) : \mathbb{Q}]$. Moreover, we clearly have that ζ_{mn}^m is a primitive n^{th} root of unity, ζ_{mn}^n is a primitive m^{th} root of unity, and $\zeta_m\zeta_n$ is a primitive mn^{th} root of unity. Therefore $\mathbb{Q}(\zeta_{mn})$ must equal the compositum $\mathbb{Q}(\zeta_m)\mathbb{Q}(\zeta_n)$. This together with the previous equality shows that $\mathbb{Q}(\zeta_m) \cap \mathbb{Q}(\zeta_n) = \mathbb{Q}$.

Exercise 1.5. If p is a prime number, then show that

$$\Phi_p(X) = \frac{X^p - 1}{X - 1} = X^{p-1} + X^{p-2} + \cdots + X + 1$$

and for any $e \geq 1$, $\Phi_{p^e}(X) = \Phi_p(X^{p^{e-1}})$. Use this and the Eisenstein Criterion for $\Phi_{p^e}(X + 1)$ to show directly that $\Phi_{p^e}(X)$ is irreducible in $\mathbb{Q}[X]$.

Exercise 1.6. [This exercise assumes some familiarity with Elementary Number Theory.[3]] Let p be an odd prime, and ζ be a primitive p^{th} root of unity. Consider the Gauss sum $g = \sum_{t=1}^{p-1} \left(\frac{t}{p}\right) \zeta^t$. Show that $g^2 = (-1)^{(p-1)/2}p$. Deduce that the quadratic extension $\mathbb{Q}(\sqrt{p})$ is contained in p^{th} or $(2p)^{\text{th}}$ cyclotomic extension. Conclude that any quadratic extension is contained in some cyclotomic extension.

Example 3: Finite fields

Let F be a finite field. Its characteristic must be a prime number, say p. Thus we may assume that it contains $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$ as a subfield. The extension $F/\mathbb{F}_p$ has to be finite and if its degree is m, then, evidently, F contains precisely $q = p^m$ elements. Now since $F^* = F \setminus \{0\}$ is a group of order $q - 1$, each of the q elements of F satisfies the polynomial $X^q - X$. Thus F is a splitting field of $X^q - X$ over $\mathbb{F}_p$. It follows that for any prime power q, there is, up to isomorphism, a unique field of order q. Explicitly, it is the splitting field of $X^q - X$ over $\mathbb{Z}/p\mathbb{Z}$. For this reason, one uses the notation $\mathbb{F}_q$ or $GF(q)$ to denote a field of order q. Now suppose L is a finite extension of F of degree n. Then L is a finite field and $|L| = q^n$. Also, L is a splitting field over $\mathbb{F}_p$ (and hence over F) of the polynomial $X^{q^n} - X$ which has distinct roots (since its derivative is -1, which is never zero). It follows that L/F is a Galois extension. The map $\sigma : L \to L$ defined by $\sigma(\alpha) = \alpha^q$ is an F–automorphism of L (Verify!). Its powers $\mathrm{id}, \sigma, \sigma^2, \ldots, \sigma^{n-1}$ are distinct because otherwise $\sigma^i = \mathrm{id}$ for some i with $0 < i < n$ and thus every $x \in L$ satisfies $x^{q^i} = x$, which is a contradiction since $|L| = q^n > q^i$. Moreover, $\sigma^n = \mathrm{id}$. Since $\mathrm{Gal}(L/F)$ must have order $n = [L : F]$, it follows that the Galois group of L/F is the cyclic group of order n generated by σ. The map σ which is a canonical generator of the Galois group of L/F is called the *Frobenius automorphism.*

[3] All you need to know really is that if p is prime and a is an integer not divisible by p, then the Legendre symbol $\left(\frac{a}{p}\right)$ is, by definition, equal to 1 if $a \equiv x^2 (\mathrm{mod}\ p)$ for some integer x, and is equal to -1 otherwise. It is multiplicative, i.e., $\left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right)\left(\frac{b}{p}\right)$, and Euler's Criterion, viz., $\left(\frac{a}{p}\right) \equiv a^{(p-1)/2} (\mathrm{mod}\ p)$ holds for any odd prime p.

1.3 Norm, Trace and Discriminant

In this section we briefly recall the notions of norm, trace and the discriminant in the context of field extensions.

Suppose L/K is a finite extension of degree n. Given any $\alpha \in L$, we define its *trace* w.r.t. L/K, denoted by $\mathrm{Tr}_{L/K}(\alpha)$, to be the trace of the K–linear transformation $x \mapsto \alpha x$ of $L \to L$. The determinant of this linear transformation is called the *norm* of α w.r.t L/K and is denoted by $N_{L/K}(\alpha)$. Equivalently, if $\Phi(X) = X^n + a_1 X^{n-1} + \cdots + a_n$ is the characteristic polynomial of the above linear transformation (which is called the *field polynomial* of α w.r.t. L/K), then $\mathrm{Tr}(\alpha) = -a_1$ and $N(\alpha) = (-1)^n a_n$. As done here, the subscript L/K is usually dropped if it is clear from the context.

Basic properties of norm and trace are as follows.

(i) $\mathrm{Tr}_{L/K}$ is a K–linear map of $L \to K$. For $a \in K$, $\mathrm{Tr}(a) = na$.

(ii) $N_{L/K}$ is a multiplicative map of $L \to K$ (i.e., $N(\alpha\beta) = N(\alpha)N(\beta)$ for $\alpha, \beta \in L$). For $a \in K$, $N(a) = a^n$.

(iii) If L/K is a Galois extension, then trace is the sum of the conjugates whereas the norm is the product of the conjugates. More precisely, for any $\alpha \in L$, we have

$$\mathrm{Tr}_{L/K}(\alpha) = \sum_{\sigma \in \mathrm{Gal}(L/K)} \sigma(\alpha) \qquad \text{and} \qquad N_{L/K}(\alpha) = \prod_{\sigma \in \mathrm{Gal}(L/K)} \sigma(\alpha).$$

(iv) Norm and trace are transitive. That is, if E is a subfield of L containing K, then for any $\alpha \in L$, we have

$$\mathrm{Tr}_{L/K}(\alpha) = \mathrm{Tr}_{E/K}(\mathrm{Tr}_{L/E}(\alpha)) \qquad \text{and} \qquad N_{L/K}(\alpha) = N_{E/K}(N_{L/E}(\alpha)).$$

In fact, Property (iii) holds in a more general context. Indeed, if L/K is separable and N is some (fixed) normal extension of K containing L, then every $\alpha \in L$ has exactly $n = [L : K]$ conjugates (w.r.t. L/K) in N [these are, by definition, the elements $\sigma(\alpha)$ as σ varies over all K–homomorphisms of $L \to N$]. In the case $L = K(\alpha)$, these n conjugates are distinct and they are precisely the roots (in N) of the minimal polynomial $\mathrm{Irr}(\alpha, K)$ of α over K. In any case, if L/K is separable and $\alpha^{(1)}, \alpha^{(2)}, \ldots, \alpha^{(n)}$ denote the conjugates of α w.r.t. L/K, then we have

$$\mathrm{Tr}_{L/K}(\alpha) = \alpha^{(1)} + \alpha^{(2)} + \cdots + \alpha^{(n)} \qquad \text{and} \qquad N_{L/K}(\alpha) = \alpha^{(1)}\alpha^{(2)} \ldots \alpha^{(n)}.$$

It may also be noted that in the above set-up, the field polynomial of α w.r.t. L/K is given by $\prod_{i=1}^{n} \left(X - \alpha^{(i)}\right)$, and moreover, it equals $\mathrm{Irr}(\alpha, K)^{[L:K(\alpha)]}$. For a more detailed discussion of the notions of norm and trace and proofs of the above results, one may refer to Appendix A or the books [18] or [20].

Remark 1.7. It should be noted that the definitions of trace and norm make sense even when L is a ring containing the field K as a subring such that L is of finite dimension n as a vector space over K. In this generality, the properties 1 and 2 above continue to hold. We shall have an occasion to use trace in this general context in some later sections.

We shall now review the notion of discriminant as it appears in the theory of field extensions. For connection of this to the classical notions of discriminant (such as that of a quadratic or a cubic), see Appendix B.

Let K be field and L be a ring which contains K as a subfield and which has finite dimension n as a vector space over K. [In most of the applications, L will be a field extension of K of degree n.] As remarked above, the notions of trace and norm of elements of L w.r.t K make sense in this general set-up. Given any n elements $\alpha_1, \ldots, \alpha_n \in L$, the *discriminant* $D_{L/K}(\alpha_1, \ldots, \alpha_n)$ of $\alpha_1, \ldots, \alpha_n$ w.r.t. L/K is defined to be the determinant of the $n \times n$ matrix $\left(\mathrm{Tr}_{L/K}(\alpha_i \alpha_j)\right)$ [$1 \leq i, j \leq n$]. Note that $D_{L/K}(\alpha_1, \ldots, \alpha_n)$ is an element of K.

Lemma 1.8. *If $\alpha_1, \ldots, \alpha_n \in L$ satisfy $D_{L/K}(\alpha_1, \ldots, \alpha_n) \neq 0$, then $\{\alpha_1, \ldots, \alpha_n\}$ is a K–basis of L.*

Proof. It suffices to show that $\alpha_1, \ldots, \alpha_n$ are linearly independent over K. Suppose $\sum_{i=1}^n c_i \alpha_i = 0$ for some $c_1, \ldots, c_n \in K$. Multiplying the equation by α_j and taking the trace, we find that $\sum_{i=1}^n c_i \mathrm{Tr}(\alpha_i \alpha_j) = 0$. By hypothesis, the matrix $\left(\mathrm{Tr}_{L/K}(\alpha_i \alpha_j)\right)$ is nonsingular. Hence it follows that $c_j = 0$ for $j = 1, \ldots, n$. □

Lemma 1.9. *If $\{\alpha_1, \ldots, \alpha_n\}$ and $\{\beta_1, \ldots, \beta_n\}$ are two K–bases of L and $\alpha_i = \sum_{j=1}^n a_{ij} \beta_j$, $a_{ij} \in K$, then we have*

$$D_{L/K}(\alpha_1, \ldots, \alpha_n) = [\det(a_{ij})]^2 D_{L/K}(\beta_1, \ldots, \beta_n).$$

In particular, since (a_{ij}) is nonsingular, $D_{L/K}(\alpha_1, \ldots, \alpha_n) = 0$ iff $D_{L/K}(\beta_1, \ldots, \beta_n) = 0$.

Proof. For any $i, j \in \{1, \ldots, n\}$, we have

$$\alpha_i \alpha_j = \left(\sum_{k=1}^n a_{ik} \beta_k\right) \alpha_j = \sum_{k=1}^n a_{ik} \beta_k \left(\sum_{l=1}^n a_{jl} \beta_l\right) = \sum_{k=1}^n \sum_{l=1}^n a_{ik} a_{jl} \beta_k \beta_l.$$

Taking trace of both sides, and letting A denote the matrix (a_{ij}), we see that

$$\left(\mathrm{Tr}(\alpha_i \alpha_j)\right) = A^{\mathrm{t}} \left(\mathrm{Tr}(\beta_i \beta_j)\right) A$$

and so the result follows. □

Remarks 1.10. 1. We shall say that the discriminant of L/K is zero (or nonzero) and write $D_{L/K} = 0$ (or $D_{L/K} \neq 0$) if for some K–basis $\{\alpha_1, \ldots, \alpha_n\}$ of L, $D_{L/K}(\alpha_1, \ldots, \alpha_n)$ is zero (or nonzero). The last lemma justifies this terminology.

2. Observe that $\mathrm{Tr}_{L/K}(xy)$ is clearly a symmetric K–bilinear form [which means that the map $(x, y) \mapsto \mathrm{Tr}_{L/K}(xy)$ of $L \times L \to K$ is a symmetric K–bilinear map]. The condition that $D_{L/K} \neq 0$ is equivalent to saying that this form is non-degenerate. From Linear Algebra, one knows that if the non-degeneracy condition is satisfied, then for any K–basis $\{\alpha_1, \ldots, \alpha_n\}$ of L, we can find a "dual basis" $\{\beta_1, \ldots, \beta_n\}$ of L over K such that $\mathrm{Tr}_{L/K}(\alpha_i \beta_j) = \delta_{ij}$, where δ_{ij} is the usual Kronecker delta which is 1 if $i = j$ and 0 otherwise.

We now prove an important result which is very useful in explicit computations of the discriminant. Here, and henceforth in this section, we shall require L to be a field.

Theorem 1.11. *If L/K is a finite separable field extension, then its discriminant is nonzero. In fact, if α is a primitive element (so that $L = K(\alpha)$ and $\{1, \alpha, \alpha^2, \ldots, \alpha^{n-1}\}$ is a K–basis of L) and $f(X)$ is its minimal polynomial, then we have*

$$D_{L/K}(1, \alpha, \alpha^2, \ldots, \alpha^{n-1}) \;=\; \prod_{i>j} \left(\alpha^{(i)} - \alpha^{(j)}\right)^2 \;=\; (-1)^{n(n-1)/2}\, N_{L/K}(f'(\alpha))$$

where $\alpha^{(1)}, \alpha^{(2)}, \ldots, \alpha^{(n)}$ denote the conjugates of α w.r.t. L/K and $f'(\alpha)$ denotes the derivative of $f(X)$ evaluated at α.

Proof. Since L/K is separable, the trace of any element of L equals the sum of its conjugates w.r.t. L/K (in some fixed normal extension N of K containing L). Thus if $\{u_1, \ldots, u_n\}$ is a K–basis of L and ${u_i}^{(1)}, {u_i}^{(2)}, \ldots, {u_i}^{(n)}$ denote the conjugates of u_i w.r.t. L/K, then we have $\mathrm{Tr}(u_i u_j) = \sum_{k=1}^{n} u_i^{(k)} u_j^{(k)}$. In other words, the matrix $(\mathrm{Tr}(u_i u_j))$ equals the product of the matrix $\left(u_i^{(j)}\right)$ with its transpose. Therefore

$$D_{L/K}(u_1, \ldots, u_n) \;=\; \begin{vmatrix} u_1^{(1)} & u_1^{(2)} & \ldots & u_1^{(n)} \\ u_2^{(1)} & u_2^{(2)} & \ldots & u_2^{(n)} \\ \vdots & \vdots & \ddots & \vdots \\ u_n^{(1)} & u_n^{(2)} & \ldots & u_n^{(n)} \end{vmatrix}^2 .$$

In case $u_1, u_2, \ldots, u_n$ are $1, \alpha, \ldots, \alpha^{(n-1)}$ respectively, then the determinant above is a Vandermonde determinant and the RHS becomes

$$\begin{vmatrix} 1 & 1 & \ldots & 1 \\ \alpha^{(1)} & \alpha^{(2)} & \ldots & \alpha^{(n)} \\ \vdots & \vdots & \ddots & \vdots \\ \left(\alpha^{n-1}\right)^{(1)} & \left(\alpha^{n-1}\right)^{(2)} & \ldots & \left(\alpha^{n-1}\right)^{(n)} \end{vmatrix}^2 = \prod_{i>j} \left(\alpha^{(i)} - \alpha^{(j)}\right)^2 = (-1)^{n(n-1)/2} \prod_{i \neq j} \left(\alpha^{(i)} - \alpha^{(j)}\right).$$

Moreover, we clearly have

$$f(X) = \prod_{i=1}^{n} \left(X - \alpha^{(i)}\right), \quad f'(X) = \sum_{i=1}^{n} \prod_{j \neq i} \left(X - \alpha^{(j)}\right), \quad \text{and} \quad N_{L/K}(f'(\alpha)) = \prod_{i=1}^{n} f'\left(\alpha^{(i)}\right).$$

Therefore, we obtain the desired formulae. Our first assertion follows from the fact that if $L = K(\alpha)$ is separable over K, then the conjugates $\alpha^{(1)}, \alpha^{(2)}, \ldots, \alpha^{(n)}$ of α w.r.t L/K are distinct. □

Corollary 1.12. *If L/K is a finite separable extension, then the symmetric bilinear form $\mathrm{Tr}_{L/K}(xy)$ is nondegenerate.*

Remark 1.13. The converse of the above Theorem, viz., if $D_{L/K} \neq 0$ then L/K is separable, is also true. For a proof, see [20].

Chapter 2

Ring Extensions

In this chapter, we review some basic facts from Ring Theory.

2.1 Basic Processes in Ring Theory

There are three basic processes in Algebra using which we can obtain a new ring from a given ring[1]. Let us discuss them briefly.

Polynomial Ring: Given a ring A, we can form the ring of all polynomials in n variables (say, $X_1, \ldots, X_n$) with coefficients in A. This ring is denoted by $A[X_1, \ldots, X_n]$. Elements of $A[X_1, \ldots, X_n]$ look like

$$f = \sum a_{i_1 \ldots i_n} X_1^{i_1} \ldots X_n^{i_n}, \qquad a_{i_1 \ldots i_n} \in A,$$

where $(i_1, \ldots, i_n)$ vary over a finite set of nonnegative integral n–tuples. A typical term (excluding the coefficient), viz., $X_1^{i_1} \ldots X_n^{i_n}$, is called a *monomial*; its (usual) *degree* is $i_1 + \cdots + i_n$. If $f \neq 0$, then the (total) *degree* of f is defined by $\deg f = \max\{i_1 + \cdots + i_n : a_{i_1 \ldots i_n} \neq 0\}$. Usual convention is that $\deg 0 = -\infty$. A *homogeneous polynomial* of degree d in $A[X_1, \ldots, X_n]$ is simply a finite A–linear combination of monomials of degree d. The set of all homogeneous polynomials of degree d is denoted by $A[X_1, \ldots, X_n]_d$. Note that any $f \in A[X_1, \ldots, X_n]$ can be uniquely written as $f = f_0 + f_1 + \ldots$, where $f_i \in A[X_1, \ldots, X_n]_i$ and $f_i = 0$ for $i > \deg f$; we may call f_i's to be the *homogeneous components* of f. If $f \neq 0$ and $d = \deg f$, then clearly $f_d \neq 0$ and $f = f_0 + f_1 + \cdots + f_d$.

Quotient Ring: That is, the residue class ring A/I obtained by 'moding out' an ideal I from a ring A. This is same as taking a homomorphic image. Passing to A/I from A has the effect of making I the null element. We have a natural surjective homomorphism $q : A \to A/I$ given by $q(x) = x + I$ for $x \in A$. There is a one-to-one correspondence between the ideals of A containing I and the ideals of A/I given by $J \mapsto q(J) = J/I$ and $J' \mapsto q^{-1}(J')$.

Localization: That is, the ring of fractions $S^{-1}A$ of a ring A w.r.t. a multiplicatively closed (m.c.) subset S of A [i.e., a subset S of A such that $1 \in S$ and $a, b \in S \Rightarrow ab \in S$]. Elements of $S^{-1}A$ are, essentially, fractions of the type $\frac{a}{s}$, where $a \in A$ and $s \in S$; the notion of equality in $S^{-1}A$ is understood as follows. $\frac{a}{s} = \frac{b}{t} \Leftrightarrow u(at - bs) = 0$, for some $u \in S$.

[1] here, and hereafter, by a ring we mean a commutative ring with identity.

Quite often, we consider $S^{-1}A$ when A is a domain and $0 \notin S$; in this case, the notion of equality (or, if you like, equivalence) is simpler and more natural. Note that if A is a domain and $S = A \setminus \{0\}$, then $S^{-1}A$ is nothing but the quotient field of A. Important instance of localization is when $S = A \setminus \mathfrak{p}$, where $\mathfrak{p}$ is a prime ideal of A; in this case $S^{-1}A$ is customarily denoted by $A_{\mathfrak{p}}$. Passing from A to $A_{\mathfrak{p}}$ has the effect of making $\mathfrak{p}$ into a maximal ideal that consists of all nonunits; indeed, $A_{\mathfrak{p}}$ is a *local ring* [which means, a ring with a unique maximal ideal] with $\mathfrak{p}A_{\mathfrak{p}}$ as its unique maximal ideal. In general, we have a natural homomorphism $\phi : A \to S^{-1}A$ defined by $\phi(x) = \frac{x}{1}$. This is injective if S consists of nonzerodivisors, and in this case A may be regarded as a subring of $S^{-1}A$. Given an ideal I of A, the ideal of $S^{-1}A$ generated by $\phi(I)$ is called the *extension* of I, and is denoted by $IS^{-1}A$ or by $S^{-1}I$. For an ideal J of $S^{-1}A$, the inverse image $\phi^{-1}(J)$ is an ideal of A and is called the contraction of J to A. By abuse of language, the contraction of J is sometimes denoted by $J \cap A$. We have $S^{-1}(J \cap A) = J$ and $S^{-1}I \cap A \supseteq I$, and the last inclusion can be strict. This implies that there is a one-to-one correspondence between the ideals J of $S^{-1}A$ and the ideals I of A such that $\{a \in A : as \in I \text{ for some } s \in S\} = I$. This, in particular, gives a one-to-one correspondence between the prime ideals of $S^{-1}A$ and the prime ideals P of A such that $P \cap S = \emptyset$.

Exercise 2.1. Show that localization commutes with taking homomorphic images. More precisely, if I is an ideal of a ring A and S is a m. c. subset of A, then show that $S^{-1}A/S^{-1}I$ is isomorphic to $\bar{S}^{-1}(A/I)$, where $\bar{S}$ denotes the image of S in A/I.

Given ideals I_1 and I_2 in a ring A, their *sum* $I_1 + I_2 = \{a_1 + a_2 : a_1 \in I_1,\ a_2 \in I_2\}$, their *product* $I_1 I_2 = \{\sum a_i b_i : a_i \in I_1,\ b_i \in I_2\}$, and intersection $I_1 \cap I_2$ are all ideals. Analogue of division is given by the *colon ideal* $(I_1 : I_2)$, which is defined to be the ideal $\{a \in A : aI_2 \subseteq I_1\}$. If I_2 equals a principal ideal (x), then $(I_1 : I_2)$ is often denoted simply by $(I_1 : x)$. The ideals I_1 and I_2 are said to be *comaximal* if $I_1 + I_2 = A$. We can also consider the *radical* of an ideal I, which is defined by $\sqrt{I} = \{a \in A : a^n \in I \text{ for some } n \geq 1\}$, and which is readily seen to be an ideal (by Binomial Theorem!). One says that I is a *radical ideal* if $\sqrt{I} = I$. Note that the notions of sum and intersections of ideals extend easily to arbitrary families of ideals.

Exercise 2.2. Show that colon commutes with intersections. That is, if $\{I_i\}$ is a family of ideals of a ring A, then for any ideal J of A, we have $\cap(I_i : J) = (\cap I_i : J)$. Further, if $\{I_i\}$ is a finite family, then show that $\sqrt{\cap I_i} = \cap\sqrt{I_i}$. Give examples to show that these results do not hold (for finite families) if intersections are replaced by products.

A useful fact about ideals is the following. The case when the ring in question is $\mathbb{Z}$ is considered, for example, in Ch'in Chiu-Shao's *Mathematical Treatise* in the year 1247.

Proposition 2.3 (Chinese Remainder Theorem). *Let $I_1, I_2, \ldots, I_n$ are pairwise comaximal ideals in a ring A (i.e., $I_i + I_j = A$ for all $i \neq j$). Then:*

(i) $I_1 I_2 \ldots I_n = I_1 \cap I_2 \cap \cdots \cap I_n$.

(ii) Given any $x_1, \ldots, x_n \in A$, there exists $x \in A$ such that $x \equiv x_j (\mathrm{mod}\ I_j)$ for $1 \leq j \leq n$.

(iii) The map $x(\mathrm{mod}\ I_1 I_2 \cdots I_n) \mapsto (x(\mathrm{mod}\ I_1), \ldots, x(\mathrm{mod}\ I_n))$ defines an isomorphism of $A/I_1 I_2 \ldots I_n$ onto the direct sum $A/I_1 \oplus A/I_2 \oplus \cdots \oplus A/I_n$.

Proof. (i) Given any $i \in \{1, \ldots, n\}$, let $J_i = I_1 \cdots I_{i-1} I_{i+1} \cdots I_n$. Since $I_i + I_j = A$, we can find $a_{ij} \in I_j$ such that $a_{ij} \equiv 1 (\mathrm{mod}\ I_i)$, for all $j \neq i$. Let $a_i = \prod_{j \neq i} a_{ij}$. Then $a_i \equiv 1 (\mathrm{mod}\ I_i)$ and $a_i \in J_i$. Thus $I_i + J_i = A$. Now, $x = x_1 a_1 + \cdots + x_n a_n$ satisfies $x \equiv x_j (\mathrm{mod}\ I_j)$ for $1 \leq j \leq n$.

(ii) Clearly, $I_1 I_2 \dots I_n \subseteq I_1 \cap I_2 \cap \dots \cap I_n$. To prove the other inclusion, we induct on n. The case of $n = 1$ is trivial. Next, if $n = 2$, then we can find $a_1 \in I_1$ and $a_2 \in I_2$ such that $a_1 + a_2 = 1$. Now, $a \in I_1 \cap I_2$ implies that $a = aa_1 + aa_2$, and thus $a \in I_1 I_2$. Finally, if $n > 2$, then as in (i), let $J_1 = I_2 \cdots I_n$ and note that $I_1 + J_1 = A$. Hence by induction hypothesis and the case of two ideals, $I_1 \cap I_2 \cap \dots \cap I_n = I_1 \cap J_1 = I_1 J_1 = I_1 I_2 \cdots I_n$.

(iii) The map $x (\mathrm{mod}\ I_1 I_2 \cdots I_n) \mapsto (x (\mathrm{mod}\ I_1), \dots, x (\mathrm{mod}\ I_n))$ is clearly well-defined and a homomorphism. By (i), it is surjective and by (ii), it is injective. □

Exercise 2.4. With $I_1, \dots, I_n$ and A as in Proposition 2.3, show that the map in (iii) induces an isomorphism of $(A/I_1 I_2 \dots I_n)^\times$ onto the direct sum $(A/I_1)^\times \oplus (A/I_2)^\times \oplus \dots \oplus (A/I_n)^\times$. Deduce that the Euler ϕ-function is multiplicative.

2.2 Noetherian Rings and Modules

A ring A is said to be *noetherian* if every ideal of A is finitely generated. It is easy to see that this condition equivalent to either of the two conditions below.

(i) (Ascending Chain Condition or a.c.c.) If $I_1, I_2, \dots$ are ideals of A such that $I_1 \subseteq I_2 \subseteq \dots$, then there exists $m \geq 1$ such that $I_n = I_m$ for $n \geq m$.

(ii) (Maximality Condition) Every nonempty set of ideals of A has a maximal element.

The class of noetherian rings has a special property that it is closed w.r.t. each of the three fundamental processes. Indeed, if A is a noetherian ring, then it is trivial to check that both A/I and $S^{-1}A$ are noetherian, for any ideal I of A and any m. c. subset S of A; moreover, the following basic result implies, using induction, that $A[X_1, \dots, X_n]$ is also noetherian.

Theorem 2.5 (Hilbert Basis Theorem). *If A is a noetherian ring, then so is $A[X]$.*

Proof. Let I be any ideal of $A[X]$. For $0 \neq f \in I$, let $\mathrm{LC}(f)$ denote the leading coefficient of f, and $J = \{0\} \cup \{LC(f) : f \in I,\ f \neq 0\}$. Then J is an ideal of A and so we can find $f_1, \dots, f_r \in I \setminus \{0\}$ such that $J = (\mathrm{LC}(f_1), \dots, \mathrm{LC}(f_r))$. Let $d = \max\{\deg f_i : 1 \leq i \leq r\}$. For $0 \leq i < d$, let $J_i = \{0\} \cup \{LC(f) : f \in I,\ \deg f = i\}$; then J_i is an ideal of A and so we can find $f_{i1}, \dots, f_{ir_i} \in I$ such that $J_i = (\mathrm{LC}(f_{i1}), \dots, \mathrm{LC}(f_{ir_i}))$. Now if I' is the ideal of $A[X]$ generated by $\{f_1, \dots, f_r\} \cup \{f_{ij} : 0 \leq i < d,\ 1 \leq j \leq r_i\}$, then $I' \subseteq I$ and for any $0 \neq f \in I$, there is $f' \in I'$ such that $\deg(f - f') < \deg f$. Thus an inductive argument yields $I = I'$. □

A field as well as a PID (e.g., $\mathbb{Z}$, the ring of integers) is clearly noetherian, and constructing from these, using combinations of the three fundamental processes, we obtain a rather inexhaustible source of examples of noetherian rings. Especially important among these are finitely generated algebras over a field or, more generally, over a noetherian ring. Let us recall the relevant definitions.

Definition 2.6. Let B be a ring and A be a subring of B. Given any $b_1, \dots, b_n \in B$, we denote by $A[b_1, \dots, b_n]$ the smallest subring of B containing A and the elements $b_1, \dots, b_n$. This subring consists of all polynomial expressions $f(b_1, \dots, b_n)$ as f varies over $A[X_1, \dots, X_n]$. We say that B is a *finitely generated* (f. g.) *A–algebra* or an *A–algebra of finite type* if there exist $b_1, \dots, b_n \in B$ such that $B = A[b_1, \dots, b_n]$. Finitely generated k–algebras, where k is a field, are sometimes called *affine rings*.

A *module* over a ring A or an A–module is simply a vector space except that the scalars come from the ring A instead of a field. Some examples of A–modules are: ideals I of A, quotient rings A/I, localizations $S^{-1}A$, and f. g. A–algebras $A[x_1, \ldots, x_n]$. The notions of submodules, quotient modules, direct sums of modules and isomorphism of modules are defined in an obvious fashion. The concept of localization (w.r.t. m. c. subsets of A) also carries to A–modules, and an analogue of the property in Exercise 2.1 can be verified easily. Direct sum of (isomorphic) copies of A is called a free A–module; $A^n = \underbrace{A \oplus \cdots \oplus A}_{n \text{ times}}$ is referred to as the free A–module of rank n.

Let M be an A–module. Given submodules $\{M_i\}$ of M, their sum

$$\sum M_i = \{\sum x_i : x_i \in M_i \text{ and all except finitely many } x_i\text{'s are } 0\}$$

and their intersection $\cap M_i$ are also submodules of M. Products of submodules doesn't make sense but the colon operation has an interesting and important counterpart. If M_1, M_2 are submodules of M, we define $(M_1 : M_2)$ to be the ideal $\{a \in A : aM_2 \subseteq M_1\}$ of A. The ideal $(0 : M)$ is called the *annihilator* of M and is denoted by $\mathrm{Ann}(M)$; for $x \in M$, we may write $\mathrm{Ann}(x)$ for the ideal $(0 : x)$, i.e., for $\mathrm{Ann}(Ax)$. Note that if I is an ideal of A, then $\mathrm{Ann}(A/I) = I$ and if $\mathrm{Ann}(M) \supseteq I$, then M may be regarded as an A/I–module. Let us also note that for any submodules M_1, M_2 of M, we always have the isomorphisms $(M_1 + M_2)/M_2 \simeq M_1/(M_1 \cap M_2)$, and, if $M_2 \subseteq M_1$ and N is a submodule of M_2, $(M_1/N)/(M_2/N) \simeq M_1/M_2$.

We say that M is *finitely generated* (f. g.) or that M is a *finite A–module* if there exist $x_1, \ldots, x_n \in M$ such that $M = Ax_1 + \cdots + Ax_n$. Note that in this case M is isomorphic to a quotient of A^n. We can, analogously, consider the a.c.c. for submodules of M, and in the case it is satisfied, we call M to be *noetherian*. Artinian modules are defined similarly. Observe that M is noetherian iff every submodule of M is finitely generated. In general, if M is f. g., then a submodule of M needn't be f. g., i.e., M needn't be noetherian. However, the following basic result assures that 'most' f. g. modules are noetherian.

Lemma 2.7. *Finitely generated modules over noetherian rings are noetherian.*

Proof (Sketch). First note that given a submodule N of M, we have that M is noetherian iff both N and M/N are noetherian. Use this and induction to show that if A is noetherian, then so is A^n, and, hence, any of its quotient modules. □

Another basic fact about modules is the following.

Lemma 2.8 (Nakayama's Lemma). *Let M be a* f. g. *A–module and I be an ideal of A such that $IM = M$. Then there exists $a \in I$ such that $(1 - a)M = 0$. In particular, if $I \neq A$ and A is a domain or a local ring, then $M = 0$.*

Proof. Write $M = Ax_1 + \cdots + Ax_n$. Then $x_i = \sum_{j=1}^{n} a_{ij}x_j$, for some $a_{ij} \in I$. Let $d = \det(\delta_{ij} - a_{ij})$. Then $d = 1 - a$, for some $a \in I$, and, by Cramer's rule, $dx_j = 0$ for all j. □

Remark 2.9. The 'determinant trick' in the above proof shows more generally that if M and I are as in (3.2) above and $\phi : M \to M$ is an A–linear map such that $\phi(M) \subseteq IM$, then there exist $a_1, \ldots, a_n \in I$ such that $\phi^n + a_1\phi^{n-1} + \cdots + a_n = 0$. Thus Nakayama's Lemma may be considered as an analogue of Cayley–Hamilton Theorem of Linear Algebra.

2.3 Integral Extensions

The theory of algebraic field extensions has a useful analogue to ring extensions, which is discussed in this section.

Let B be a ring and A be a subring of B. We may express this by saying that B is a (ring) extension of A or that B is an overring of A.

Definition 2.10. An element $x \in B$ is said to be *integral* over A if it satisfies a monic polynomial with coefficients in A, i.e., $x^n + a_1 x^{n-1} + \cdots + a_n = 0$ for some $a_1, \ldots, a_n \in A$. If every element of B is integral over A, then we say that B is an *integral extension* of A or that B is *integral* over A.

Evidently, if $x \in B$ satisfies an integral equation such as above, then $1, x, x^2, \ldots, x^{n-1}$ generate $A[x]$ as an A–module. And if B' is a subring of B containing $A[x]$ such that $B' = Ax_1 + \cdots + Ax_n$, then for any $b \in B'$, $bx_i = \sum a_{ij} x_j$ for some $a_{ij} \in A$ so that b satisfies the monic polynomial $\det(X\delta_{ij} - a_{ij}) \in A[X]$. Thus we obtain the following criteria.

$$\begin{aligned} x \in B \text{ is integral over } A &\Leftrightarrow A[x] \text{ is a finite } A\text{–module} \\ &\Leftrightarrow \text{a subring } B' \text{ of } B \text{ containing } A[x] \text{ is a finite } A\text{–module.} \end{aligned}$$

In particular, if B is a finite A–module, then B is integral over A. The converse is true if we further assume (the necessary condition) that B is a f. g. A–algebra. This follows by observing that the above criteria implies, using induction, that if $x_1, \ldots, x_n \in B$ are integral over A, then $A[x_1, \ldots, x_n]$ is a finite A–module. This observation also shows that the elements of B which are integral over A form a subring, say C, of B. If $C = B$, we say that A is *integrally closed* in B. A domain is called *integrally closed* or *normal* if it is integrally closed in its quotient field. Note that if S is a m. c. subset of A, B is integral over A, and J is an ideal of B, then $S^{-1}B$ (resp: B/J) is integral over $S^{-1}A$ (resp: $A/J \cap A$); moreover, if A is a normal domain and $0 \notin S$, then $S^{-1}A$ is also a normal domain.

Exercise 2.11. Show that a UFD is normal. Also show that if A is a domain, then A is normal iff $A[X]$ is normal. Further, show that if A is a normal domain, K is its quotient field, and x is an element of a field extension L of K, then x is integral over A implies that the minimal polynomial of x over K has its coefficients in A.

Example 2.12. Let $B = k[X, Y]/(Y - X^2)$, and let x, y denote the images of X, Y in B so that $B = k[x, y]$. Let $A = k[y]$. Then x is integral over A, and hence B is integral over A. On the other hand, if $B = k[X, Y]/(XY - 1) = k[x, y]$, then x is not integral over $A = k[y]$. It may be instructive to note, indirectly, that $B \simeq k[Y, 1/Y]$ is not a finite $k[Y]$–module. These examples correspond, roughly, to the fact that the projection of parabola along the x–axis onto the y–axis is a 'finite' map in the sense that the inverse image of every point is at 'finite distance', whereas in the case of hyperbola, this isn't so. Similar examples in "higher dimensions" can be constructed by considering projections of surfaces onto planes, solids onto 3–space, and so on. Examples of integral (resp: non–integral) extensions of $\mathbb{Z}$ are given by subrings B of number fields (viz., subfields of $\mathbb{C}$ of finite degree over $\mathbb{Q}$) such that $B \subseteq \mathcal{O}_K$ (resp: $B \not\subseteq \mathcal{O}_K$), where $\mathcal{O}_K$ denotes the ring of integers in K. Indeed, $\mathcal{O}_K$ is nothing but the integral closure of $\mathbb{Z}$ in K.

A precise definition of dimension for arbitrary rings can be given as follows.

Definition 2.13. The *(Krull) dimension* of a ring A is defined as

$$\dim A = \max\{n : \exists \text{ distinct primes } \mathfrak{p}_0, \mathfrak{p}_1, \ldots, \mathfrak{p}_n \text{ of } A \text{ such that } \mathfrak{p}_0 \subset \mathfrak{p}_1 \subset \cdots \subset \mathfrak{p}_n\}.$$

Remark 2.14. Observe that a field has dimension 0. A PID which is not a field, in particular $\mathbb{Z}$ as well as $k[X]$, is clearly of dimension 1. It can be proved that $\dim k[X_1, \ldots, X_n] = n$. For more on this topic, see [1].

Some of the basic results about integral extensions are as follows. In the five results given below, B denotes an integral extension of A and $\mathfrak{p}$ denotes a prime ideal of A.

Theorem 2.15. *A is a field if and only if B is a field. Also, if $\mathfrak{q}$ is a prime ideal of B such that $\mathfrak{q} \cap A = \mathfrak{p}$, then $\mathfrak{p}$ is maximal iff $\mathfrak{q}$ is maximal. Moreover, if $\mathfrak{q}'$ is any prime ideal of B such that $\mathfrak{q} \subset \mathfrak{q}'$ and $\mathfrak{q}' \cap A = \mathfrak{p}$, then $\mathfrak{q} = \mathfrak{q}'$.*

Corollary 2.16. $\dim B \leq \dim A$. *In particular, if B is a domain and* $\dim A \leq 1$, *then* $\dim A = \dim B$.

Theorem 2.17 (Lying Over Theorem). *There exists a prime ideal $\mathfrak{q}$ of B such that $\mathfrak{q} \cap A = \mathfrak{p}$. In particular, $\mathfrak{p}B \cap A = \mathfrak{p}$.*

Theorem 2.18 (Going Up Theorem). *If $\mathfrak{q}$ is a prime ideal of B such that $\mathfrak{q} \cap A = \mathfrak{p}$, and $\mathfrak{p}'$ is a prime ideal of A such that $\mathfrak{p} \subseteq \mathfrak{p}'$, then there exists a prime ideal $\mathfrak{q}'$ of B such that $\mathfrak{q} \subseteq \mathfrak{q}'$ and $\mathfrak{q}' \cap A = \mathfrak{p}$.*

Corollary 2.19. $\dim A = \dim B$.

Proofs (Sketch). Easy manipulations with integral equations of relevant elements proves the first assertion of Theorem 2.15; the second and third assertions follow from the first one by passing to quotient rings and localizations respectively. To prove Theorem 2.17, consider $A' = A_{\mathfrak{p}}$ and $B' = S^{-1}B$ where $S = A \setminus \mathfrak{p}$. Then B' is an integral extension of A' and if $\mathfrak{q}'$ is any maximal ideal of B', then $q' \cap A'$ is necessarily maximal and thus $\mathfrak{q}' \cap A' = \mathfrak{p}A'$. Now $\mathfrak{q} = \mathfrak{q}' \cap B$ lies over $\mathfrak{p}$, and thus Theorem 2.17 is proved. Theorem 2.18 follows by applying Theorem 2.17 to appropriate quotient rings. □

Exercise 2.20. Prove the two corollaries above using the results preceding them.

Remark 2.21. It may be noted that Corollary 2.19 is an analogue of the simple fact that if L/K is an algebraic extension of fields containing a common subfield k, then $\text{tr.deg.}_k L = \text{tr.deg.}_k K$. Recall that if K is a ring containing a field k, then elements $\theta_1, \ldots, \theta_d$ of K are said to be *algebraically independent* over k if they do not satisfy any algebraic relation over k, i.e., $f(\theta_1, \ldots, \theta_d) \neq 0$ for any $0 \neq f \in k[X_1, \ldots, X_n]$. A subset of K is *algebraically independent* if every finite collection of elements in it are algebraically independent. If K is a field then any two maximal algebraically independent subsets have the same cardinality, called the *transcendence degree* of K/k and denoted by $\text{tr.deg.}_k K$; such subsets are then called *transcendence bases* of K/k; note that an algebraically independent subset S is a transcendence basis of K/k iff K is algebraic over $k(S)$, the smallest subfield of K containing k and S. If B is a domain containing k and K is its quotient field, then one sets $\text{tr.deg.}_k B = \text{tr.deg.}_k K$. Finally, note that $k[X_1, \ldots, X_n]$ and its quotient field $k(X_1, \ldots, X_n)$ are clearly of transcendence degree n over k. A good reference for this material is [20, Ch. 2].

2.4 Discriminant of a Number Field

In this section, we shall first discuss some basic properties of normal domains. A key result here is the so called Finiteness Theorem. This will lead to the notion of an integral basis and the notion of absolute discriminant of a number field.

Proposition 2.22. *Let A be a domain with K as its quotient field. Then we have the following.*

(i) If an element α (in some extension L of K) is algebraic over K, then there exists $c \in A$ such that $c \neq 0$ and $c\alpha$ is integral over A. Consequently, if $\{\alpha_1, \ldots, \alpha_n\}$ is a K–basis of L, then there exists $d \in A$ such that $d \neq 0$ and $\{d\alpha_1, \ldots, d\alpha_n\}$ is a K–basis of L whose elements are integral over A.

(ii) If A is normal, and $f(X)$, $g(X)$ are monic polynomials in $K[X]$ such that $f(X)g(X) \in A[X]$, then both $f(X)$ and $g(X)$ are in $A[X]$.

(iii) If A is normal, L/K is a finite separable extension and $\alpha \in L$ is integral over A, then the coefficients of the minimal polynomial of α over K as well as the field polynomial of α w.r.t. L/K are in A. In particular, $\mathrm{Tr}_{L/K}(\alpha) \in A$ and $N_{L/K}(\alpha) \in A$, and moreover, if $\{\alpha_1, \ldots, a_n\}$ is a K–basis of L consisting of elements which are integral over A, then $D_{L/K}(\alpha_1, \ldots, \alpha_n) \in A$.

Proof. (i) If α satisfies the monic polynomial $X^n + a_1X^{n-1} + \cdots + a_n \in K[X]$, then we can find a common denominator $c \in A$ such that $c \neq 0$ and $a_i = \frac{c_i}{c}$ for some $c_i \in A$. Multiplying the above polynomial by c^n, we get a monic polynomial in $A[X]$ satisfied by $c\alpha$.
(ii) The roots of $f(X)$ as well as $g(X)$ (in some extension of K) are integral over A because they satisfy the monic polynomial $f(X)g(X) \in A[X]$. Now the coefficients of $f(X)$ as well as $g(X)$ are the elementary symmetric functions of their roots (up to a sign), and therefore these are also integral over A. But the coefficients are in K. It follows that both $f(X)$ and $g(X)$ are in $A[X]$.
(iii) If α is integral over A, then clearly so is every conjugate of α w.r.t. L/K. Now an argument similar to that in (ii) above shows that the coefficients of $\mathrm{Irr}(\alpha, K)$ as well as the field polynomial of α w.r.t. L/K are in A. □

It may be observed that a proof of the FACT in Section 1.2 follows from (ii) above. We are now ready to prove the following important result.

Theorem 2.23 (Finiteness Theorem). *Let A be a normal domain with quotient field K. Assume that L/K is a finite separable extension of degree n. Let B be the integral closure of A in L. Then B is contained in a free A–module generated by n elements. In particular, if A is also assumed to be noetherian, then B is a finite A–module and a noetherian ring.*

Proof. In view of (i) in the Proposition above, we can find a K–basis $\{\alpha_1, \ldots, \alpha_n\}$ of L, which is contained in B. Let $\{\beta_1, \ldots, \beta_n\}$ be a dual basis, w.r.t. the nondegenerate bilinear form $\mathrm{Tr}_{L/K}(xy)$, corresponding to $\{\alpha_1, \ldots, \alpha_n\}$. Let $x \in B$. Then $x = \sum_j b_j\beta_j$ for some $b_j \in K$. Now $\mathrm{Tr}(\alpha_i x) = \sum_j b_j \mathrm{Tr}(\alpha_i\beta_j) = b_i$. Moreover, since $\alpha_i x$ is integral over A, it follows from the Proposition above that $b_i \in A$. Thus B is contained in the A–module generated by $\beta_1, \ldots, \beta_n$. This module is free since $\beta_1, \ldots, \beta_n$ are linearly independent over K. □

When A is a PID, or better still, when $A = \mathbb{Z}$, the conclusion of Finiteness Theorem can be sharpened using the following lemma.

Lemma 2.24. *Let A be a PID, M be an A–module generated by n elements $x_1, \ldots, x_n$, and let N be a submodule of M.*

(i) N is generated by at most n elements. In fact, we can find $a_{ij} \in A$ for $1 \leq i \leq j \leq n$ such that

$$N = Ay_1 + \cdots + Ay_n \quad \text{where} \quad y_i = \sum_{j \geq i} a_{ij} x_j \text{ for } 1 \leq i \leq n. \tag{2.1}$$

(ii) Assume that $A = \mathbb{Z}$ and M is a $\mathbb{Z}$-submodule of K, where K is a number field with $[K : \mathbb{Q}] = n$. Further assume that N contains a $\mathbb{Q}$-basis of K. Then M/N is finite and we can choose $a_{ij} \in A$, for $1 \leq i \leq j \leq n$, satisfying (2.1) and with the additional property

$$a_{ii} > 0 \text{ for } 1 \leq i \leq n \quad \text{and} \quad |M/N| = a_{11} a_{22} \cdots a_{nn} = \det(a_{ij}) \tag{2.2}$$

where, by convention, $a_{ij} = 0$ for $j < i$.

Proof. (i) We have $M = Ax_1 + \cdots + Ax_n$. Let us use induction on n. Let

$$I = \{a \in A : ax_1 + a_2 x_2 + \cdots + a_n x_n \in N \text{ for some } a_2, \ldots, a_n \in A\}.$$

Then I is an ideal of A and thus $I = (a_{11})$ for some $a_{11} \in A$. Also, there exist $a_{12}, \ldots, a_{1n} \in A$ such that $y_1 \in N$ where $y_1 = a_{11}x_1 + a_{12}x_2 + \cdots + a_{1n}x_n$. If $n = 1$, we have $N = Ix_1 = Ay_1$, where $y_1 = a_{11}x_1$ and thus the result is proved in this case. If $n > 1$, then let $M_1 = Ax_2 + \ldots Ax_n$ and $N_1 = N \cap M_1$. By induction hypothesis, we can find $a_{ij} \in A$ for $2 \leq i \leq j \leq n$ such that

$$N_1 = Ay_2 + \cdots + Ay_n \quad \text{where} \quad y_i = \sum_{j \geq i} a_{ij} x_j \text{ for } 2 \leq i \leq n.$$

Now if $y \in N$, then $y = a_1 x_1 + a_2 x_2 + \cdots + a_n x_n$ for some $a_1, \ldots, a_n \in A$. Moreover $a_1 \in I$ and thus $a_1 = \lambda_1 a_{11}$ for some $\lambda_1 \in A$. Hence $y - \lambda_1 y_1 \in N_1$ and so $y - \lambda_1 y_1 = \lambda_2 y_2 + \cdots + \lambda_n y_n$ for some $\lambda_2, \ldots, \lambda_n \in A$. It follows that $N = Ay_1 + \cdots + Ay_n$ and $y_i = \sum_{j \geq i} a_{ij} x_j$, as desired.

(ii) To begin with, let $a_{ij} \in A = \mathbb{Z}$ and $y_i \in N$ be such that (2.1) holds. If N contains a $\mathbb{Q}$-basis of K, then it is clear that $K = \mathbb{Q}y_1 + \cdots + \mathbb{Q}y_n$ and hence $y_1, \ldots, y_n$ are linearly independent over $\mathbb{Q}$. Now, if some $a_{ii} = 0$, then we see easily that y_i is a $\mathbb{Q}$-linear combination of $y_{i+1}, \ldots, y_n$, which is a contradiction. Thus, $a_{ii} \neq 0$ for $1 \leq i \leq n$ and so replacing some y_i's by $-y_i$'s, if necessary, we can assume that $a_{ii} > 0$ for $1 \leq i \leq n$.

Given any $x \in M$, write $x = a_1 x_1 + \cdots + a_n x_n$, where $a_1, \ldots, a_n \in \mathbb{Z}$. We can find unique integers q_1 and r_1 such that $a_1 = a_{11} q_1 + r_1$ and $0 \leq r_1 < a_{11}$. Hence

$$x - q_1 y_1 = r_1 x_1 + b_2 x_2 + \cdots + b_n x_n \quad \text{for some } b_2, \ldots, b_n \in \mathbb{Z}.$$

Next, let $q_2, r_2 \in \mathbb{Z}$ be such that $b_2 = a_{22} q_2 + r_2$ and $0 \leq r_2 < a_{22}$. Hence

$$x - q_1 y_1 - q_2 y_2 = r_1 x_1 + r_2 x_2 + c_3 x_3 + \cdots + b_n x_n \quad \text{for some } c_3, \ldots, c_n \in \mathbb{Z}.$$

Continuing in this way, we obtain $q_1, \ldots, q_n \in \mathbb{Z}$ and $r_1, \ldots, r_n \in \mathbb{Z}$ such that

$$x - (q_1 y_1 + \cdots + q_n y_n) = r_1 x_1 + \cdots + r_n x_n \quad \text{with } 0 \leq r_i < a_{ii}.$$

Thus $r_1 x_1 + \cdots + r_n x_n$ is a representative of x in M/N. Moreover, this representative is unique because the difference of two such representatives will be an element of N of the form $s_1 x_1 + \cdots + s_n x_n$, where $s_i \in \mathbb{Z}$ with $|s_i| < a_{ii}$, and from (2.1), one sees easily that if s_j is the first nonzero integer among $s_1, \ldots, s_n$, then a_{jj} divides s_j, which is a contradiction. It follows that the elements of M/N are in bijection with n-tuples $(r_1, \ldots, r_n)$ of integers with $0 \leq r_i < a_{ii}$. Consequently, $|M/N| = a_{11} a_{22} \cdots a_{nn}$. □

Corollary 2.25. *Let A, K, L, n, B be as in the Finiteness Theorem. Assume that A is a PID. Then B is a free A–module of rank n, i.e., there exist n linearly independent elements $y_1, \ldots, y_n \in B$ such that $B = Ay_1 + \cdots + Ay_n$.*

Proof. Follows from Finiteness Theorem 2.23 and Lemma 2.24 (i). □

The above Corollary applied in the particular case of $A = \mathbb{Z}$, shows that the ring of integers of a number field always has a $\mathbb{Z}$–basis. Such a basis is called an *integral basis* of that ring or of the corresponding number field.

In general, suppose K is a number field with $[K : \mathbb{Q}] = n$, and N is a $\mathbb{Z}$-submodule of $M = \mathcal{O}_K$ such that N contains a $\mathbb{Q}$-basis of K. Then by Lemma 2.24 (ii), we see that N has a $\mathbb{Z}$-basis of n elements, and we call this an *integral basis* of N. Notice that if $\{\alpha_1, \ldots, \alpha_n\}$ is an integral basis of $N \subseteq \mathcal{O}_K$, then by Proposition 2.22 (iii), $D_{L/K}(\alpha_1, \ldots, \alpha_n)$ is an integer. Further, if $\{u_1, \ldots, u_n\}$ is any $\mathbb{Q}$–basis of K contained in N, then $u_i = \sum_j a_{ij} \alpha_j$ for some $n \times n$ nonsingular matrix (a_{ij}) with entries in $\mathbb{Z}$. If $d = \det(a_{ij})$, then $d \in \mathbb{Z}$ and we have $D_{L/K}(u_1, \ldots, u_n) = d^2 D_{L/K}(\alpha_1, \ldots, \alpha_n)$. If $\{u_1, \ldots, u_n\}$ is also an integral basis of N, then clearly $d = \pm 1$. It follows that any two integral bases of N have the same discriminant, and among all bases of K contained in N, the discriminant of an integral basis has the least absolute value. We denote the discriminant of an integral basis of N by $\Delta(N)$ and call this the *(absolute) discriminant* of N. In case $N = \mathcal{O}_K$, the discriminant $\Delta(\mathcal{O}_K)$ is denoted by d_K and called the *(absolute) discriminant* of K. The two discriminants $\Delta(N)$ and $d_K = \Delta(\mathcal{O}_K)$ are related by the formula

$$\Delta(N) = |\mathcal{O}_K / N|^2 d_K \tag{2.3}$$

which is an immediate consequence of Lemmas 1.9 and 2.24 (ii) where in the latter we take $x_1, \ldots, x_n$ to be an integral basis of K.

There are two cases when the formula (2.3) is particularly useful. One is when $K = \mathbb{Q}(\alpha)$ is generated by a single element α which is integral over $\mathbb{Z}$ and $N = \mathbb{Z}[\alpha]$. In this case, if we know that $\Delta(\mathbb{Z}[\alpha]) = D_{K/\mathbb{Q}}(1, \alpha, \ldots, \alpha^{n-1})$ is squarefree, then we can conclude from (2.3) that $\mathcal{O}_K = \mathbb{Z}[\alpha]$. Another case is when N is a nonzero ideal I of $\mathcal{O}_K$. Note that $I \neq 0$ implies that $I \cap \mathbb{Z} \neq 0$ since A is integral over $\mathbb{Z}$; now, if m is a nonzero integer in $I \cap \mathbb{Z}$ and $\{\alpha_1, \ldots, \alpha_n\}$ is a $\mathbb{Q}$-basis of K contained in $\mathcal{O}_K$, then $\{m\alpha_1, \ldots, m\alpha_n\}$ is a $\mathbb{Q}$-basis of K contained in I. Thus I does satisfy the hypothesis for the existence of an integral basis and for the formula (2.3) to hold with $N = I$. This case will be taken up again in Chapter 4.

Remark 2.26. An alternative proof of the existence of an integral basis of K can be given by picking a $\mathbb{Q}$–basis of K contained in $\mathcal{O}_K$ whose discriminant has the least possible absolute value, and showing that this has to be an integral basis. Try this! Or see Appendix B for a proof along these lines.

We now discuss two examples to illustrate the computation of discriminant and determination of integral bases.

Example 1: Quadratic Fields.

Let K be a quadratic field and $\mathcal{O}$ be its ring of integers. As noted before, we have $K = \mathbb{Q}(\sqrt{m})$, where m is a squarefree integer. We now attempt to give a more concrete description of $\mathcal{O}$. First, note that $\mathbb{Z}[\sqrt{m}] = \{r + s\sqrt{m} : r, s \in \mathbb{Z}\} \subseteq \mathcal{O}$. Let $x = a + b\sqrt{m} \in \mathcal{O}$ for some $a, b \in \mathbb{Q}$. Then $\mathrm{Tr}(x) = 2a$ and $N(x) = a^2 - mb^2$ (verify!) and both of them must be in $\mathbb{Z}$. Since m is squarefree and $a^2 - mb^2 \in \mathbb{Z}$, we see that $a \in \mathbb{Z}$ if and only if $b \in \mathbb{Z}$. Thus if $a \notin \mathbb{Z}$, then we can find an odd integer a_1 such that $2a = a_1$, and relatively prime integers b_1 and c_1 with $c_1 > 1$ such that $b = \frac{b_1}{c_1}$. Now

$$\left(a_1 = 2a \in \mathbb{Z} \text{ and } a^2 - mb^2 \in \mathbb{Z}\right) \Rightarrow \left(4 | c_1^2 a_1^2 \text{ and } c_1^2 | 4mb_1^2\right) \Rightarrow c_1 = 2.$$

Hence b_1 is odd and $a_1^2 - mb_1^2 \equiv 0 (\mathrm{mod}\ 4)$. Also a_1 is odd, and therefore, $m \equiv 1 (\mathrm{mod}\ 4)$. It follows that if $m \not\equiv 1 (\mathrm{mod}\ 4)$, then $a, b \in \mathbb{Z}$, and so in this case, $\mathcal{O} = \{a + b\sqrt{m} : a, b \in \mathbb{Z}\}$ and $\{1, \sqrt{m}\}$ is an integral basis. In the case $m \equiv 1 (\mathrm{mod}\ 4)$, the preceding observations imply that

$$\mathcal{O} \subseteq \left\{ \frac{a_1 + b_1\sqrt{m}}{2} : a_1, b_1 \text{ are integers having the same parity, i.e., } a_1 \equiv b_1 (\mathrm{mod}\ 2) \right\}$$

and, moreover, $\frac{1+\sqrt{m}}{2} \in \mathcal{O}$ since it is a root of $X^2 - X - \frac{m-1}{4}$; therefore $\mathcal{O} = \mathbb{Z}[\frac{1+\sqrt{m}}{2}]$ and $\{1, \frac{1+\sqrt{m}}{2}\}$ is an integral basis. We can now compute the discriminant of K as follows.

$$d_K = \begin{cases} \det \begin{pmatrix} 2 & 0 \\ 0 & 2m \end{pmatrix} & = 4m \qquad \text{if } m \equiv 2, 3 (\mathrm{mod}\ 4) \\ \det \begin{pmatrix} 2 & 1 \\ 1 & (1+m)/2 \end{pmatrix} & = m \qquad \text{if } m \equiv 1 (\mathrm{mod}\ 4). \end{cases}$$

It may be remarked that the integer $d = d_K$ determines the quadratic field K completely, and the set $\{1, \frac{d+\sqrt{d}}{2}\}$ is always an integral basis of K. (Verify!)

Example 2: Cyclotomic Fields.

Let p be an odd prime and $\zeta = \zeta_p$ be a primitive p^{th} root of unity. Consider the cyclotomic field $K = \mathbb{Q}(\zeta)$. We know that $K/\mathbb{Q}$ is a Galois extension and its Galois group is isomorphic to $(\mathbb{Z}/p\mathbb{Z})^\times$, which is cyclic of order $p - 1$. The minimal polynomial of ζ over $\mathbb{Q}$ is given by

$$\Phi_p(X) = \frac{X^p - 1}{X - 1} = X^{p-1} + X^{p-2} + \cdots + X + 1 = \prod_{i=1}^{p-1} \left(X - \zeta^i\right).$$

We now try to determine $\mathcal{O}_K$, the ring of integers of K, and d_K, the discriminant of K. Let us first note that since $\zeta \in \mathcal{O}_K$, the ring $\mathbb{Z}[\zeta]$, which is generated as a $\mathbb{Z}$–module by $1, \zeta, \zeta^2, \ldots, \zeta^{p-1}$,

is clearly contained in $\mathcal{O}_K$. Moreover, we have

$$D_{K/\mathbb{Q}}(1,\zeta,\ldots,\zeta^{p-1}) = (-1)^{(p-1)(p-2)/2} N_{K/\mathbb{Q}}(\Phi_p'(\zeta)) = (-1)^{(p-1)/2} N_{K/\mathbb{Q}}\left(\frac{p\zeta^{p-1}}{(\zeta-1)}\right).$$

Since $\Phi_p(X)$ is the minimal polynomial of $K = \mathbb{Q}(\zeta)$ over $\mathbb{Q}$, we clearly see that $N_{K/\mathbb{Q}}(\zeta) = (-1)^{p-1} \cdot 1 = 1$. And since the minimal polynomial of $\zeta - 1$ is

$$\Phi_p(X+1) = \frac{(X+1)^p - 1}{X} = \sum_{i=1}^{p} \binom{p}{i} X^{i-1} = X^{p-1} + pX^{p-2} + \cdots + \binom{p}{2} X + p,$$

we see that $N(\zeta - 1) = (-1)^{p-1} p = p$. Thus $N(\Phi_p'(\zeta)) = \frac{p^{p-1} \cdot 1}{p} = p^{p-2}$. On the other hand, $N(\zeta - 1)$ is the product of its conjugates, and so we obtain the identity

$$p = (\zeta - 1)(\zeta^2 - 1)\ldots(\zeta^{p-1} - 1),$$

which implies that the ideal $(\zeta - 1)\mathcal{O}_K \cap \mathbb{Z}$ contains $p\mathbb{Z}$. But $(\zeta - 1)$ is not a unit in $\mathcal{O}_K$ (lest every conjugate $(\zeta^i - 1)$ would be a unit and hence p would be a unit in $\mathbb{Z}$). So it follows that $(\zeta - 1)\mathcal{O}_K \cap \mathbb{Z} = p\mathbb{Z}$. Now suppose $x \in \mathcal{O}_K$. Then $x = c_0 + c_1\zeta + \cdots + c_{p-1}\zeta^{p-1}$ for some $c_i \in \mathbb{Q}$. We shall now show that c_i are, in fact, in $\mathbb{Z}$. To this effect, consider $(\zeta - 1)x = c_0(\zeta - 1) + c_1(\zeta^2 - \zeta) + \cdots + c_{p-1}(\zeta^p - \zeta^{p-1})$. We have $\mathrm{Tr}(\zeta - 1) = -p$ and $\mathrm{Tr}(\zeta^{i+1} - \zeta^i) = 1 - 1 = 0$ for $1 \leq i < p$. Therefore $c_0 p = -\mathrm{Tr}((\zeta - 1)x) \in (\zeta - 1)\mathcal{O}_K \cap \mathbb{Z} = p\mathbb{Z}$, and so $c_0 \in \mathbb{Z}$. Next, $\zeta^{-1}(x - c_0) = \zeta^{p-1}c_0$ is an element of $\mathcal{O}_K$ which equals $c_1 + c_2\zeta + \cdots + c_{p-1}\zeta^{p-2}$. Using the previous argument, we find that $c_1 \in \mathbb{Z}$. Continuing in this way, we see that $c_i \in \mathbb{Z}$ for $0 \leq i \leq p-1$. It follows that $\mathcal{O}_K = \mathbb{Z}[\zeta]$ and $\{1, \zeta, \zeta^2, \ldots, \zeta^{p-1}\}$ is an integral basis of $\mathcal{O}_K$. As a consequence, we obtain that

$$d_K = D_{K/\mathbb{Q}}(1, \zeta, \zeta^2, \ldots, \zeta^{p-1}) = (-1)^{(p-1)/2} p^{p-2}.$$

Exercise 2.27. Let $n = p^e$ where p is a prime and e is a positive integer. Show that the ring of integers of $\mathbb{Q}(\zeta_n)$ is $\mathbb{Z}[\zeta_n]$ and the discriminant of $\mathbb{Q}(\zeta_n)$ is equal to $(-1)^{\varphi(p)/2} p^{p^{e-1}(pe-e-1)}$. Deduce that, in particular, the only prime dividing this discriminant is p and that the sign of this discriminant is negative only if $n = 4$ or $p \equiv 3 (\mathrm{mod}\ 4)$.

Remark 2.28. If n is any integer > 1 and $\zeta = \zeta_n$ is a primitive n^{th} root of unity, then it can be shown that the ring of integers of $\mathbb{Q}(\zeta_n)$ is $\mathbb{Z}[\zeta_n]$ and the discriminant of $\mathbb{Q}(\zeta_n)$ equals

$$(-1)^{\varphi(n)/2} \frac{n^{\varphi(n)}}{\prod_{p|n} p^{\varphi(n)/(p-1)}}.$$

The proof is somewhat difficult. Interested reader may see [19].

Exercise 2.29 (Stickelberger's Theorem). If K is a number field, then $d_K \equiv 0$ or $1 (\mathrm{mod}\ 4)$. [Hint: Let $\{u_1, \ldots, u_n\}$ be an integral basis of K so that $d_K = \left[\det\left(u_i^{(j)}\right)\right]^2$, where $u_i^{(1)}, \ldots, u_i^{(n)}$ denote the conjugates of u_i w.r.t. $K/\mathbb{Q}$. Write the above determinant as $P - N$, where P and N denote the contribution from even and odd permutations, respectively. Show that $P + N$ and PN are integers and $d_K = (P+N)^2 - 4PN$.] Verify this congruence from the formulae above when K is a quadratic field or a cyclotomic field,

Exercise 2.30. Let $K = \mathbb{Q}(\alpha)$ where α is a root of $X^3 + 2X + 1$. Show that $\Delta(\mathbb{Z}[\alpha]) = -59$. Deduce that $\{1, \alpha, \alpha^2\}$ is an integral basis of K.

Chapter 3

Dedekind Domains and Ramification Theory

In the investigation of Fermat's Last Theorem and Higher Reciprocity Laws, mathematicians in the 19th century were led to ask if the unique factorization property enjoyed by the integers also holds in the ring of integers in an algebraic number field, especially in the ring of cyclotomic integers. In 1844, E. Kummer showed that this does not hold, in general. About three years later, he showed that the unique factorization in such rings, or at least in rings of cyclotomic integers, is possible if numbers are replaced by the so called "ideal numbers". Kummer's work was simplified and furthered by R. Dedekind[1]. The concept of an ideal in a ring was thus born. In effect, Dedekind showed that the ring of integers of an algebraic number field has the following property:

Every nonzero ideal in this ring factors uniquely as a product of prime ideals.

Integral domains with this property are now known as *Dedekind domains* (or also *Dedekind rings*)[2]. In a famous paper[3], Emmy Noether gave a set of abstract axioms for rings whose ideal theory agrees with that of ring of integers of an algebraic number field. This leads to a characterization of Dedekind domains. In the next section, we will take this abstract characterization as the definition of a Dedekind domain, and then prove properties such as

[1] Dedekind published his ideas as a supplement to Dirichlet's lectures on Number Theory, which were first published in 1863. Dedekind's supplements occur in the third and fourth editions, published in 1879 and 1894, of Dirichlet's *Vorlesungen über Zahlentheorie*. Another approach towards understanding and extending the ideas of Kummer was developed by L. Kronecker, whose work was apparently completed in 1859 but was not published until 1882. For more historical details, see the article "The Genesis of Ideal Theory" by H. Edwards, published in Archives for History of Exact Sciences, Vol. 23 (1980), and the articles by P. Ribenboim and H. Edwards in "Number Theory Related to Fermat's Last Theorem", Birkhäuser, 1982.

[2] The term *Dedekind domains* was coined by I.S. Cohen [Duke Math. J. **17** (1950), pp. 27–42]. In fact, Cohen defines a Dedekind domain to be an integral domain in which every nonzero proper ideals factors as a product of prime ideals, and he notes that the uniqueness of factorization is automatic, thanks to the work of Matusita [Japan J. Math. **19** (1944), pp. 97–110].

[3] *Abstrakter Aufbau der Idealtheorie in algebraischen Zahlund Funktionenkörpern*, Math. Ann. **96** (1927), pp. 26–61. The *Aufbau* paper followed another famous paper *Idealtheorie in Ringbereichen* [Math. Ann. **83** (1921), pp. 24–66] in which rings with ascending chain condition on ideals are studied; the term *noetherian rings* for such rings was apparently originated by Chevalley [Ann. Math. **44** (1943), pp. 690–708]. Incidentally, Emmy Noether had a great appreciation of Dedekind's work and her favorite expression to her students was *Alles steht schon bei Dedekind*!

the unique factorization of ideals as a consequence. In the subsequent sections, we study the phenomenon of ramification and discuss a number of basic results concerning it.

3.1 Dedekind Domains

An integral domain A is called a *Dedekind domain* if A is noetherian, normal and every nonzero prime ideal in A is maximal. Note that the last condition is equivalent to saying that $\dim A \leq 1$, or in other words, either A is a field or A is one dimensional.

Example 3.1. Any PID is a Dedekind domain (check!). In particular, $\mathbb{Z}$ and the polynomial ring $k[X]$ over a field k are Dedekind domains.

Example 3.2. The ring $\mathbb{Z}[\sqrt{-5}]$, which is the ring of integers of the quadratic field $\mathbb{Q}(\sqrt{-5})$ is a Dedekind domain. Indeed, this ring is noetherian being the quotient of a polynomial ring over $\mathbb{Z}$, it is normal being the ring of integers of a number field, and it is one dimensional, being an integral extension of $\mathbb{Z}$. However, $\mathbb{Z}[\sqrt{-5}]$ is not a PID because, for instance, the ideal $P = (2, 1+\sqrt{-5})$ is not principal. Indeed if P were generated by a single element $a+b\sqrt{-5}$, then a would have to be an even integer which divides 1, and this is impossible. As it turns out, the fact that the Dedekind domain $\mathbb{Z}[\sqrt{-5}]$ is not a PID is related to failure of unique factorization in $\mathbb{Z}[\sqrt{-5}]$, which is illustrated by the two distinct factorizations 2×3 and $(1+\sqrt{-5})(1-\sqrt{-5})$ of the number 6. Note, however, that if we pass to ideals and consider the principal ideal (6) generated by 6 in $\mathbb{Z}[\sqrt{-5}]$, then there is no problem because

$$(6) = (2, 1+\sqrt{-5})(2, 1-\sqrt{-5})(3, 1+\sqrt{-5})(3, 1-\sqrt{-5})$$

and it can be seen that the ideals on the right are distinct prime ideals and the above factorization is of (6) into prime ideals is unique up to rearrangement of factors.

Many more examples of Dedekind domains can be generated from the following basic result.

Theorem 3.3 (Extension Theorem). *Let A be a Dedekind domain, K its quotient field, L a finite separable extension of K, and B the integral closure of A in L. Then B is a Dedekind domain.*

Proof. By Finiteness Theorem 2.23, B is noetherian. It is obvious that A is normal. Lastly, by Corollary 2.19 we see that $\dim B = \dim A \leq 1$. □

Since $\mathbb{Z}$ is a Dedekind domain, we obtain as an immediate consequence the following corollary.

Corollary 3.4. *If K is a number field, then $\mathcal{O}_K$, the ring of integers of K, is a Dedekind domain.*

Exercise 3.5. Let A be a Dedekind domain with quotient field K. If S is any multiplicatively closed subset of A such that $0 \notin S$, then show that the localization $S^{-1}A$ of A at S is a Dedekind domain with quotient field K. Moreover, if L is an algebraic extension of K, then show that the integral closure of $S^{-1}A$ in L is $S^{-1}B$.

We shall now proceed to prove a number of basic properties of a Dedekind domain. In particular, we shall establish the fact about unique factorization of ideals as products of prime ideals, which was alluded to in the beginning of this section.

Definition 3.6. Let A be a domain and K be its quotient field. By a *fractionary ideal* of A we mean an A-submodule J of K such that $dJ \subseteq A$ for some $d \in A$, $d \neq 0$.

Note that a finitely generated A–submodule of K is a fractionary ideal of A. Conversely, if A is noetherian, then every fractionary ideal of A is finitely generated.

To distinguish from fractionary ideals, the (usual) ideals of A are sometimes called the *integral ideals* of A. Products of fractionary ideals is defined in the same way as the product of integral ideals, and w.r.t. this product, the set

$$\mathcal{F}_A = \{J : J \text{ a fractionary ideal of } A \text{ and } J \neq (0)\}$$

nonzero fractionary ideals is a commutative monoid with A as its identity element. Note that $\mathcal{F}_A$ contains the subset of nonzero principal fractionary ideals, viz.,

$$\mathcal{P}_A = \{Ax : x \in K, \text{ and } x \neq (0)\}$$

and this subset is, in fact, a group. In case A is a PID, we see easily (from Corollary 2.25, for example) that $\mathcal{F}_A = \mathcal{P}_A$, and in this case $\mathcal{F}_A$ is a group. We will soon show that more generally, if A is any Dedekind domain, then $\mathcal{F}_A$ is a group.

Lemma 3.7. *Every nonzero ideal of a noetherian ring A contains a finite product of nonzero prime ideals of A.*

Proof. Assume the contrary. Then the family of nonzero nonunit ideals of A not containing a finite product of nonzero prime ideals of A is nonempty. Let I be a maximal element of this family. Then $I \neq A$ and I can not be prime. Hence there exist $a, b \in A \setminus I$ such that $ab \in I$. Now $I + Aa$ and $I + Ab$ are ideals strictly larger than I, and $I \supseteq (I + Aa)(I + Ab)$. In particular, $I + Aa$ and $I + Ab$ are nonzero nonunit ideals. So by the maximality of I, both $I + Aa$ and $I + Ab$ contain a finite product of nonzero prime ideals, and hence so does I. This is a contradiction. □

Lemma 3.8. *Let A be a noetherian normal domain and K be its quotient field. If $x \in K$ and I is a nonzero ideal of I such that $xI \subseteq I$, then $x \in A$.*

Proof. Since $xI \subseteq I$, we have $x^n I \subseteq I$ for $n \geq 1$. Thus if we let $J = A[x]$, then $JI \subseteq I$. In particular, if $d \in I$, $d \neq 0$, then $dJ \subseteq A$. So J is a fractionary ideal of A and since A is noetherian, $J = A[x]$ is a f.g. A-module. Therefore, x is integral over A and since A is normal, $x \in A$. □

Lemma 3.9. *Let A be a Dedekind domain and K be its quotient field. If P is any nonzero prime ideal of A, then*

$$P' = (A :_K P) = \{x \in K : xP \subseteq A\}$$

is a fractionary ideal of A, which strictly contains A. Moreover, $PP' = A = P'P$. In particular, P is invertible and $P^{-1} = P'$.

Proof. Clearly, P' is an A-module. Also, $dP' \subseteq A$ for any $d \in P$, $d \neq 0$. Thus P' is a fractional ideal of A. It is clear that $P' \supseteq A$. To show that $P' \neq A$, choose any $d \in P$, $d \neq 0$. By Lemma 3.7, we can find nonzero prime ideals $P_1, \ldots, P_n$ of A such that $(d) \supseteq P_1 \cdots P_n$.

Suppose n is the least positive integer with this property. Now, $P_1 \cdots P_n \subseteq P$, and since P is prime, we have $P_i \subseteq P$ for some i. But A is a 1-dimensional ring, and so $P_i = P$. Define $I = P_1 \cdots P_{i-1} P_{i+1} \cdots P_n$ (note that $I = A$ if $n = 1$). Then by the minimality of n, $I \not\subseteq (d)$. Let $c \in I$ be such that $c \notin (d)$. Then $cd^{-1} \notin A$. But $PI \subseteq (d)$, and this implies that $P(c) \subseteq (d)$, and so $cd^{-1} \in P'$. Thus $P' \neq A$. Next, to show that $PP' = A$, observe that $P = PA \subseteq PP' \subseteq A$. Thus PP' is an (integral) ideal of A containing the maximal ideal P. Hence $PP' = A$ or $PP' = P$. But if $x \in P' \setminus A$, then by Lemma 3.8, $xP \not\subseteq P$, and hence $PP' \neq P$. It follows that $PP' = A$. □

Theorem 3.10. *If A is a Dedekind domain, then $\mathcal{F}_A$, the set of nonzero fractionary ideals of A, forms an abelian group (w.r.t products of fractionary ideals).*

Proof. It suffices to show that every nonzero (integral) ideal of A is invertible, because if $J \in \mathcal{F}_A$, then dJ is a nonzero ideal of A for some $d \in A$, $d \neq 0$, and $(d)(dJ)^{-1}$ is then the inverse of J.

Now if some nonzero ideal of A is not invertible, then we can find a nonzero ideal I of A, which is not invertible and which is maximal with this property. Clearly $I \neq A$ and so there is a nonzero prime ideal P of A such that $I \subseteq P$. By Lemma 3.9, P^{-1} exists and $I = IA \subseteq IP^{-1} \subseteq PP^{-1} = A$. Moreover, if $I = IP^{-1}$, then by Lemma 3.8, $P^{-1} \subseteq A$, which contradicts Lemma 3.9. Thus IP^{-1} is an ideal of A which is strictly larger than I. So by the maximality of I, the ideal IP^{-1} is invertible. But then so is $I = (IP^{-1})P$. This is a contradiction. □

Theorem 3.11. *Let A be a Dedekind domain. Then every nonzero ideal I of A can be factored as a product of prime ideals, and this factorization is unique up to a rearrangement of the factors. More generally, every nonzero fractional ideal J of A factors as $J = \mathfrak{p}_1^{e_1} \cdots \mathfrak{p}_h^{e_h}$, for some nonnegative integer h, distinct prime ideals $\mathfrak{p}_1, \ldots, \mathfrak{p}_h$ and nonzero integers $e_1, \ldots, e_h$.*[4] *Furthermore, the prime ideals $\mathfrak{p}_1, \ldots, \mathfrak{p}_h$ and the corresponding exponents $e_1, \ldots, e_h$ are uniquely determined by J.*

Proof. Assume for a moment that the assertion for integral ideals is proved. Then for any $J \in \mathcal{F}_A$, there exists $d \in A$, $d \neq 0$ such that dJ is a nonzero ideal of A. Now if $dJ = \mathfrak{p}_1 \cdots \mathfrak{p}_k$ and $(d) = \mathfrak{q}_1 \cdots \mathfrak{q}_l$, where $\mathfrak{p}_i$ and $\mathfrak{q}_j$ are prime ideals then $J = \mathfrak{p}_1 \cdots \mathfrak{p}_k \mathfrak{q}_1^{-1} \cdots \mathfrak{q}_l^{-1}$. Moreover, if we also have $J = P_1 \cdots P_m Q_1^{-1} \cdots Q_n^{-1}$ for some prime ideals P_i and Q_j (necessarily nonzero but not necessarily distinct), then $\mathfrak{p}_1 \cdots \mathfrak{p}_k Q_1 \cdots Q_n = \mathfrak{q}_1 \cdots \mathfrak{q}_l P_1 \cdots P_m$ and the uniqueness for factorization of integral ideals can be used. This yields the desired results for nonzero fractional ideals.

To prove the existence of factorization of nonzero ideals of A into prime ideals, we can proceed as in the proof of Theorem 3.10. Thus, let I be a nonzero ideal of A which can not be factored as a product of prime ideals and which is maximal with this property. Then $I \neq A$ and if P is a nonzero prime ideal containing I, then IP^{-1} is an ideal of A which is strictly larger than I. So by the maximality of I, the ideal IP^{-1} is a product of prime ideals. Multiplying on the right by P, we find that I is also a product of prime ideals. This is a contradiction.

To prove the uniqueness, let I be any nonzero ideal of A and suppose $I = \mathfrak{p}_1 \cdots \mathfrak{p}_r$ for some $r \geq 0$ and prime ideals $\mathfrak{p}_1, \ldots, \mathfrak{p}_r$. We induct on r to show that any other factorization of I as

[4] As per usual conventions, $\mathfrak{p}^{-m} = \left(\mathfrak{p}^{-1}\right)^m$, for any positive integer m. Also, when $h = 0$, a product such as $\mathfrak{p}_1^{e_1} \cdots \mathfrak{p}_h^{e_h}$ is the empty product and it equals $(1) = A$.

a product of prime ideals differs from $\mathfrak{p}_1 \cdots \mathfrak{p}_r$ by a rearrangement of factors. If $r = 0$, this is evident since a nonempty product of prime ideals will be contained in any one of the factors, which is a proper subset of A. Assume that $r \geq 1$ and the result holds for ideals which are products of $r-1$ prime ideals. Now if $I = \mathfrak{q}_1 \cdots \mathfrak{q}_s$ for some $s \geq 0$ and prime ideals $\mathfrak{q}_1, \ldots, \mathfrak{q}_s$, then it is clear that $s > 0$. Moreover, $\mathfrak{q}_1 \cdots \mathfrak{q}_s \subseteq \mathfrak{p}_1$ implies that $\mathfrak{q}_j \subseteq \mathfrak{p}_1$ for some j. But since $I \neq (0)$, each $\mathfrak{q}_j$ is a nonzero prime ideal and hence maximal. Thus $\mathfrak{q}_j = \mathfrak{p}_1$. Multiplying I by $\mathfrak{p}_1^{-1}$ we find that $\mathfrak{p}_2 \cdots \mathfrak{p}_r = \mathfrak{q}_1 \cdots \mathfrak{q}_{j-1}\mathfrak{q}_{j+1} \cdots \mathfrak{q}_s$. Thus by induction hypothesis $r - 1 = s - 1$ and $\mathfrak{p}_2, \ldots \mathfrak{p}_r$ are the same as $\mathfrak{q}_1, \ldots, \mathfrak{q}_{j-1}, \mathfrak{q}_{j+1}, \ldots, \mathfrak{q}_s$ after a rearrangement. This implies that $r = s$ and $\mathfrak{p}_1, \ldots, \mathfrak{p}_r$ equal $\mathfrak{q}_1, \ldots, \mathfrak{q}_s$ after a rearrangement. □

Remark 3.12. Either of the following four conditions can be taken as a definition for an integral domain A to be a Dedekind domain.

(1) A is noetherian, normal and every nonzero prime ideal of A is maximal.

(2) Nonzero fractional ideals of A form a group with respect to multiplication.

(3) Every nonzero ideal of A factors uniquely as a product of prime ideals.

(4) Every nonzero ideal of A factors as a product of prime ideals.

Note that (3) $\Rightarrow$ (4) is obvious and from Theorems 3.10 and 3.11, we have (1) $\Rightarrow$ (2) and (1) $\Rightarrow$ (3). Moreover, if (2) holds, then A is noetherian because if I is a nonzero ideal of A, then $II^{-1} = A$ implies that $\sum_{i=1}^{n} a_i b_i = 1$ for some $a_i \in I$, $b_i \in I^{-1}$, and consequently, $I = (a_1, \ldots, a_n)$. Further, if (2) holds, then as in the proof of Theorem 3.11, the existence of a nonzero ideal of A which can not be factored as a product of prime ideals leads to a contradiction. This shows that (2) $\Rightarrow$ (4). Hence, to prove the equivalence of (1), (2), (3) and (4) it suffice to show that (4) $\Rightarrow$ (1). This can be done but it needs a little bit of work; for details, we refer to [20, Ch. V, §6].

Exercise 3.13. Use Theorem 3.11 to show that for every nonzero prime ideal $\mathfrak{p}$ of A, we can define a function $n_{\mathfrak{p}} : \mathcal{F}_A \to \mathbb{Z}$ such that for any $J \in \mathcal{F}_A$, we have $n_{\mathfrak{p}}(J) = 0$ for all except finitely many $\mathfrak{p}$, and

$$J = \prod_{\mathfrak{p}} \mathfrak{p}^{n_{\mathfrak{p}}(J)}$$

where the product is over all nonzero prime ideals $\mathfrak{p}$ of A. Further show that J is an integral ideal of A if and only if $n_{\mathfrak{p}}(J) \geq 0$ for all nonzero prime ideals $\mathfrak{p}$ of A. Deduce that for $J_1, J_2 \in \mathcal{F}_A$,

$$J_1 \subseteq J_2 \iff n_{\mathfrak{p}}(J_1) \geq n_{\mathfrak{p}}(J_2) \text{ for all nonzero prime ideals } \mathfrak{p} \text{ of } A.$$

Use this to show that if I_1, I_2 are integral ideals of A, then $I_1 \subseteq I_2$ if and only if I_2 divides I_1, i.e., $I_1 = I_2 I_3$ for some integral ideal I_3 of A. Finally, for any $J_1, J_2 \in \mathcal{F}_A$ and a nonzero prime ideal $\mathfrak{p}$ of A, prove the following.

(i) $n_{\mathfrak{p}}(J_1 J_2) = n_{\mathfrak{p}}(J_1) + n_{\mathfrak{p}}(J_2)$ and $n_{\mathfrak{p}}(J_1 J_2^{-1}) = n_{\mathfrak{p}}(J_1) - n_{\mathfrak{p}}(J_2)$.

(ii) $n_{\mathfrak{p}}(J_1 + J_2) = \min\{n_{\mathfrak{p}}(J_1), n_{\mathfrak{p}}(J_2)\}$ and $n_{\mathfrak{p}}(J_1 \cap J_2^{)} = \max\{n_{\mathfrak{p}}(J_1), n_{\mathfrak{p}}(J_2)\}$.

We have seen in Example 3.2 that a Dedekind domain need not be a UFD. On the other hand, if a Dedekind domain A is a UFD and P is any nonzero prime ideal of A, then P must contain an irreducible element because otherwise there will be an infinite strictly ascending chain $(a_1) \subset (a_2) \subset \cdots$ of principal ideals contained in P, contradicting that A is noetherian. Now if $p \in P$ is irreducible, then (p) is a nonzero prime ideal, and hence maximal. Hence, $P = (p)$. Next, by Theorem 3.11, every nonzero ideal of A is a product of prime ideals and therefore, it is principal. Thus A is a PID. Consequently, if a Dedekind domain A is a UFD, then $\mathcal{F}_A = \mathcal{P}_A$ or in other words, the quotient group $\mathcal{F}_A/\mathcal{P}_A$ is trivial.

Definition 3.14. Let A be a Dedekind domain and K be its quotient field. The *ideal class group* of A, denoted by $\mathcal{C}_A$, is defined to be the quotient $\mathcal{F}_A/\mathcal{P}_A$. When K is a number field and $A = \mathcal{O}_K$ is its ring of integers, $\mathcal{C}_A$ is often denoted by $\mathcal{C}_K$ and called the ideal class group of K. The elements of $\mathcal{C}_K$ are called the *ideal classes* of K.

As remarked earlier, if A is a Dedekind domain, then

$$A \text{ is a UFD } \iff A \text{ is a PID } \iff \mathcal{C}_A \text{ is trivial.}$$

Thus the size of the ideal class group $\mathcal{C}_A$ is a measure of how far A is from being a UFD. In the case when K is a number field and $A = \mathcal{O}_K$, it turns out that $\mathcal{C}_K$ is a finite (abelian) group. The order of this group is denoted by h_K and is called the *class number* of K. The finiteness of class number will be proved in Chapter 4 using some general results of Minkowski. A shorter proof is outlined in Exercise 4.3.

We end this section with a result which gives a sufficient condition for a Dedekind domain to be a PID.

Proposition 3.15. *A local Dedekind domain is a PID. More generally, if a Dedekind domain has only finitely many maximal ideals, then it is a PID.*

Proof. Let A be a Dedekind domain with only finitely many maximal ideals, say, $P_1, \ldots, P_r$. Note that the ideals $P_1, \ldots, P_r$, and more generally, their powers $P_1^{m_1}, \ldots, P_r^{m_r}$ are pairwise comaximal. Fix any $i \in \{1, \ldots, r\}$. Note that $P_i \neq P_i^2$ (because otherwise $P_i = A$). So we can find $a_i \in P_i \setminus P_i^2$. By Chinese Remainder Theorem [cf. Prop. 2.3], there exists $a \in A$ such that

$$a \equiv a_i (\text{mod } P_i^2) \quad \text{and} \quad a \equiv 1 (\text{mod } P_j) \text{ for } 1 \leq j \leq r,\ j \neq i.$$

Now, (a) is a nonzero ideal of A with $(a) \subseteq P_i$, and the factorization of (a) into prime ideals can neither contain P_j for any $j \neq i$ nor can it contain a power of P_i with exponent 2 or more. Hence $(a) = P_i$. Since every nonzero ideal of A is a product of the P_i's, it must be principal. Thus A is a PID. □

Remark 3.16. A ring with only finitely many maximal ideals is sometimes called a *semilocal ring*. Thus the above Proposition says that a semilocal Dedekind domain is a PID. In the case of local Dedekind domains, we can, in fact, say more. Namely, a local Dedekind domain is what is called a discrete valuation ring or a DVR. An integral domain A with quotient field K is a *discrete valuation ring* if there exists a map $v : K \setminus \{0\} \to \mathbb{Z}$ with the properties

$$v(xy) = v(x) + v(y) \quad \text{and} \quad v(x+y) \geq \min\{v(x), v(y)\} \quad \text{for all } x, y \in K \setminus \{0\}$$

and $A = \{x \in K : x = 0 \text{ or } v(x) \geq 0\}$. The map v is called a *valuation* of K and A is called its *valuation ring*. In case A is a local Dedekind domain, A has only one nonzero prime ideal, i say P, and for any nonzero element x of the quotient field of A, we can write $Ax = P^n$ for a unique integer n, and the map given by $x \mapsto n$ is a valuation of K whose valuation ring is A.

Exercise 3.17. Let A be a Dedekind domain. If P is a nonzero prime ideal of A and e a positive integer, then show that A/P^e is a principal ideal ring. Use this and the Chinese Remainder Theorem to show that if I is any nonzero ideal of A, then R/I is a principal ideal ring. Deduce that every ideal of A can be generated by two elements.

3.2 Extensions of Primes

In the ring $\mathcal{O}_K$ of integers of a number field K, a prime p of $\mathbb{Z}$ may not remain a prime. For instance in the ring of integers of $\mathbb{Q}(\sqrt{-1})$, namely, in the ring $\mathbb{Z}[i]$ [5], the rational primes 2 and 5 are no longer primes but 3 is. However, by Theorem 3.11, the ideal generated by p in this ring can be uniquely factored as a product of prime ideals. Roughly speaking, the phenomenon of a prime splitting into several primes in an extension, is known as ramification. In this context, there is a beautiful analogue of the formula $\sum_{i=1}^{g} e_i f_i = n$, which holds when a monic polynomial $f(X)$ of degree n with coefficients in a field F, factors as $f(X) = p_1(X)^{e_1} \cdots p_g(X)^{e_g}$, where $g \geq 0$, $e_i > 0$ and $p_i(X)$ are distinct monic irreducible polynomials in $F[X]$ of degree f_i. We now proceed to give some relevant definitions and prove the $\sum_{i=1}^{g} e_i f_i = n$ formula in the general setting of Dedekind domains.

In this section, we shall assume that A, K, L, B are as in the Extension Theorem 3.3. We will also let n denote the degree of L/K.

Definition 3.18. Let $\mathfrak{p}$ be a prime ideal of A. A prime ideal P of B is said to *lie over* $\mathfrak{p}$ if $P \cap A = \mathfrak{p}$.

Since B is a Dedekind domain, for any nonzero prime ideal $\mathfrak{p}$ of A, the extension $\mathfrak{p}B$ of $\mathfrak{p}$ to B is a nonzero ideal of B and hence it can be uniquely written as

$$\mathfrak{p}B = \prod_{i=1}^{g} P_i^{e_i}$$

where $P_1, P_2, \ldots, P_g$ are distinct nonzero prime ideals of B and e_i are positive integers.

Exercise 3.19. With $\mathfrak{p}$ and P_i as above, show that a prime ideal P of B lies over $\mathfrak{p}$ iff $P = P_i$ for some i. Also show that $\mathfrak{p}B \cap A = \mathfrak{p} = P_i^{e_i} \cap A$. Deduce that $B/\mathfrak{p}B$ as well as $B/P_i^{e_i}B$ can be regarded as vector spaces over the field $A/\mathfrak{p}$. Further show that B/P_i is a field extension of $A/\mathfrak{p}$ whose degree is at most n.

Definition 3.20. With $\mathfrak{p}$, P_i, etc. as above, the positive integer e_i is called the *ramification index* of P_i over $\mathfrak{p}$ and is denoted by $e(P_i/\mathfrak{p})$; the field degree $[B/P_i : A/\mathfrak{p}]$ is called the *residue degree* (or the *residue class degree*) of P_i over $\mathfrak{p}$ and is denoted by $f(P_i/\mathfrak{p})$. If $e_i > 1$ for some

[5] Elements of $\mathbb{Z}[i]$ are often called the *Gaussian integers*. These were first studied by C. F. Gauss in his work on biquadratic reciprocity.

i, then we say that $\mathfrak{p}$ is ramified in B (or in L). Otherwise, it is said to be *unramified.* [6] The extension L/K is said to be *unramified* if every nonzero prime ideal of A is unramified in L.

Exercise 3.21. Let A, K, L, B and $\mathfrak{p}$ be as above. Suppose L' is a finite separable extension of L and B' is the integral closures of B in L'. Show that B' is the integral closure of A in L'. Further, if P a prime of B lying over $\mathfrak{p}$ and P' a prime of B' lying over P, then show that P' lies over $\mathfrak{p}$ and the following transitivity relations hold:

$$e(P'/\mathfrak{p}) = e(P'/P)e(P/\mathfrak{p}) \quad \text{and} \quad f(P'/\mathfrak{p}) = f(P'/P)f(P/\mathfrak{p}).$$

We are now ready to prove the main result of this section.

Theorem 3.22. *Let A, K, L, B be as above and $n = [L : K]$. Suppose $\mathfrak{p}$ is a nonzero prime ideal of A and we have*

$$\mathfrak{p}B = \prod_{i=1}^{g} P_i^{e_i}$$

where $P_1, P_2, \ldots, P_g$ are distinct prime ideals of B and $e_1, \ldots, e_g$ are positive integers. Then, upon letting $f_i = [B/P_i : A/\mathfrak{p}]$, we have

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

Proof. Let $S = A \setminus \mathfrak{p}$ and $A' = S^{-1}A$ be the localization of A at $\mathfrak{p}$. Then $B' = S^{-1}B$ is the integral closure of A' in L, and $\mathfrak{p}B' = P_1'^{e_1} \ldots P_g'^{e_g}$, where $P_i' = P_i B'$. Moreover, the primes $P_1', \ldots, P_g'$ are distinct, $A'/\mathfrak{p}A' \simeq A/\mathfrak{p}$ and $B'/P_i' \simeq B/P_i$. Thus we see that in order to prove the equality $\sum e_i f_i = n$, we can replace $A, B, \mathfrak{p}, P_i$ by $A', B', \mathfrak{p}', P_i'$ respectively.

In view of the observations above, we shall assume without loss of generality that A is a local Dedekind domain with $\mathfrak{p}$ as its unique nonzero prime ideal. Then, by the Corollary 2.25, B is a free A–module of rank $n = [L : K]$. Write $B = Ay_1 + \cdots + Ay_n$, where $y_1, \ldots, y_n$ are some elements of B. Now for the vector space $B/\mathfrak{p}B$ over $A/\mathfrak{p}$, we clearly have

$$B/\mathfrak{p}B = \sum_{i=1}^{n} (A/\mathfrak{p})\, \bar{y}_i$$

where $\bar{y}_i$ denotes the residue class of y_i mod $\mathfrak{p}B$. Moreover,

$$\sum \bar{a}_i \bar{y}_i = 0 \Longrightarrow \sum a_i y_i \in \mathfrak{p}B \Longrightarrow a_i \in \mathfrak{p}$$

where $a_i \in A$ and $\bar{a}_i$ denotes its residue class mod $\mathfrak{p}$, and the last implication follows since $\{y_1, \ldots, y_n\}$ is a free A–basis of B. It follows that $\bar{y}_1, \ldots, \bar{y}_n$ are linearly independent over $A/\mathfrak{p}$, and hence

$$\dim_{A/\mathfrak{p}} B/\mathfrak{p}B = n.$$

[6] To be accurate, we should define $\mathfrak{p}$ to be *ramified* if $e_i > 1$ for some i or B/P_i is inseparable over $A/\mathfrak{p}$ for some i. However, in number theoretic applications, $A/\mathfrak{p}$ will usually be a finite field and so the question of separability of residue field extensions doesn't arise.

Now we count the same dimension by a different method. First, note that since $P_1, \ldots, P_g$ are distinct maximal ideals, $P_1^{e_1}, \ldots, P_g^{e_g}$ are pairwise comaximal. Since $\mathfrak{p}B = P_1^{e_1} \cdots P_g^{e_g}$, by Chinese Remainder Theorem, we get an isomorphism (of rings as well as of $(A/\mathfrak{p})$–vector spaces)

$$B/\mathfrak{p}B \simeq \bigoplus_{i=1}^{g} B/P_i^{e_i}.$$

Now let us find the dimension of the $A/\mathfrak{p}$–vector space B/P^e where $P = P_i$ and $e = e_i$ for some i. First, we note that for any $j \geq 1$, $\mathfrak{p}P^j \subseteq P^{j+1}$, and hence P^j/P^{j+1} can be considered as a vector space over $A/\mathfrak{p}$. We claim that we have an isomorphism

$$B/P^e \simeq B/P \oplus P/P^2 \oplus \cdots \oplus P^{e-1}/P^e.$$

To see this, use induction on e and the fact that for $e > 1$, we clearly have

$$B/P^{e-1} \simeq \frac{B/P^e}{P^{e-1}/P^e}.$$

Next, we note that B is a Dedekind domain having only finitely many prime ideals (in fact, (0) and $P_1, \ldots, P_g$ are the only primes of B), and so B must be a PID. Let t be a generator of P, and consider the map

$$B/P \to P^j/P^{j+1}$$

induced by the multiplication map $x \mapsto t^j x$ of $B \to P^j$. This map is an $A/\mathfrak{p}$–homomorphism, and it is clearly bijective. So

$$\dim_{A/\mathfrak{p}}(P^j/P^{j+1}) = \dim_{A/\mathfrak{p}}(B/P) = f(P/\mathfrak{p})$$

and consequently, from the above direct sum representations, we get

$$\dim_{A/\mathfrak{p}}(B/\mathfrak{p}B) = \sum_{i=1}^{g} \dim_{A/\mathfrak{p}}(B/P_i^{e_i}) = \sum_{i=1}^{g} e_i f_i,$$

which yields the desired identity. This completes the proof. □

Examples:

1. Consider the quadratic field $K = \mathbb{Q}(i)$, where i denotes a square root of -1. We know that $\mathcal{O}_K$ is the ring $\mathbb{Z}[i]$ of Gaussian integers. If p is a prime $\equiv 1 (\mathrm{mod}\ 4)$, then we know (by a classical result of Fermat) that p can be written as a sum of two squares. Thus there exist $a, b \in \mathbb{Z}$ such that $p = a^2 + b^2 = (a + bi)(a - bi)$. It can be seen that $(a + bi)$ and $(a - bi)$ are distinct prime ideals in $\mathcal{O}_K$. Thus for the prime ideal $p\mathbb{Z}$, we have $g = 2$, $e_1 = e_2 = 1$ and (since $\sum e_i f_i = 2$) $f_1 = f_2 = 1$. On the other hand, it is not difficult to see that a prime $\equiv 3 (\mathrm{mod}\ 4)$ generates a prime ideal in $\mathbb{Z}[i]$ and so for such a prime, we have $g = 1 = e_1$ and $f_1 = 2$. The case of $p = 2$ is special. We have $2 = (1 + i)(1 - i)$. But $(1 + i)$ and $(1 - i)$ differ only by a unit (namely, $-i$) and thus they generate the same prime ideal. So 2 is a ramified prime and for it, we have $g = 1 = f_1$ and $e_1 = 2$.

2. In Example 2 of Section 2.4, where we discussed the p^{th} cyclotomic field $K = \mathbb{Q}(\zeta_p)$, we have proved the identity

$$p = (\zeta - 1)(\zeta^2 - 1)\dots(\zeta^{p-1} - 1),$$

and also the fact that $(\zeta - 1)\mathcal{O}_K \cap \mathbb{Z} = p\mathbb{Z}$. We note that for any integer i not divisible by p, we can find an integer j such that $ij \equiv 1 (\text{mod } p)$, and thus $(\zeta^i - 1)/(\zeta - 1) = 1 + \zeta + \dots + \zeta^{i-1} \in \mathbb{Z}[\zeta]$ and its inverse $(\zeta - 1)/(\zeta^i - 1) = (\zeta^{ij} - 1)/(\zeta^i - 1)$ is also in $\mathbb{Z}[\zeta]$. Therefore, the fraction $(\zeta^i - 1)/(\zeta - 1)$ is a unit in $\mathbb{Z}[\zeta]$. Consequently, $(\zeta^i - 1)$ and $(\zeta - 1)$ generate the same ideal, say P. Now the above identity together with the previous Theorem shows that $p\mathbb{Z}[\zeta] = P^{p-1}$ and P is a prime ideal. Thus we find that in this case $g = 1 = f_1$ and $e_1 = p - 1 = [K : \mathbb{Q}]$.

The last example illustrates the following definition.

Definition 3.23. A nonzero prime ideal $\mathfrak{p}$ of A is said to be *totally ramified* in L (or in B) if $\mathfrak{p}B = P^n$ for some prime ideal P of B.

3.3 Kummer's Theorem

In this section we prove a theorem, due to Kummer, which shows how the decomposition of extended prime ideals can be "read off" from the factorization of a polynomial, for a certain class of rings. It may be observed that the hypothesis of this theorem is satisfied in the case of quadratic and cyclotomic extensions.

We shall use the following notation. Given a domain A and a maximal ideal $\mathfrak{p}$ in A, we let $\bar{A}$, denote the residue field $A/\mathfrak{p}$; for any polynomial $p(X) \in A[X]$, by $\bar{p}(X)$ we denote its reduction mod $\mathfrak{p}$, i.e., the polynomial in $\bar{A}[X]$ whose coefficients are the $\mathfrak{p}$–residues of the corresponding coefficients of $p(X)$.

Theorem 3.24. *Let A be a Dedekind domain, K its quotient field, L a finite separable extension of K, and B the integral closure of A in L. Let $\mathfrak{p}$ be a nonzero prime ideal of A. Assume that $B = A[\alpha]$ for some $\alpha \in B$. Let $f(X) = \text{Irr}(\alpha, K)$. Suppose*

$$\bar{f}(X) = \prod_{i=1}^{g} \bar{p}_i(X)^{e_i}$$

is the factorization of $\bar{f}(X)$ into powers of distinct monic irreducible polynomials in $\bar{A}[X]$. Let $p_i(X)$ be the monic polynomial in $A[X]$ whose reduction mod $\mathfrak{p}$ is $\bar{p}_i(X)$. Then the primes in B lying over $\mathfrak{p}$ are precisely given by $P_1, \dots, P_g$ where $P_i = \mathfrak{p}B + p_i(\alpha)B$. Moreover,

$$\mathfrak{p}B = \prod_{i=1}^{g} P_i^{e_i}$$

is the factorization of $\mathfrak{p}B$ into powers of distinct primes in B, the ramification index of P_i over $\mathfrak{p}$ is the above exponent e_i, and the residue degree f_i of P_i over $\mathfrak{p}$ is the degree of the irreducible factor $\bar{p}_i(X)$.

Proof. Fix some i with $1 \le i \le g$. Let $\bar{\alpha}_i$ be a root of $\bar{p}_i(X)$. Consider the maps

$$A[X] \to \bar{A}[X] \to \bar{A}[X]/(\bar{p}_i(X)) \simeq \bar{A}[\bar{\alpha}_i]$$

where the first map sends a polynomial in $A[X]$ to its reduction mod $\mathfrak{p}$, and the second one is the natural quotient map. The composite of these maps is a homomorphism from $A[X]$ onto $\bar{A}[\bar{\alpha}_i]$, and its kernel is clearly given by $\mathfrak{p}A[X] + p_i(X)A[X]$. This kernel contains $f(X)$, and thus we get the induced map of $A[X]/(f(X))$ onto $\bar{A}[\bar{\alpha}_i]$. Since $B = A[\alpha] \simeq A[X]/(f(X))$, we get a map φ_i of B onto $\bar{A}[\bar{\alpha}_i]$. Note that $\ker \varphi_i$ is equal to $\mathfrak{p}B + p_i(\alpha)B$. Since $\bar{p}_i(X)$ is irreducible in $\bar{A}[X]$, $\ker \varphi_i$ is a prime ideal in B which contains $\mathfrak{p}$. It is therefore a maximal ideal in B lying over $\mathfrak{p}$. Also $\bar{A}$ is a field and

$$[B/\ker \varphi_i : A/\mathfrak{p}] = \dim_{\bar{A}} \bar{A}[\bar{\alpha}_i] = \deg \bar{p}_i(X).$$

Now suppose P is any maximal ideal of B lying over $\mathfrak{p}$. Since

$$f(X) - p_1(X)^{e_1} \dots p_g(X)^{e_g} \in \mathfrak{p}A[X]$$

and $f(\alpha) = 0$, we see that

$$p_1(\alpha)^{e_1} \dots p_g(\alpha)^{e_g} \in \mathfrak{p}B \subseteq P$$

and hence $p_i(\alpha) \in P$ for some i, and then it follows that P must be equal to $\mathfrak{p}B + p_i(\alpha)B$. This shows that the primes lying in B over $\mathfrak{p}$ are precisely $P_1, \dots, P_g$ where $P_i = \mathfrak{p}B + p_i(\alpha)B$, and that the residue degree $f_i = f(P_i/\mathfrak{p})$ equals $\deg \bar{p}_i(X)$. To prove the remaining assertion, let e_i' denote the ramification index of P_i over $\mathfrak{p}$, so that

$$\mathfrak{p}B = P_1^{e_1'} \dots P_g^{e_g'}.$$

Since $P_i = \mathfrak{p}B + p_i(\alpha)B$, we have

$$P_i^{e_i} \subseteq \mathfrak{p}B + p_i(\alpha)^{e_i}B$$

and hence, in view of the above observation that $p_1(\alpha)^{e_1} \dots p_g(\alpha)^{e_g} \in \mathfrak{p}B$, we have

$$P_1^{e_1} \dots P_g^{e_g} \subseteq \mathfrak{p}B + p_1(\alpha)^{e_1} \dots p_g(\alpha)^{e_g}B \subseteq \mathfrak{p}B = P_1^{e_1'} \dots P_g^{e_g'}.$$

Consequently $e_i \geq e_i'$ for all i. But we know that

$$\sum_{i=1}^{g} e_i f_i = \deg f(X) = [L : K] = \sum_{i=1}^{g} e_i' f_i.$$

Therefore $e_i = e_i'$ for all i. This completes the proof. □

Remark 3.25. If K is a number field, then by Primitive Element Theorem, there exists $\alpha \in K$ such that $K = \mathbb{Q}(\alpha)$. We can also choose this α to be in $\mathcal{O}_K$. However, a choice of α for which $\mathcal{O}_K = \mathbb{Z}[\alpha]$ may not always be possible. In other words, the hypothesis of Kummer's Theorem may not always be satisfied. As indicated earlier, quadratic fields and cyclotomic fields do satisfy the hypothesis of Kummer's Theorem. Exercise 2.30 gives another example of a number field $K = \mathbb{Q}(\alpha)$ for which $\mathcal{O}_K = \mathbb{Z}[\alpha]$. On the other hand, the following exercise gives an example, due to Dedekind, of a number field K for which doesn't satisfy the hypothesis of Kummer's Theorem.

Exercise 3.26. Let $\alpha \in \mathbb{C}$ be a root of $X^3 - X^2 - 2X - 8$ and $K = \mathbb{Q}(\alpha)$. Prove the following: (i) $[K : \mathbb{Q}] = 3$; (ii) if $\beta = (\alpha^2 + \alpha)/2$, then $\beta^3 - 3\beta^2 - 10\beta - 9 = 0$, and hence $\beta \in \mathcal{O}_K$; (iii) $D_{K/\mathbb{Q}}(1, \alpha, \alpha^2) = -4(503)$ and $D_{K/\mathbb{Q}}(1, \alpha, \beta) = -503$, and hence $\{1, \alpha, \beta\}$ is an integral basis of $\mathcal{O}_K$; (iv) for any $\theta \in \mathcal{O}_K$, $D_{K/\mathbb{Q}}(1, \theta, \theta^2)$ is an even integer; (v) $\mathcal{O}_K \neq \mathbb{Z}[\theta]$ for any $\theta \in \mathcal{O}_K$.

3.4 Dedekind's Discriminant Theorem

Suppose we have a number field K whose ring of integers $\mathcal{O}_K$ is of the form $\mathbb{Z}[\alpha]$. Let $f(X)$ be the minimal polynomial of α over $\mathbb{Q}$ and p be a rational prime[7]. Let $\bar{f}(X) \in \mathbb{Z}/p\mathbb{Z}[X]$ denote the reduction of $f(X)$ mod $p\mathbb{Z}$. Then, by Kummer's Theorem, p ramifies in K iff $\bar{f}(X)$ has a multiple root. Now, the polynomial $\bar{f}(X)$ has a multiple root iff its (classical) discriminant is zero (as an element of $\mathbb{Z}/p\mathbb{Z}$). The last condition means that $\mathrm{Disc}_X f(X) = \pm d_K$ is divisible by p. Thus we find that in this situation we have:

$$p \text{ ramifies in } K \text{ iff } p \text{ divides } d_K.$$

In fact, this turns out to be true even in a more general situation. This section is devoted to a proof of this fundamental result, which is due to Dedekind.

Theorem 3.27. *Let A be a Dedekind domain and K be its quotient field. Let L be a finite separable extension of K of degree n, and B be the integral closure of A in L. Let $\mathfrak{p}$ be a nonzero prime ideal of A. Assume that the field $A/\mathfrak{p}$ is perfect (which means that every algebraic extension of this field is separable)*[8]*. Then we have:*

$$\mathfrak{p} \text{ ramifies in } L \Longleftrightarrow \mathfrak{p} \supseteq \mathcal{D}_{B/A}.$$

In particular, if the above assumption on the residue field is satisfied by every nonzero prime ideal of A, then there are only a finitely many prime ideals in A which ramify in L.

Proof. If we consider the localizations $A' = S^{-1}A$ and $B' = S^{-1}B$ where $S = A \setminus \mathfrak{p}$, then it is readily seen that $\mathcal{D}_{B'/A'} = \mathcal{D}_{B/A}A'$ and $\mathfrak{p}$ ramifies in L iff $\mathfrak{p}' = \mathfrak{p}A'$ ramifies in L. Thus to prove the first assertion, we can and will assume without loss of generality that A is a local Dedekind domain and $\mathfrak{p}$ is its unique maximal ideal.

Let $\mathfrak{p}B = P_1^{e_1}P_2^{e_2}\cdots P_g^{e_g}$, where $P_1, P_2, \ldots, P_g$ are distinct prime ideals of B and $e_1, e_2, \ldots, e_g$ are their ramification indices. As noted in the proof of Theorem 3.22, we have $\mathfrak{p}B \cap A = \mathfrak{p} = P_i^{e_i} \cap A$, and we have an isomorphism of $A/\mathfrak{p}$–vector spaces

$$B/\mathfrak{p}B \simeq \bigoplus_{i=1}^{g} B/P_i^{e_i}.$$

Let us set $\bar{A} = A/\mathfrak{p}$ and $\bar{B} = B/\mathfrak{p}B$. For $x \in B$, let $\bar{x}$ denote the image of x in $\bar{B}$. Note that we clearly have

$$\mathrm{Tr}_{\bar{B}/\bar{A}}(\bar{x}) = \overline{\mathrm{Tr}_{L/K}(x)} \qquad \text{for all } x \in B.$$

Now if $\{\alpha_1, \ldots, \alpha_n\}$ is any K–basis of L contained in B such that $\{\bar{\alpha}_1, \ldots, \bar{\alpha}_n\}$ is an $\bar{A}$–basis of $\bar{B}$, then using the above identity for traces, we see that

$$D_{\bar{B}/\bar{A}}(\bar{\alpha}_1, \ldots, \bar{\alpha}_n) = \overline{D_{L/K}(\alpha_1, \ldots, \alpha_n)}. \tag{1}$$

[7] It is a common practice in Number Theory to call the usual primes as *rational primes* (and the usual integers as *rational integers*) so as to distinguish from primes (and integers) in the rings of integers of algebraic number fields.

[8] This assumption would always be satisfied in number theoretic applications since $A/\mathfrak{p}$ would usually be a finite field.

Next, we show that if $\bar{B} \simeq \bar{B}_1 \oplus \cdots \oplus \bar{B}_g$, where the isomorphism is of $\bar{A}$–vector spaces, then we have

$$\mathcal{D}_{\bar{B}/\bar{A}} = \prod_{i=1}^{g} \mathcal{D}_{\bar{B}_i/\bar{A}}. \tag{2}$$

To see the above identity, it suffices to consider the case when $g = 2$ since the general case would follow by induction on g. For convenience of notation, let us denote the element of B corresponding to $(u, 0) \in \bar{B}_1 \oplus \bar{B}_2$ by u itself and, similarly, the element of B corresponding to $(0, v) \in \bar{B}_1 \oplus \bar{B}_2$ by v itself. It is clear that we can choose $\bar{A}$–bases $\{u_1, \ldots, u_r\}$ and $\{v_1, \ldots, v_s\}$ of $\bar{B}_1$ and $\bar{B}_2$ respectively such that $\{u_1, \ldots, u_r, v_1, \ldots, v_s\}$ is an $\bar{A}$–basis of $\bar{B}$. In view of the above convention, we see that $u_i v_j = 0$. Thus $\mathrm{Tr}_{\bar{B}/\bar{A}}(u_i v_j) = 0$, and so

$$D_{\bar{B}/\bar{A}}(u_1, \ldots, u_r, v_1, \ldots, v_s) = \left| \begin{array}{c|c} \mathrm{Tr}(u_i u_{i'}) & 0 \\ \cdots\cdots & \cdots\cdots \\ 0 & \mathrm{Tr}(v_j v_{j'}) \end{array} \right| = D_{\bar{B}_1/\bar{A}}(u_1, \ldots, u_r) D_{\bar{B}_2/\bar{A}}(v_1, \ldots, v_s).$$

Since $\bar{A}$ is a field and the non-vanishing of any of the above discriminants is independent of the choice of the corresponding $\bar{A}$–bases, the desired equality of discriminant ideals follows. Thus we have proved (2).

Now suppose $\mathfrak{p}$ is a ramified prime. Then $e_i > 1$ for some i and thus the ring $B/P_i^{e_i}$ contains a nonzero nilpotent element (which may be taken to be any element of $P_i^{e_i - 1} \setminus P_i^{e_i}$), and hence so does $\bar{B}$. Let $\beta \in B$ be such that $\bar{\beta} \in \bar{B}$ is a nonzero nilpotent element. Extend $\{\bar{\beta}\}$ to an $\bar{A}$–basis $\{\bar{\beta}_1, \ldots, \bar{\beta}_n\}$ of $\bar{B}$ with $\beta_1 = \beta$. Since $\bar{\beta}_1$ is nilpotent, so is $\bar{\beta}_1 \bar{\beta}_j$ for $1 \leq j \leq n$. Hence $\mathrm{Tr}(\bar{\beta}_1 \bar{\beta}_j) = 0$ for $1 \leq j \leq n$ [because if $u \in \bar{B}$ is nilpotent, then 0 is clearly the only eigenvalue of the linear transformation $x \mapsto ux$ of $\bar{B} \to \bar{B}$ and $\mathrm{Tr}(u)$ equals the sum of all eigenvalues of this linear transformation]. Consequently, $D_{\bar{B}/\bar{A}}(\bar{\beta}_1, \ldots, \bar{\beta}_n) = 0$, and so $\mathcal{D}_{\bar{B}/\bar{A}}$ is the zero ideal. Thus if $\{\alpha_1, \ldots, \alpha_n\}$ is an A–basis of B (which exists by Finiteness Theorem), then $\{\bar{\alpha}_1, \ldots, \bar{\alpha}_n\}$ is an $\bar{A}$–basis of $\bar{B}$ and in view of (1), we see that $D_{L/K}(\alpha_1, \ldots, \alpha_n) \in \mathfrak{p}B$. It follows that $\mathcal{D}_{B/A} \subseteq \mathfrak{p}B \cap A = \mathfrak{p}$.

To prove the converse, assume that $\mathfrak{p} \supseteq \mathcal{D}_{B/A}$. Suppose, if possible, $\mathfrak{p}$ is unramified. Then $e_i = 1$ for all i and thus $\bar{B}$ is isomorphic (as an $\bar{A}$–vector space) to the direct sum of the fields $\bar{B}_i = B/P_i$. Since $\bar{A}$ is perfect, the extension $\bar{B}_i/\bar{A}$ is separable, and therefore $\mathcal{D}_{\bar{B}_i/\bar{A}} \neq 0$, for $1 \leq i \leq g$. Thus by (2), we have $\mathcal{D}_{\bar{B}/\bar{A}} \neq 0$. But, in view of (1), this contradicts the assumption that $\mathcal{D}_{B/A} \subseteq \mathfrak{p}$. It follows that $\mathfrak{p}$ must be a ramified prime.

The final assertion about the number of ramified prime is an immediate consequence of the above characterization and the fact that $\mathcal{D}_{B/A}$ is a nonzero ideal of the Dedekind domain A. □

Corollary 3.28. *Let K be a number field. A rational prime p ramifies in K iff p divides d_K. In particular, only finitely many primes of $\mathbb{Z}$ ramify in K.*

3.5 Ramification in Galois Extensions

In the case of Galois extensions, the fundamental identity $\sum e_i f_i = n$, which was proved in Section 3.2, takes a particularly simple form. This short section is devoted to a proof of this simpler identity. The key idea in the proof is the "norm argument" in the Lemma below.

Lemma 3.29. *Let A be a normal domain, K its quotient field, L a Galois extension of K, B the integral closure of A, and $\mathfrak{p}$ a prime ideal of A. Then the primes of B lying over $\mathfrak{p}$ are conjugates of each other, i.e., for any prime ideals P, Q of B such that $P \cap A = \mathfrak{p} = Q \cap A$, we have $Q = \sigma(P)$ for some $\sigma \in \mathrm{Gal}(L/K)$. In particular, the number of prime ideals of B lying over $\mathfrak{p}$ is finite, and , in fact, $\leq [L : K]$.*

Proof. We use a similar reduction as in the proof of Theorem 3.22. Thus we note that if $S = A \setminus \mathfrak{p}$, then the integral closure of $A' = S^{-1}A$ in L is $B' = S^{-1}B$, and PB' and QB' are prime ideals of B' lying over $\mathfrak{p}A'$. Moreover if $QB' = \sigma(PB')$, for some $\sigma \in \mathrm{Gal}(L/K)$, then we clearly have

$$Q = QB' \cap B = \sigma(PB') \cap B = \sigma(PB') \cap \sigma(B) = \sigma(PB' \cap B) = \sigma(P).$$

So we assume without loss of generality that $\mathfrak{p}$ is a maximal ideal of A. Now since B/A is integral, Q and P are maximal ideals of B. Suppose $Q \neq \sigma(P)$ for any $\sigma \in \mathrm{Gal}(L/K)$. By Chinese Remainder Theorem, we can find some $x \in B$ such that

$$x \equiv 0 (\mathrm{mod}\, Q) \quad \text{and} \quad x \equiv 1 (\mathrm{mod}\, \sigma(P)) \ \ \forall \sigma \in \mathrm{Gal}(L/K).$$

Consider the norm

$$N_{L/K}(x) = \prod_{\sigma \in \mathrm{Gal}(L/K)} \sigma(x).$$

By Proposition 2.22, this lies in A and hence in $Q \cap A = \mathfrak{p}$. Now P is a prime ideal of B containing $\mathfrak{p}$, and thus it follows that $\sigma(x) \in P$ for some $\sigma \in \mathrm{Gal}(L/K)$. But this contradicts the choice of x. □

Corollary 3.30. *Let A be a normal domain, K its quotient field, L a finite separable extension of K, B the integral closure of A in L, and $\mathfrak{p}$ a prime ideal in A. Then there exists only a finite number of prime ideals in B lying over $\mathfrak{p}$.*

Proof. Let L' be a least Galois extension of K containing L and B' be the integral closure of A in L'. Suppose P and Q are distinct prime ideals in B lying over $\mathfrak{p}$. Since B' is integral over B, there exist prime ideals P' and Q' in B' lying over P and Q respectively. Clearly P' and Q' are distinct and they both lie over $\mathfrak{p}$. Hence, by Lemma 3.29, we get the desired result. □

Theorem 3.31. *Let A be a Dedekind domain, K its quotient field, L a Galois extension of K, B the integral closure of A, and $\mathfrak{p}$ a nonzero prime ideal of A. Then for the primes of B lying over $\mathfrak{p}$, the ramification indices are the same and the residue degrees are the same. In other words, we have*

$$\mathfrak{p}B = (P_1 P_2 \dots P_g)^e$$

where $P_1, \dots, P_g$ are distinct prime ideals of B, and $f(P_1/\mathfrak{p}) = \cdots = f(P_g/\mathfrak{p})$ $(= f$ say$)$. Moreover, if we let $n = [L : K]$, then we have

$$efg = n.$$

Proof. Let $\mathfrak{p}B = P_1^{e_1} \dots P_g^{e_g}$, where $P_1, \dots, P_g$ are distinct prime ideals of B, and let $f_i = f(P_i/\mathfrak{p})$ for $1 \le i \le g$. For any $\sigma \in \mathrm{Gal}(L/K)$, we clearly have $\sigma(\mathfrak{p}) = \mathfrak{p}$ and $\sigma(B) = B$, and hence $\sigma(\mathfrak{p}B) = \mathfrak{p}B$. By Lemma 3.29, for any i with $1 \le i \le g$, there exists $\sigma \in \mathrm{Gal}(L/K)$ such that $\sigma(P_i) = P_1$, and consequently, $B/P_i \simeq \sigma(B)/\sigma(P_i) = B/P_1$. Thus $e_i = e_1$ and $f_i = f_1$. Since we have already shown that $\sum_{i=1}^{g} e_i f_i = n$, the theorem follows. □

Remark 3.32. With the notation and assumptions as in Theorem 3.31, we see that the ramification index $e(P/\mathfrak{p})$ of a prime P of B lying over $\mathfrak{p}$ is independent of the choice of P. Thus it is sometimes denoted by $e_{\mathfrak{p}}$. Likewise, in the case of Galois extensions, the notation $f_{\mathfrak{p}}$ and $g_{\mathfrak{p}}$ is sometimes used.

3.6 Decomposition and Inertia Groups

The identity $efg = n$, proved in the last section, is a starting point of a beautiful theory of ramification of primes developed by Hilbert. Some basic aspects of this theory will be discussed in this section. In order to avoid repetition, we state below the notations and assumptions that will be used throughout this section.

Notation and Assumption: Let A be a Dedekind domain and K be its quotient field. Let L be a Galois extension of K and B be the integral closure of A in L. Let G denote the Galois group of L/K. Let $\mathfrak{p}$ be a nonzero prime ideal of A. Let $\bar{A} = A/\mathfrak{p}$. Assume that $\bar{A}$ is a perfect field.[9] Let $e = e_{\mathfrak{p}}$, $f = f_{\mathfrak{p}}$. and $g = g_{\mathfrak{p}}$.

Observe that $|G| = [L : K] = efg$. Also note that if P is any prime of B lying over $\mathfrak{p}$, then the set primes of B lying over $\mathfrak{p}$ is precisely $\{\sigma(P) : \sigma \in \mathrm{Gal}(L/K)\}$. Thus the Galois group G acts naturally on this set of g primes and the action is transitive.

Definition 3.33. Given any prime ideal P of B lying over $\mathfrak{p}$, the *decomposition group* of P w.r.t. L/K is defined to be the subgroup of G consisting of automorphisms σ such that $\sigma(P) = P$. It is denoted by $D_P(L/K)$ or simply by D_P or D if the reference to L/K and/or P is clear from the context. The fixed field of $D_P(L/K)$ is called the *decomposition field* of P w.r.t. L/K, and is denoted by K_D.

Note that $D_P(L/K)$ is the stabilizer of P for the natural action of G on the set of primes of B lying over $\mathfrak{p}$. Hence $|D_P(L/K)| = |G|/g = ef$. Thus $[L : K_D] = ef$ and $[K_D : K] = g$. Also note that if Q is any prime ideal of B lying over $\mathfrak{p}$, then $Q = \sigma(P)$ for some $\sigma \in G$, and we have

$$\tau \in D_Q(L/K) \Leftrightarrow \tau(\sigma(P)) = \sigma(P) \Leftrightarrow \sigma^{-1}\tau\sigma \in D_P(L/K)$$

and so $D_Q = \sigma D_P \sigma^{-1}$. Thus if D_P is a normal subgroup of G (which, for example, is the case if L/K is abelian), then it depends only on $\mathfrak{p}$ and it may be denoted by $D_{\mathfrak{p}}$.

Lemma 3.34. *Let P be a prime ideal of B lying over $\mathfrak{p}$, and $D = D_P(L/K)$ be its decomposition group. Let $A_D = B \cap K_D$ be the integral closure of A in K_D and let $P_D = P \cap A_D$. Then P is the only prime of B lying over P_D, and we have*

$$P_D B = P^e \quad \text{and} \quad f(P/P_D) = f.$$

[9] In number theoretic applications, $\bar{A}$ will usually be a finite field and thus this assumption is valid.

If D is a normal subgroup of G, then K_D/K is a Galois extension and $\mathfrak{p}A_D$ is a product of g distinct and conjugate primes of K_D with residue degree 1.

Proof. Since L/K_D is Galois, the set of primes of B lying over P_D is given by $\{\sigma(P) : \sigma \in \mathrm{Gal}(L/K_D)\} = \{P\}$. Further, if $e' = e(P/P_D)$ and $f' = f(P/P_D)$, then we know from Exercise 3.21 that $e'|e$ and $f'|f$. On the other hand, $e'f' = [L : K_D] = ef$. Hence $e' = e$ and $f' = f$. This proves our first assertion, and also it shows that $e(P_D/\mathfrak{p}) = 1$ and $f(P_D/\mathfrak{p}) = 1$. If D is normal, then clearly K_D/K is Galois and $e(P'/\mathfrak{p}) = 1 = f(P'/\mathfrak{p})$, for any prime P' of A_D lying over $\mathfrak{p}$. Since $[K_D : K] = g$, we obtain the desired result. □

For the remainder of this section, let us fix a prime P of B lying over $\mathfrak{p}$ and let $D = D_P(L/K)$. Let $\bar{B} = B/P$. Then $\bar{B}$ is a field extension of $\bar{A}$ of degree f. By our assumption, $\bar{B}/\bar{A}$ is separable. Now if $\sigma \in D$, then σ clearly induces an $\bar{A}$–automorphism $\bar{\sigma}$ of $\bar{B}$. We thus obtain a homomorphism

$$\epsilon : D \to \mathrm{Gal}(\bar{B}/\bar{A}) \qquad \text{defined by } \epsilon(\sigma) = \bar{\sigma}.$$

The kernel of ϵ is called the *inertia group* of P w.r.t. L/K and is denoted by $T_P(L/K)$ or simply by T_P or T. Clearly, T is a normal subgroup of D. Note that the inertia group can be alternatively defined as follows.

$$T_P(L/K) = \{\sigma \in G : \sigma(x) = x (\mathrm{mod}\ P) \text{ for all } x \in B\}.$$

The fixed field of T is called the *inertia field* of P w.r.t. L/K and is denoted by K_T. Observe that $K \subset K_D \subset K_T \subset L$, and K_T/K_D is a Galois extension with Galois group D/T. A better description of this group and its order is given by the following lemma.

Lemma 3.35. *The extension $\bar{B}/\bar{A}$ of residue fields is normal, and $\epsilon : D \to \mathrm{Gal}(\bar{B}/\bar{A})$ defines an isomorphism of D/T onto $\mathrm{Gal}(\bar{B}/\bar{A})$.*

Proof. Let $\bar{\alpha} \in B$ be any element, and $\alpha \in B$ be its representative. Let $f(X)$ be the minimal polynomial of α over K. Since $\alpha \in B$, $f(X) \in A[X]$. Moreover, since L/K is normal, L and hence B contains all the roots of $f(X)$. Now $f(\alpha) = 0$ and thus $\mathrm{Irr}(\bar{\alpha}, \bar{A})$ divides $\bar{f}(X)$, the reduction of $f(X)$ mod $\mathfrak{p}$. It follows that $\bar{B}$ contains all the roots of $\mathrm{Irr}(\bar{\alpha}, \bar{A})$. Thus $\bar{B}/\bar{A}$ is normal.

Next, we can find $\bar{\theta} \in \bar{B}$ such that $\bar{B} = \bar{A}(\bar{\theta})$ because $\bar{B}/\bar{A}$ is a finite separable extension. Let $\theta \in B$ be a representative of B. By Chinese Remainder Theorem, we can find some $\beta \in B$ such that for any $\sigma \in G$ we have

$$\beta \equiv \theta (\mathrm{mod}\ \sigma(P)) \text{ for } \sigma \in D \quad \text{and} \quad \beta \equiv 0 (\mathrm{mod}\ \sigma(P)) \text{ for } \sigma \notin D.$$

Clearly $\bar{\beta} = \bar{\theta}$ and thus $\bar{B} = \bar{A}(\bar{\beta})$. Let $\gamma \in \mathrm{Gal}(\bar{B}/\bar{A})$ be any element. As in the previous paragraph, we see that $\gamma(\bar{\beta})$ is the image of some conjugate of β. Thus $\gamma(\bar{\beta}) = \overline{\sigma(\beta)}$ for some $\sigma \in G$. If $\sigma \notin D$, then by the choice of β we have $\sigma(\beta) \in P$, i.e., $\gamma(\beta) = \overline{\sigma(\beta)} = \bar{0}$, which is impossible. It follows that $\gamma = \bar{\sigma} = \epsilon(\sigma)$. This proves the Theorem. □

Corollary 3.36. *We have* $|T| = e = [L : K_T]$ *and* $[K_T : K_D] = f$. *Further, if* $A_T = B \cap K_T$ *is the integral closure of* A *in* K_T *and* $P_T = P \cap A_T$, *then we have*

$$P_D A_T = P_T \quad \text{with} \quad f(P_T/P_D) = f \qquad \text{and} \qquad P_T B = P^e \quad \text{with} \quad f(P/P_T) = 1.$$

In particular, we see that $\mathfrak{p}$ *is unramified in* K_T.

Proof. Since $|D| = ef$ and $[\bar{B} : \bar{A}] = f$, it follows from Lemma 3.35 that $|T| = e = [L : K_T]$ and $[K_T : K_D] = f$. Now if we consider the extension L/K_T and the prime P lying over P_T (i.e., replace $K, A, \mathfrak{p}$ by K_T, A_T, P_T respectively), then we have $D_P(L/K_T) = T_P(L/K_T) = \mathrm{Gal}(L/K_T) = T$ and the above results show that $e(P/P_T) = e$ and $e(P/P_T)f(P/P_T) = e$. The desired result follows from this using the transitivity relations for ramification indices and residue degrees. □

Exercise 3.37. Let E be a subfield of L containing K and $A_E = B \cap E$ be the integral closure of A in E. Let $P_E = P \cap A_E$. Show that $D_P(L/E) = D_P(L/K) \cap \mathrm{Gal}(L/E)$ and $T_P(L/E) = T_P(L/K) \cap \mathrm{Gal}(L/E)$.

Exercise 3.38. Let H be the subgroup of G generated by the subgroups $T_P(L/K)$ as P varies over all nonzero prime ideals of B. Let E be the fixed field of H. Show that E/K is an unramified extension.

Exercise 3.39. For $n \geq 0$, define $G_n = \{\sigma \in G : \sigma(x) \equiv x (\mathrm{mod}\ P^{n+1})\}$. Show that G_n are subgroups of G with $G_0 = T$. Prove that $G_n = \{1\}$ for all sufficiently large n. Also show that G_0/G_1 is isomorphic to a subgroup of the multiplicative group of nonzero elements of $\bar{B} = B/P$, and therefore it is cyclic. Further show that for $n \geq 1$, G_n/G_{n+1} is isomorphic to a subgroup of the additive group $\bar{B}$. Deduce that the inertia group T is a solvable group.

Remark 3.40. Let $K_\mathfrak{p}$ be the completion of K w.r.t. the valuation of K corresponding to $\mathfrak{p}$ (whose valuation ring is $A_\mathfrak{p}$), and L_P be the completion of L w.r.t. the valuation of L corresponding to P. Then we know that L_P can be regarded as a field extension of $K_\mathfrak{p}$. Since $K_\mathfrak{p}$ is complete, there is only one prime of L_P lying over the prime (or the corresponding valuation) of $K_\mathfrak{p}$. And since the residue fields of these primes in the completions coincide with the residue fields $\bar{A}$ and $\bar{B}$ respectively, it follows that the residue degrees are the same. Hence using the Theorem proved in the last section, we see that the ramification index corresponding to $L_P/K_\mathfrak{p}$ is precisely e, and we have $ef = [L_P : K_\mathfrak{p}]$. Moreover, every element of the decomposition group $D = D_P(L/K)$ extends by continuity to an $K_\mathfrak{p}$–automorphism of L_P, and since $|D| = ef$, it follows that $\mathrm{Gal}(L_P/K_\mathfrak{p}) \simeq D_P(L/K)$. In particular, if P is unramified, then $T = \{1\}$ and thus D is isomorphic to $\mathrm{Gal}(\bar{B}/\bar{A})$. Furthermore, if $\bar{A}$ is finite (which is the case if K is a number field), then $\mathrm{Gal}(\bar{B}/\bar{A})$ is cyclic, and thus whenever P is unramified, we have $\mathrm{Gal}(L_P/K_\mathfrak{p}) \simeq \mathrm{Gal}(\bar{B}/\bar{A}) \simeq \mathrm{Gal}(\bar{L}_P/\bar{K}_\mathfrak{p})$, where $\bar{L}_P$ and $\bar{K}_\mathfrak{p}$ denote the residue fields of (the valuation rings of) L_P and $K_\mathfrak{p}$ respectively, so that the local Galois group $\mathrm{Gal}(L_P/K_\mathfrak{p})$ is cyclic. For more on these matters, see [17]

3.7 Quadratic and Cyclotomic Extensions

In this section we shall consider the examples of quadratic and cyclotomic fields and try to determine explicitly the splitting of rational primes when extended to these number fields.

Example 1: Quadratic Fields

Let K be a quadratic field. As noted earlier, we have $K = \mathbb{Q}(\sqrt{m})$, for some uniquely determined squarefree integer m (with $m \neq 0, 1$). Let $\mathcal{O}$ be the ring of integers of K. We have also seen that

$$\mathcal{O} = \begin{cases} \mathbb{Z}[\sqrt{m}] & \text{if } m \equiv 2, 3 (\text{mod } 4) \\ \mathbb{Z}[\frac{1+\sqrt{m}}{2}] & \text{if } m \equiv 1 (\text{mod } 4). \end{cases}$$

In particular, we see that the hypothesis of Kummer's Theorem 3.24 is satisfied.

Now let p be a rational prime. We are interested in the decomposition of the extended ideal $p\mathcal{O}$. The formula $\sum_{i=1}^{g} e_i f_i = n$ shows that g as well as e_i, f_i can only be 1 or 2, and that the situation has to be one of the following.

(i) $g = 2,\ e_1 = f_1 = e_2 = f_2 = 1$ so that $p\mathcal{O} = P_1 P_2$ for some distinct primes P_1, P_2 of $\mathcal{O}$ with $\mathcal{O}/P_i \simeq \mathbb{Z}/p\mathbb{Z}$. In this case, we say that p is a *decomposed* (or *split*) prime, or that p *decomposes* (or *splits*) in $\mathcal{O}$.

(ii) $g = 1,\ e_1 = 2,\ f_1 = 1$ so that $p\mathcal{O} = P^2$ for some prime P of $\mathcal{O}$ with $\mathcal{O}/P \simeq \mathbb{Z}/p\mathbb{Z}$. In this case p is a *ramified* prime.

(iii) $g = 1,\ e_1 = 1,\ f_1 = 2$ so that $p\mathcal{O} = P$ for some prime P of $\mathcal{O}$ with $[\mathcal{O}/P : \mathbb{Z}/p\mathbb{Z}] = 2$. In this case, we say that p is an *inertial* prime.

Now let's figure out which one is which. First we consider

Case 1: $m \not\equiv 1 (\text{mod } 4)$, i.e., $m \equiv 2, 3 (\text{mod } 4)$.

In this case, $\mathcal{O} = \mathbb{Z}[\sqrt{m}]$ and $f(X) = X^2 - m$ is the minimal polynomial of $\sqrt{m}$ over $\mathbb{Q}$. By Kummer's Theorem 3.24, the factorization of $p\mathcal{O}$ is determined by the factorization of $\bar{f}(X)$, the reduction of $f(X)$ modulo p. If $p|m$ or $p = 2$, then $\bar{f}(X) = X^2$ or $(X-1)^2$, and hence $(p)\mathcal{O} = P^2$, with $P = (p, \sqrt{m})$ or $P = (p, 1 - \sqrt{m})$, and p is ramified. If $p \not| m$ and $p \neq 2$, then $\bar{f}(X)$ is either irreducible in $(\mathbb{Z}/p\mathbb{Z})[X]$ or has two distinct roots in $\mathbb{Z}/p\mathbb{Z}$ (why?). The latter is the case if and only if m is a square mod p, i.e., $m \equiv x^2 (\text{mod } p)$ for some integer x. So we know which primes are decomposed and which are inertial. The result can be conveniently expressed using the *Legendre symbol*, which is defined thus.[10]

$$\left(\frac{m}{p}\right) = \begin{cases} 1 & \text{if } p \not| m \text{ and } m \text{ is a square mod } p \\ -1 & \text{if } p \not| m \text{ and } m \text{ is not a square mod } p \\ 0 & \text{if } p|m. \end{cases}$$

What we have shown so far is that if $m \equiv 2, 3 (\text{mod } 4)$, then

$$\text{the rational prime } p \text{ is } \begin{cases} \text{decomposed} & \text{if } p \neq 2 \text{ and } \left(\frac{m}{p}\right) = 1 \\ \text{ramified} & \text{if } p = 2 \text{ or } \left(\frac{m}{p}\right) = 0 \\ \text{inertial} & \text{if } p \neq 2 \text{ and } \left(\frac{m}{p}\right) = -1. \end{cases}$$

[10] It may be noted that the Legendre symbol can be effectively computed using its basic properties, viz., $\left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right)\left(\frac{b}{p}\right)$, $\left(\frac{a}{p}\right) = \left(\frac{b}{p}\right)$ if $a \equiv b (\text{mod } p)$, and the Gauss' Law of Quadratic Reciprocity which states that for any odd prime p, we have $\left(\frac{-1}{p}\right) = (-1)^{\frac{p-1}{2}}$, $\left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}}$, and last but not the least, $\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{\frac{p-1}{2}\frac{q-1}{2}}$, where q is any odd prime.

Now let's consider

Case 2: $m \equiv 1 (\text{mod } 4)$.

In this case, $\mathcal{O} = \mathbb{Z}\left[\frac{1+\sqrt{m}}{2}\right]$ and $f(X) = X^2 - X - \frac{m-1}{4}$ is the minimal polynomial of $\frac{1+\sqrt{m}}{2}$ over $\mathbb{Q}$. If $p = 2$, then $\bar{f}(X)$ has a root mod p iff $\frac{m-1}{4} \equiv 0 (\text{mod } 2)$, i.e., $m \equiv 1 (\text{mod } 8)$ [because $x^2 - x = x(x-1) \equiv 0 (\text{mod } 2)$ for any $x \in \mathbb{Z}$], and in this case, each of the two distinct elements in $\mathbb{Z}/2\mathbb{Z}$ is a root of $\bar{f}(X)$, which implies that 2 is a decomposed prime. If $p = 2$ and $m \not\equiv 1 (\text{mod } 8)$, then $\bar{f}(X)$ has to be irreducible in $(\mathbb{Z}/2\mathbb{Z})[X]$, and so 2 is an inertial prime. Now assume that $p \neq 2$. Then the "roots" $\frac{1 \pm \sqrt{m}}{2}$ of $X^2 - X - \frac{m-1}{4}$ will exist in $\mathbb{Z}/p\mathbb{Z}$ if and only if $\sqrt{m}$ exists in $\mathbb{Z}/p\mathbb{Z}$, or equivalently, m is a square mod p. Moreover, $\bar{f}(X)$ has multiple roots in $\mathbb{Z}/p\mathbb{Z}$ iff $p|m$. (Verify!) Thus, by Kummer's Theorem 3.24, we find that p is ramified iff $p|m$, and if $p \neq 2$ and $p \not| m$, then p is decomposed or inertial according as m is or is not a square mod p. So if $m \equiv 1 (\text{mod } 4)$, then

$$p \text{ is } \begin{cases} \text{decomposed} & \text{if } p = 2 \text{ and } m \equiv 1 (\text{mod } 8) \text{ or if } p \neq 2 \text{ and } \left(\frac{m}{p}\right) = 1 \\ \text{ramified} & \text{if } p|m, \text{ i.e., } \left(\frac{m}{p}\right) = 0 \\ \text{inertial} & \text{if } p = 2 \text{ and } m \not\equiv 1 (\text{mod } 8) \text{ or if } p \neq 2 \text{ and } \left(\frac{m}{p}\right) = -1. \end{cases}$$

Recall that the discriminant of the quadratic field $K = \mathbb{Q}(\sqrt{m})$ is given by

$$d_K = \begin{cases} 4m & \text{if } m \equiv 2, 3 (\text{mod } 4) \\ m & \text{if } m \equiv 1 (\text{mod } 4). \end{cases}$$

Now the above observations concerning ramified primes in K can be expressed in a unified manner as follows.

$$p \text{ is a ramified prime in } K \Leftrightarrow p|d_K.$$

This verifies the theorem of Dedekind, which was proved in Section 3.4.

Exercise 3.41. (Fermat's Two Square Theorem): Show that the ring of integers of the quadratic field $\mathbb{Q}(i)$, where $i^2 = -1$, is the ring $\mathbb{Z}[i]$ of Gaussian integers. Show that the decomposed primes are precisely the primes of the form $4k + 1$. Use this and the fact that $\mathbb{Z}[i]$ is a PID to show that any prime of the form $4k + 1$ can be written as a sum of two squares. Further, use the fact that primes of the form $4k + 3$ are inertial in $\mathbb{Z}[i]$ to show that any positive integer n, with $n = p_1^{e_1} \ldots p_h^{e_h}$ where $p_1, \ldots, p_h$ are distinct primes and $e_1, \ldots, e_h$ are positive integers, can be written as a sum of two squares if and only if e_i is even whenever $p_i \equiv 3 (\text{mod } 4)$.

Example 2: Cyclotomic Fields

Let p be an odd prime number and ζ be a primitive p–th root of unity. Let $\mathcal{O}$ be the ring of integers of the cyclotomic field $K = \mathbb{Q}(\zeta)$. We have noted earlier that the prime p is totally ramified in K. In fact, we have $(p)\mathcal{O} = P^{p-1}$ where P is the prime ideal of $\mathcal{O}$ generated by $(\zeta - 1)$. We also know that $d_K = (-1)^{\frac{p-1}{2}} p^{p-2}$. Hence p is the only ramified prime. (This fact can also be seen from Kummer's Theorem 3.24 which is applicable since $\mathcal{O} = \mathbb{Z}[\zeta]$). Let q be a rational prime different from p. Then $q\mathcal{O}$ is a product of g distinct prime ideals of $\mathcal{O}$. Let Q be a prime ideal of $\mathcal{O}$ lying over $q\mathbb{Z}$, and let $f = [\mathcal{O}/Q : \mathbb{F}_q] = (p-1)/g$, where $\mathbb{F}_q = \mathbb{Z}/q\mathbb{Z}$.

Then f (and hence g) can be determined as follows. If $\bar{\zeta}$ denotes the image of ζ in the field $\bar{\mathcal{O}} = \mathcal{O}/Q$, then we have $\bar{\mathcal{O}} = \mathbb{F}_q(\bar{\zeta})$ and $\bar{\zeta}^p = 1$. Thus $\bar{\zeta}$ is a nonzero element of $\bar{\mathcal{O}}^*$, which is a multiplicative group of order $q^f - 1$. So it follows that p divides $q^f - 1$, i.e., $q^f \equiv 1 (\mathrm{mod}\ p)$. Moreover, if for some $l < f$, $q^l \equiv 1 (\mathrm{mod}\ p)$, then $\bar{\zeta}$ would be in a field of q^l elements and hence this field have to contain $\bar{\mathcal{O}} = \mathbb{F}_q(\bar{\zeta})$, which is a contradiction. Therefore f is the least positive integer such that $q^f \equiv 1 (\mathrm{mod}\ p)$. In this way f and hence g is explicitly determined. The prime ideals lying above $q\mathbb{Z}$ can be determined by considering the factorization of $X^p - 1$ in $\mathbb{Z}/q\mathbb{Z}[X]$ by using Kummer's Theorem 3.24. For example, if $p = 7$ and $q = 5$, then we find that $f = 6$ and $g = 1$; moreover, $Q = (5, 1 + \zeta + \zeta^2 + \zeta^3 + \zeta^4 + \zeta^5 + \zeta^6) = (5)$ is the only prime ideal of $\mathcal{O}$ lying over $5\mathbb{Z}$.

Exercise 3.42. Let p, ζ and K be as above. Let H be the unique subgroup of index 2 in the cyclic group $\mathrm{Gal}(\mathbb{Q}(\zeta)/\mathbb{Q})$. The fixed field of H, say E, is a quadratic field. Show that $E = \mathbb{Q}(\sqrt{p^*})$ where $p^* = (-1)^{\frac{p-1}{2}} p$. Let q be an odd prime different from p, f be as above, and let $g = \frac{p-1}{f}$. Show that q decomposes in E iff $\left(\frac{p^*}{q}\right) = 1$. Next, if q decomposes in E, then show that g is even and $\left(\frac{q}{p}\right) = 1$. [You may use the elementary fact that $\left(\frac{a}{p}\right) \equiv a^{\frac{p-1}{2}} (\mathrm{mod}\ p)$.] Conversely, if g is even, then show that the decomposition field of q contains E, and so q decomposes in E. Further, if g is odd, then use the minimality of f to show that $\left(\frac{q}{p}\right) = -1$. Deduce from all this that $\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{\frac{(p-1)}{2}\frac{(q-1)}{2}}$.

Chapter 4

Class Number and Lattices

In this chapter, we will concentrate on the case of (algebraic) number fields. We shall see how number fields give rise to lattices in $\mathbb{R}^n$ in a natural way. We will then prove some results of Minkowski concerning lattices and deduce some of its number-theoretic consequences. In particular, we will show that the class number of any number field is always finite, and also that in any number field other than $\mathbb{Q}$, some prime (of $\mathbb{Z}$) is always ramified.

4.1 Norm of an ideal

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

To every nonzero fractional ideal J of A, we associate a nonzero rational number, denoted $\mathsf{N}(J)$, and called the *norm* of J, as follows. For a nonzero prime ideal $\mathfrak{p}$ of A, we define

$$\mathsf{N}(\mathfrak{p}) = p^f \quad \text{if } p \in \mathbb{Z} \text{ is such that } \mathfrak{p} \cap \mathbb{Z} = p\mathbb{Z} \text{ and } f = f(\mathfrak{p}/p\mathbb{Z}) = [A/\mathfrak{p} : \mathbb{Z}/p\mathbb{Z}].$$

This definition is extended to nonzero fractional ideals by multiplicativity. Thus, if $J \in \mathcal{F}_A$ and if $J = \mathfrak{p}_1^{e_1} \cdots \mathfrak{p}_h^{e_h}$ is its factorization as in Theorem 3.11, then

$$\mathsf{N}(J) = p_1^{e_1 f_1} \cdots p_h^{e_h f_h}, \quad \text{if } p_1, \ldots, p_h \in \mathbb{Z} \text{ are such that } \mathfrak{p}_i \cap \mathbb{Z} = p_i\mathbb{Z} \text{ and } f_i = f(\mathfrak{p}_i/p_i\mathbb{Z}).$$

It is clear that N is multiplicative, i.e., $\mathsf{N}(J_1 J_2) = \mathsf{N}(J_1)\mathsf{N}(J_2)$ for any $J_1, J_2 \in \mathcal{F}_A$; moreover,

$$J \text{ is an integral ideal of } A \Longrightarrow \mathsf{N}(J) \in \mathbb{Z}, \quad \text{for any } J \in \mathcal{F}_A.$$

If $\mathfrak{p}$ is a nonzero prime ideal of A lying over $p\mathbb{Z}$ and $f = f(\mathfrak{p}/p\mathbb{Z})$, then as in the proof of Theorem 3.22, we see that for any positive integer e, $A/\mathfrak{p}^e$ is isomorphic to e copies of $A/\mathfrak{p}$, as a vector space over $\mathbb{Z}/p\mathbb{Z}$. Thus, $\mathsf{N}(\mathfrak{p}^e) = p^{ef} = |A/\mathfrak{p}^e|$. Using this and the Chinese Remainder Theorem, we see that

$$\mathsf{N}(I) = |A/I|, \quad \text{for any nonzero integral ideal } I \text{ of } A.$$

Thus, from (2.3), we obtain the following important relation between the ideal norm and the discriminant:

$$\Delta(I) = \mathsf{N}(I)^2 d_K \quad \text{for any nonzero integral ideal } I \text{ of } A. \tag{4.1}$$

The ideal norm behaves just like the norm of an element w.r.t. $K/\mathbb{Q}$ when we pass from K to a larger number field L. More precisely, if L/K is a finite extension, $J \in \mathcal{F}_A$ and $B = \mathcal{O}_L$, then $JB \in \mathcal{F}_B$ and from the transitivity relations in Exercise 3.21, it is readily seen that

$$\mathsf{N}(JB) = \mathsf{N}(J)^{[L:K]}. \tag{4.2}$$

The following proposition shows that in the case of principal fractional ideals the ideal norm is essentially the same as the norm of a generator.

Proposition 4.1. *If xA the principal fractionary ideal of A generated by $x \in K$, $x \neq 0$, then*

$$\mathsf{N}(xA) = |N_{K/\mathbb{Q}}(x)|.$$

Proof. Let L be a normal closure of K so that L is a finite extension of K such that $L/\mathbb{Q}$ is Galois. From (4.2) and elementary properties of the norm of an element, we have

$$\mathsf{N}(xB) = \mathsf{N}(xA)^{[L:K]} \quad \text{and} \quad N_{L/\mathbb{Q}}(x) = N_{K/\mathbb{Q}}(x)^{[L:K]}$$

where $B = \mathcal{O}_L$ is the ring of integers of L. Hence it suffices to show that $\mathsf{N}(xB) = |N_{L/\mathbb{Q}}(x)|$. With this in view, we may assume without loss of generality that $K/\mathbb{Q}$ is a Galois extension.

Now, suppose $\mathfrak{p}$ is a nonzero prime ideal of A. Let $p \in \mathbb{Z}$ be such that $\mathfrak{p} \cap \mathbb{Z} = p\mathbb{Z}$ and let $e = e(\mathfrak{p}/p\mathbb{Z})$ and $f = f(\mathfrak{p}/p\mathbb{Z})$. If $P_1, \ldots, P_g$ are the prime ideals of A lying over $p\mathbb{Z}$ (with, say, $P_1 = \mathfrak{p}$), then from Lemma 3.29 and Theorem 3.31, it is clear that

$$\mathsf{N}(\mathfrak{p})A = p^f A = (pA)^f = (P_1 \cdots P_g)^{ef} = \prod_{\sigma \in \mathrm{Gal}(K/\mathbb{Q})} \sigma(\mathfrak{p}). \tag{4.3}$$

Note that since A is integral over $\mathbb{Z}$, we have $mA \cap \mathbb{Z} = m\mathbb{Z}$. for any $m \in \mathbb{Z}$. Thus, to prove the proposition, it suffices to show that the integers $\mathsf{N}(xA)$ and $N_{K/\mathbb{Q}}(x)$ generate the same ideal in A. Let $xA = \mathfrak{p}_1^{e_1} \cdots \mathfrak{p}_h^{e_h}$ be the factorization of xA as a product of powers of distinct prime ideals of A. Then, $\mathsf{N}(xA)A = (\mathsf{N}(\mathfrak{p}_1)A)^{e_1} \cdots (\mathsf{N}(\mathfrak{p}_h)A)^{e_h}$, and so from (4.3), we see that

$$\mathsf{N}(xA)A = \prod_{i=1}^{h} \left(\prod_{\sigma \in G} \sigma(\mathfrak{p}_i) \right)^{e_i} = \prod_{\sigma \in G} \sigma \left(\prod_{i=1}^{h} \mathfrak{p}_i^{e_i} \right) = \prod_{\sigma \in G} \sigma\,(xA) = \left(\prod_{\sigma \in G} \sigma(x) \right) A = N_{K/\mathbb{Q}}(x)A$$

where $G = \mathrm{Gal}(K/\mathbb{Q})$ denotes the Galois group of K over $\mathbb{Q}$. This completes the proof. □

We shall use the notion of ideal norm to prove the finiteness of the class number of K. A basic observation is the following.

Lemma 4.2. *If every ideal class of K contains an integral ideal I with $\mathsf{N}(I) \leq C$, where C is a positive real number independent of I (but may depend on K), then $\mathcal{C}_K$ is finite.*

Proof. It suffices to show that that the number of nonzero ideals I of A with $\mathsf{N}(I) = m$ is finite, for any positive integer m. Now, if $\mathsf{N}(I) = m$, then the additive abelian group A/I has order m and thus $ma \in I$ for all $a \in A$. In particular, I contains $m\mathbb{Z}$. But from Theorem 3.22, it is clear that there are only finitely many ideals of A containing $m\mathbb{Z}$. □

In section 4.4, we use some results of Minkowski to obtain an explicit value of C for which Lemma 4.2 holds. A crude bound can, however, be obtained by a less intricate argument as shown in the book of Marcus [13, Ch. 5]. We outline it here as an exercise.

Exercise 4.3. Let $\{u_1, \ldots, u_n\}$ be an integral basis of A. Also, let $u_i^{(1)}, \ldots, u_i^{(n)}$ denote the conjugates of u_i w.r.t. $K/\mathbb{Q}$, for $1 \leq i \leq n$.

(i) Given any nonzero ideal I of A, let $m = \left[\mathsf{N}(I)^{1/n}\right]$ be the integer part of $\mathsf{N}(I)^{1/n}$. Show that there are $(m+1)^n$ elements of the form $\sum_{i=1}^n m_i u_i$ where $m_i \in \mathbb{Z}$ with $0 \leq m_i \leq m$. Deduce that I contains a nonzero element x such that $x = \sum_{i=1}^n m_i u_i$ where $m_i \in \mathbb{Z}$ with $|m_i| \leq m$.

(ii) Show that if x is as in (i) above, then

$$|N_{K/\mathbb{Q}}(x)| \leq C\,\mathsf{N}(I) \quad \text{where } C = \prod_{j=1}^{n} \sum_{i=1}^{n} |u_i^{(j)}|.$$

(iii) Show that every ideal class of K contains an ideal I' of A such that $\mathsf{N}(I') \leq C$, where C is as in (ii) above. Deduce that $\mathcal{C}_K$ is finite.

4.2 Embeddings and Lattices

Let K be a number field and let $n = [K : \mathbb{Q}]$. Since $K/\mathbb{Q}$ is separable and a normal closure of K can be found in $\mathbb{C}$ (in fact $\mathbb{C}$ also contains an algebraic closure of K), it follows that there are exactly n distinct $\mathbb{Q}$-homomorphisms of $K \to \mathbb{C}$. These homomorphisms are called the *embeddings* of K (in $\mathbb{C}$). If an embedding $\sigma : K \to \mathbb{C}$ is such that $\sigma(K) \subseteq \mathbb{R}$, then it is called a *real embedding*; otherwise it is called a *complex embedding*. Note that the word 'complex' is used here in the sense of 'non-real'. In particular, if $\sigma : K \to \mathbb{C}$ is a complex embedding, then $\bar{\sigma} : K \to \mathbb{C}$ defined by

$$\bar{\sigma}(u) = \overline{\sigma(u)} = \text{ the complex conjugate of } \sigma(u), \qquad \text{for } u \in K,$$

is an embedding of K different from σ. It follows that the number of complex embeddings of K is even. We usually denote the number of real embeddings of K by r (or by r_1) and the number of complex embeddings of K by $2s$ (or by $2r_2$). We have $r + 2s = n$. In case $s = 0$, the field K is said to be *totally real*.

Example 4.4. For $K = \mathbb{Q}(\sqrt{2})$, we have $r = 2$ and $s = 0$, since any embedding is of the form $a + b\sqrt{2} \mapsto a \pm b\sqrt{2}$. Thus $\mathbb{Q}(\sqrt{2})$ is a totally real field. On the other hand, for $K = \mathbb{Q}(i)$, we have $r = 0$ and $s = 1$. For the cubic field $K = \mathbb{Q}(\sqrt[3]{2})$, we have $r = 1$ and $s = 1$, and the embeddings of K are essentially given by $\sqrt[3]{2} \mapsto \sqrt[3]{2}$, $\sqrt[3]{2} \mapsto \omega\sqrt[3]{2}$ and $\sqrt[3]{2} \mapsto \omega^2\sqrt[3]{2}$, where ω denotes a primitive cube root of unity.

A subset L of $\mathbb{R}^n$ such that

$$L = \mathbb{Z}v_1 + \cdots + \mathbb{Z}v_n$$

for some $\mathbb{R}$-basis $\{v_1, \ldots, v_n\}$ of $\mathbb{R}^n$, is called a *lattice* in the Euclidean space $\mathbb{R}^n$. We call the set

$$P = \{\lambda_1 v_1 + \cdots + \lambda_n v_n : 0 \leq \lambda_i < 1 \text{ for } i = 1, \ldots, n\}$$

a *fundamental parallelotope* of L (w.r.t. the $\mathbb{Z}$-basis $\{v_1, \ldots, v_n\}$ of L). Note that $\mathbb{R}^n$ is covered by the translates of P by elements of L, i.e.,

$$\mathbb{R}^n = \coprod_{x \in L} x + P \tag{4.4}$$

where $\coprod$ denotes disjoint union.

It is clear that any lattice can be transformed to $\mathbb{Z}^n$ by an invertible linear transformation of $\mathbb{R}^n$, say T. If T' is another such linear transformation, then T and T' differ by an invertible linear transformation if $\mathbb{Z}^n$, or in other words, by an element of $GL_n(\mathbb{Z})$. In particular, $\det T = \pm \det T'$, and thus the absolute value $|\det T|$ is independent of choice of T. We call this absolute value the *volume* of L, and denote it by $\mathrm{Vol}(\mathbb{R}^n/L)$. Note that the volume of L is a positive real number. Moreover, from the Change of Variables formula for n-fold integrals, we readily see that the notion of the volume of a lattice L is related to the classical notion of volume of subsets of $\mathbb{R}^n$ by the formula

$$\mathrm{Vol}(\mathbb{R}^n/L) = \mathrm{vol}(P),$$

where P is a fundamental parallelotope of L and $\mathrm{vol}(P)$ denotes its volume as a subset of $\mathbb{R}^n$. Recall that for any measurable subset E of $\mathbb{R}^n$, the volume of E is defined by

$$\mathrm{vol}(E) = \int_E d\mu$$

where μ denotes the Lebesgue measure on $\mathbb{R}^n$. Note that if E is compact or contained in a compact set, then $\mathrm{vol}(E) < \infty$. Also note that if $E' = \lambda E := \{\lambda x : x \in E\}$, then E' is measurable and $\mathrm{vol}(E') = \lambda^n \mathrm{vol}(E)$.

The following result shows how number fields generate lattices, and also how their volume can be computed.

Proposition 4.5. *Let K be a number field of degree n over $\mathbb{Q}$. Let $\sigma_1, \ldots, \sigma_r$ be the real embeddings and $\tau_1, \ldots, \tau_s, \bar{\tau}_1, \ldots, \bar{\tau}_s$ be the complex embeddings of K. Define $f : K \to \mathbb{R}^n$ by,*

$$f(u) = (\sigma_1(u), \ldots, \sigma_r(u), \mathrm{Re}\tau_1(u), \ldots, \mathrm{Re}\tau_s(u), \mathrm{Im}\bar{\tau}_1(u), \ldots, \mathrm{Im}\bar{\tau}_s(u)) \quad \text{for } u \in K.$$

Then f is injective and the image of $\mathcal{O}_K$ under f is a lattice L_K in $\mathbb{R}^n$. In particular K embeds densely in $\mathbb{R}^n$. Moreover, if d_K denotes the (absolute) discriminant of K, then

$$\mathrm{Vol}\,(\mathbb{R}^n/L_K) = \frac{\sqrt{|d_K|}}{2^s}.$$

More generally, if I is any nonzero ideal of $\mathcal{O}_K$, then $f(I)$ is a lattice L_I in $\mathbb{R}^n$ and

$$\mathrm{Vol}\,(\mathbb{R}^n/L_I) = \frac{\sqrt{|d_K|}}{2^s}\mathsf{N}(I).$$

Proof. Let $\{u_1, \ldots, u_n\}$ be an integral basis of $\mathcal{O}_K$. The conjugates of u_i w.r.t. $K/\mathbb{Q}$ are precisely given by $\sigma_1(u), \ldots, \sigma_r(u), \tau_1(u), \ldots, \tau_s(u), \bar{\tau}_1(u), \ldots, \bar{\tau}_s(u)$. Thus from the expression for $D_{L/K}(u_1, \ldots, u_n)$ in the proof of Theorem 1.11, we see that

$$d_K = \begin{vmatrix} \sigma_1(u_1) & \ldots & \sigma_r(u_1) & \tau_1(u_1) & \ldots & \tau_s(u_1) & \bar{\tau}_1(u_1) & \ldots & \bar{\tau}_s(u_1) \\ \vdots & & & & & & & & \vdots \\ \sigma_1(u_n) & \ldots & \sigma_r(u_n) & \tau_1(u_n) & \ldots & \tau_s(u_n) & \bar{\tau}_1(u_n) & \ldots & \bar{\tau}_s(u_n) \end{vmatrix}^2.$$

Now, in the $n \times n$ matrix above, let us make the following elementary column operations. First, we add the the $(r+s+j)$-th column to the $(r+j)$-th column for $1 \leq j \leq s$. Next, we multiply the resulting $(r+j)$-th column by $1/2$ and subtract it from the $(r+s+j)$-th column for $1 \leq j \leq s$. As a consequence, we see that

$$d_K = (-1)^s 2^{2s} \left[\det\left(f_i(u_j)\right)\right]^2 \quad \text{and} \quad \sqrt{|d_K|} = 2^s \left|\det\left(f_i(u_j)\right)\right|$$

where $f_1, \ldots, f_n$ denote the coordinate functions of f. In particular, the determinant on the right is nonzero, and thus the vectors $f(u_1), \ldots, f(u_n)$ in $\mathbb{R}^n$ are linearly independent. It follows that f is injective and $L_K = f(\mathcal{O}_K)$ is a lattice in $\mathbb{R}^n$ with $\mathrm{Vol}\left(\mathbb{R}^n/L_K\right) = 2^{-s}\sqrt{|d_K|}$. The assertion about K being densely embedded in $\mathbb{R}^n$ follows since $f(K)$ contains the $\mathbb{Q}$-span of $f(u_1), \ldots, f(u_n)$.

In the more general case when I is a nonzero ideal of $\mathcal{O}_K$ and $L_I = f(I)$, we can proceed as before but with $\{u_1, \ldots, u_n\}$ replaced by an integral basis of I so that d_K is replaced by $\Delta(I)$. The desired formula for $\mathrm{Vol}(\mathbb{R}^n/L_I)$ is then a consequence of (4.1). □

Remark 4.6. 1. The above proof shows that the sign of the discriminant of a number field with $2s$ complex embeddings is given by $(-1)^s$. This result is sometimes called Brill's Discriminant Theorem.

2. From Proposition 4.5, it is immediate that $\mathsf{N}(I) = \mathrm{Vol}(\mathbb{R}^n/L_I)/\mathrm{Vol}(\mathbb{R}^n/L_K)$. Sometimes the norm of an ideal is defined this way as the quotient of the volumes of lattices L_I and L_K. In this case, proving the multiplicativity of ideal norm requires some effort. For an approach along these lines, see, for example, the recent book of Swinnerton-Dyer [16].

Definition 4.7. A subset S of $\mathbb{R}^n$ is called *symmetric* if $0 \in S$ and moreover, $-x \in S$ whenever $x \in S$.

Lemma 4.8. *let L be a lattice in $\mathbb{R}^n$ and S be a convex, measurable, symmetric subset of $\mathbb{R}^n$ such that $\mathrm{vol}(S) > 2^n \mathrm{Vol}(\mathbb{R}^n/L)$. Then S contains a nonzero point of L. In case S is also compact, then S contains a nonzero point of L even when $\mathrm{vol}(S) = 2^n \mathrm{Vol}(\mathbb{R}^n/L)$.*

Proof. Let P be a fundamental parallelotope for L. Then from (4.4), we see that given any measurable subset E of $\mathbb{R}^n$, we have $E = \coprod_{x \in L} E \cap (x+P)$. Therefore,

$$\mathrm{vol}(E) = \sum_{x \in L} \mathrm{vol}\left(E \cap (x+P)\right) = \sum_{x \in L} \mathrm{vol}\left((E-x) \cap P\right). \tag{4.5}$$

Now, consider $E = \frac{1}{2}S$. We have

$$\mathrm{vol}(E) = \frac{1}{2^n}\mathrm{vol}(S) > \mathrm{Vol}(\mathbb{R}^n/L) = \mathrm{vol}(P). \tag{4.6}$$

Hence, if the sets $(E-x) \cap P$ were all disjoint, as x varies over L, then the rightmost expression in (4.5) would be $\leq \mathrm{vol}(P)$, which contradicts (4.6). Therefore, there exist $a, b \in S$ and $p \in P$ such that $p = \frac{1}{2}a - x = \frac{1}{2}b - y$ for some $x, y \in L$, $x \neq y$. It follows that $0 \neq x - y = \frac{1}{2}a + \frac{1}{2}(-b) \in S \cap L$.

In case S is compact, we consider $S_n = S + \frac{1}{n}S$, and obtain nonzero points $x_n \in S_n \cap L$ from the previous case. Note that $S_n = \left(1 + \frac{1}{n}\right) S \subseteq 2S$ because S is convex and $0 \in S$. Thus, $x_n \in 2S \cap L$ for all $n \geq 1$. But $2S \cap L$ is finite since S is compact. Therefore, the sequence (x_n) has a constant subsequence, whose limit is in the closure of S, which is S itself. □

Remark 4.9. The above lemma is sometimes referred to as Minkowski's Convex Body Theorem. It is a key result in Minkowski's geometric approach to the theory of numbers. A leisurely discussion of this result along with several applications as well as references to alternative proofs and further developments, can be found in the recent book of Olds, Lax and Davidoff [14]. The exercise below gives two such applications. The first is an elementary theorem of Dirichlet, which may be regarded as a starting point for the theory of Diophantine Approximation (and in particular, the study of continued fractions). The second result is the celebrated Four Square Theorem, first proved by Lagrange in 1770. Classical proofs of Dirichlet's Theorem (using Pigeonhole principle) and Lagrange's Theorem (using Fermat's method of infinite descent) can be found in the book of Baker [2]. The applications of Minkowski's Convex Body Theorem with which we shall be concerned, appear after the exercises and in the subsequent sections.

Exercises 4.10. 1. Given any real number θ and any integer $Q > 1$ show that there exist integers p, q with $0 < q < Q$ and $|q\theta - p| \leq 1/Q$. [Hint: Let $L = \mathbb{Z}^2$ and S be the parallelogram bounded by the lines $x = \pm Q$ and $y - \theta x = \pm 1/Q$, and use Lemma 4.8.]

2. Let p be an odd prime. First, show that there exist integers a, b such that $p|a^2 + b^2 + 1$. [Hint: The numbers a^2 with $0 \leq a \leq (p-1)/2$ are mutually incongruent (mod p), and the same holds for the numbers $-1 - b^2$ with $0 \leq b \leq (p-1)/2$.] Next, show that p is a sum of squares of four integers. [Hint: Let $L \subset \mathbb{R}^4$ be the lattice spanned by $(m, 0, a, b), (0, m, b, -a), (0, 0, 1, 0)$ and $(0, 0, 0, 1)$, and S be the open disc in $\mathbb{R}^4$ centered at origin and of radius $\sqrt{2m}$, and use Lemma 4.8.] Finally, use the trivial representation $2 = 1^2 + 1^2 + 0^2 + 0^2$ and Euler's identity

$$\begin{aligned}&(x^2 + y^2 + z^2 + w^2)(x'^2 + y'^2 + z'^2 + w'^2)\\ &= (xx' + yy' + zz' + ww')^2 + (xy' - yx' + wz' - zw')^2\\ &+ (xz' - zx' + yw' - wy')^2 + (xw' - wx' + zy' - yz')^2\end{aligned}$$

to deduce that every positive integer is a sum of four squares.

Let n be a positive integer and r, s be nonnegative integers such that $r + 2s = n$. We define the (r, s)-*norm* of any $x = (x_1, \ldots, x_n) \in \mathbb{R}^n$ by

$$\mathcal{N}_{r,s}(x) = x_1 \cdots x_r \left(x_{r+1}^2 + x_{r+s+1}^2\right) \cdots \left(x_{r+s}^2 + x_n^2\right).$$

Observe that if K is a number field of degree n and r, s have their usual meaning, then for any $u \in K$ we have $N_{K/\mathbb{Q}}(u) = \mathcal{N}_{r,s}(f(u))$, where f denotes the injection of K in $\mathbb{R}^n$ given by Lemma 4.5.

Corollary 4.11. *Let n be a positive integer and r, s be nonnegative integers such that $r+2s = n$. If Ω is a compact, convex, symmetric subset of $\mathbb{R}^n$ such that*

$$\mathrm{vol}(\Omega) > 0 \quad \text{and} \quad |\mathcal{N}_{r,s}(a)| \leq 1 \text{ for all } a \in \Omega,$$

then every lattice L in $\mathbb{R}^n$ contains a nonzero vector x such that

$$|\mathcal{N}_{r,s}(x)| \leq 2^n \frac{\mathrm{Vol}(\mathbb{R}^n/L)}{\mathrm{vol}(\Omega)}.$$

Proof. Apply Lemma 4.8 with $S = \lambda\Omega$, where $\lambda = 2\sqrt[n]{\mathrm{Vol}(\mathbb{R}^n/L)/\mathrm{vol}(\Omega)}$. □

4.3 Minkowski's Theorem

We will now use the machinery developed in the previous section to prove the following important result of Minkowski.

Theorem 4.12 (Minkowski). *Let n be a positive integer and r, s be nonnegative integers such that $r + 2s = n$. If L is any lattice in $\mathbb{R}^n$, then L contains a nonzero vector x such that*

$$|\mathcal{N}_{r,s}(x)| \leq \frac{n!}{n^n} \left(\frac{8}{\pi}\right)^s \mathrm{Vol}(\mathbb{R}^n/L).$$

Proof. For any positive real number t, let $\Omega_t = \Omega_t(r, s)$ denote the set

$$\{(x_1, \ldots, x_n) \in \mathbb{R}^n : \sum_{i=1}^{r} |x_i| + 2 \sum_{j=r+1}^{r+s} \sqrt{x_j^2 + x_{j+s}^2} \leq t\}.$$

It is clear that Ω_t is a compact and symmetric subset of $\mathbb{R}^n$. Further, from the Cauchy-Schwartz inequality, we see that

$$\sqrt{(a+c)^2 + (b+d)^2} \leq \sqrt{a^2 + b^2} + \sqrt{c^2 + d^2} \quad \text{for any } a, b, c, d \in \mathbb{R}$$

and this, in turn, implies that if $x, y \in \Omega_t$ and $\lambda \in \mathbb{R}$ with $0 \leq \lambda \leq 1$, then $\lambda x + (1 - \lambda)y \in \Omega_t$. Thus Ω_t is convex. Now let $t = n$. By applying the AM-GM inequality to the n numbers $|x_1|, \ldots, |x_r|, \sqrt{x_{r+1}^2 + x_{r+s+1}^2}, \sqrt{x_{r+2}^2 + x_{r+s+2}^2}, \ldots, \sqrt{x_{r+s}^2 + x_n^2}$, we see that

$$|\mathcal{N}_{r,s}(x)| \leq 1 \quad \text{for all } x \in \Omega_n.$$

Now the desired result follows at once by applying Corollary 4.11 to $\Omega = \Omega_n$ if we prove the following.

$$\mathrm{vol}(\Omega_t) = t^n 2^r \left(\frac{\pi}{2}\right)^s \frac{1}{n!}. \tag{4.7}$$

To prove (4.7), let $V_{r,s}(t) = \mathrm{vol}(\Omega_t(r, s))$. Since $\Omega_t = t\Omega_1$, we have $V_{r,s}(t) = t^n V_{r,s}(1) = t^{r+2s} V_{r,s}(1)$. We now calculate $V_{r,s}(1)$ using double induction on r and s. First, if $r > 0$, then from the definitions of $\Omega_t(r, s)$ and $V_{r,s}(t)$, we see that

$$\begin{aligned} V_{r,s}(1) &= \int_{-1}^{1} V_{r-1,s}(1 - |x|)dx \\ &= 2\int_{0}^{1} V_{r-1,s}(1)(1 - x)^{r-1+2s} dx \\ &= \frac{2}{r + 2s} V_{r-1,s}(1). \end{aligned}$$

Thus by induction on r, we obtain

$$V_{r,s}(1) = \frac{2^r}{(r + 2s)(r - 1 + 2s) \cdots (1 + 2s)} V_{0,s}(1).$$

Next, if $s > 0$, then

$$\begin{aligned} V_{0,s}(1) &= \iint_{x^2+y^2\le 1/2} V_{0,s-1}(1-2\sqrt{x^2+y^2})\,dx\,dy \\ &= \int_0^{2\pi}\int_0^{1/2} V_{0,s-1}(1-2\rho)\rho\,d\rho\,d\theta \\ &= \int_0^{2\pi}\int_0^{1/2} V_{0,s-1}(1)(1-2\rho)^{2s-2}\rho\,d\rho\,d\theta \\ &= 2\pi V_{0,s-1}(1)\frac{1}{4(2s)(2s-1)}. \end{aligned}$$

Thus using induction on s and by noting that $V_{0,1}(1) = \iint_{x^2+y^2\le 1/2} dx\,dy = \frac{\pi}{2}\frac{1}{2}$, we see that $V_{0,s}(1) = (\pi/2)^s(1/(2s)!)$, and hence

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

This implies (4.7), and thus the theorem is proved. □

4.4 Finiteness of Class Number and Ramification

Theorem 4.13. *Let K be a number field with $[K:\mathbb{Q}] = n$ and let d_K be its (absolute) discriminant. Suppose K has $2s$ complex embeddings. Then every ideal class of K contains an ideal of I of A such that*

$$\mathsf{N}(I) \le \frac{n!}{n^n}\left(\frac{4}{\pi}\right)^s\sqrt{|d_K|}. \tag{4.8}$$

Consequently, the ideal class group $\mathcal{C}_K$ of K is finite.

Proof. Let I' be an integral ideal in a given ideal class of K. If $J' = (I')^{-1}$, then J' is a fractional ideal but we can find $d \in A$, $d \neq 0$ such that $J := \frac{1}{d}J'$ is an integral ideal. Now, consider the map $f : K \to \mathbb{R}^n$ defined in Proposition 4.5, and let $L_J = f(J)$ be the lattice in $\mathbb{R}^n$ corresponding to I. Applying Minkowski's Theorem 4.12 to the lattice L_J, we see that there exists $u \in J$ such that $u \neq 0$ and

$$\mathsf{N}(Au) = |N_{K/\mathbb{Q}}(u)| = |\mathcal{N}_{r,s}(f(u))| \le \frac{n!}{n^n}\left(\frac{8}{\pi}\right)^s \mathrm{Vol}(\mathbb{R}^n/L_J) = \frac{n!}{n^n}\left(\frac{4}{\pi}\right)^s\sqrt{|d_K|}\,\mathsf{N}(J).$$

where the last equality follows from Proposition 4.5. Using the multiplicativity of ideal norm, we see that if $I := (u)J^{-1}$, then

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

Moreover, $I = (ud)I'$ and thus I is an integral ideal in the given ideal class. This proves the desired inequality. The last assertion follows Lemma 4.2. □

In the examples below, we show how Minkowski's Theorem can be effectively used to determine the class number in several cases.

Examples 4.14. 1. Let $K = \mathbb{Q}(\sqrt{5})$. Then $n = 2$. $s = 0$ and $d_K = 5$. Thus the Minkowski's inequality (4.8) reduces to

$$\mathsf{N}(I) \leq \frac{2!}{2^2}\sqrt{5} = \frac{\sqrt{5}}{2} < 2.$$

Thus every ideal class contains an ideal I of A with $\mathsf{N}(I) = 1$, i.e., $I = A$. It follows that $\mathcal{C}_K$ is trivial and $h_K = 1$. Notice that a similar argument will show that if $K = \mathbb{Q}(\sqrt{2})$ or $\mathbb{Q}(\sqrt{3})$, then $h_K = 1$.

2. Let $K = \mathbb{Q}(\sqrt{-5})$. Then $n = 2$. $s = 1$ and $d_K = -20$. Thus the Minkowski's inequality (4.8) reduces to

$$\mathsf{N}(I) \leq \frac{2!}{2^2}\left(\frac{4}{\pi}\right)\sqrt{20} = \frac{2\sqrt{20}}{\pi} = 2.84\ldots\ .$$

Now if $\mathsf{N}(I) = 2$, then I must be a prime ideal lying over $2\mathbb{Z}$ and with residue degree 1. Since $2\mathcal{O}_K = (2, 1+\sqrt{-5})(2, 1-\sqrt{-5}) = (2, 1+\sqrt{-5})^2$, it follows that there is only one possibility for I, namely $I = (2, 1+\sqrt{-5})$. Thus there are at most two distinct ideal classes in K. Hence $h_K \leq 2$. But we know that $\mathcal{O}_K$ is not a UFD and so $h_K > 1$. Thus, $h_K = 2$.

3. Let $K = \mathbb{Q}(\sqrt{17})$. Then $n = 2$. $s = 0$ and $d_K = 17$. Thus the Minkowski's inequality (4.8) reduces to

$$\mathsf{N}(I) \leq \frac{2!}{2^2}\sqrt{17} = \frac{\sqrt{17}}{2} = 2.06\ldots\ .$$

Thus there are at most two ideal classes and $h_K \leq 2$. Moreover, if $\mathsf{N}(I) = 2$, then I must be a prime ideal lying over $2\mathbb{Z}$ and with residue degree 1. Now,

$$2 = \frac{17-9}{4} = \left(\frac{\sqrt{17}+3}{2}\right)\left(\frac{\sqrt{17}-3}{2}\right)$$

and both the factors are irreducible elements in $\mathcal{O}_K$ (check!). It follows that only ideals of $\mathcal{O}_K$ with norm 2 are the principal prime ideals $\left(\frac{\sqrt{17}+3}{2}\right)$ and $\left(\frac{\sqrt{17}-3}{2}\right)$. Thus every ideal class of K contains a principal ideal and so $h_K = 1$.

Exercise 4.15. Show that the class number of the quadratic field $\mathbb{Q}(\sqrt{d})$ is 1 if $d = -1, -2, -3, -7$ or if $d = 2, 3, 5$.

Remark 4.16. It turns out, more generally, that the class number of the imaginary quadratic field $\mathbb{Q}(\sqrt{d})$ is 1, if $d = -1, -2, -3, -7, -11, -19, -43, -67, -163$. The converse, that these are the only imaginary quadratic fields with class number 1, was proved independently, by Baker and Stark in 1967. For a beautiful exposition of this problem, known as the Gauss Class Number One Problem, and related results, see the article of D. Goldfeld in the *Bull. Amer. Math. Soc.* **13** (1985), pp. 22–37.

We end with a beautiful result, usually ascribed to Hermite and/or Minkowski, which may be viewed as an arithmetic analogue of the topological fact that $\mathbb{C}$ is simply connected[1].

[1]For more explanation, see the remarks at the end of Appendix B.

Theorem 4.17. *Let K be a number field and d_K be the (absolute) discriminant of K. If $K \neq \mathbb{Q}$, then $|d_K| > 1$ and consequently, at least one rational prime must ramify in K.*

Proof. Let $n = [K : \mathbb{Q}]$ and let r and $2s$ denote, respectively, the number of real and complex embeddings of K. Then $r \geq 0$ and $r + 2s = n$, and so $s \leq [n/2]$, where $[n/2]$ denotes the integral part of $n/2$. As a consequence,

$$\frac{n^n}{n!} = \left(\prod_{i=1}^{[n/2]} \frac{n}{i}\right)\left(\prod_{i=[n/2]+1}^{n} \frac{n}{i}\right) \geq \left(\prod_{i=1}^{[n/2]} \frac{n}{(n/2)}\right)\left(\prod_{i=[n/2]+1}^{n} 1\right) = 2^{[n/2]} \geq 2^s.$$

Thus, from the Minkowski's inequality (4.8), we see that

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

Since $K \neq \mathbb{Q}$, we have $n > 1$, and so $\sqrt{|d_K|} \geq 2^{[n/2]} > 1$ if $s = 0$ whereas $\sqrt{|d_K|} \geq (\pi/2)^s > 1$ if $s > 0$. Thus in any case, $|d_K| > 1$. Therefore, by Dedekind's Discriminant Theorem [cf. Corollary 3.28], it follows that some rational prime must ramify in K. □

Remarks 4.18. 1. If one analyzes the inequalities in the above proof a little more carefully, then we can see that

$$|d_K| \geq \frac{\pi}{3}\left(\frac{3\pi}{4}\right)^{n-1}.$$

Consequently, $n/\log|d_K|$ is bounded by a constant independent of K, and, moreover, given any $d \in \mathbb{Z}$, the degree of a number field with discriminant d is bounded. The last assertion has been refined by Hermite to show that given any integer d, there are only finitely many number fields with discriminant d. For details concerning these finer results, we refer to the book of Samuel [15].

2. Some of the techniques in this chapter are useful to prove a celebrated result of Dirichlet, which states that if K is a number field with r real embeddings and $2s$ complex embeddings, then the group ${\mathcal{O}_K}^\times$ of units of $\mathcal{O}_K$ is isomorphic to $\mu_K \times \mathbb{Z}^{r+s-1}$, where μ_K is a finite cyclic group consisting of the roots of unity in K. Dirichlet's Unit Theorem may be regarded as a vast generalization of some classical observations concerning the solutions of the Brahmagupta-Bhaskaracharya-Pell-Fermat equation[2] $X^2 - dY^2 = 1$. For a proof of Dirichlet's Unit Theorem, we refer to the books of Samuel [15] or Lang [12].

[2]For a historical discussion of this famous equation, see the write up at the MacTutor History of Mathematics archive: `http://www-gap.dcs.st-and.ac.uk/ history/HistTopics/Pell.html`, and the references therein.

Bibliography

[1] M. Atiyah and I. G. MacDonald, Introduction to Commutative Algebra, Addison–Wesley, 1969.

[2] A. Baker, A Concise Introduction to the Theory of Numbers, Cambridge University Press, 1984.

[3] J. W. S. Cassels and A. Fröhlich (Eds.), Algebraic Number Theory, Academic Press, 1967.

[4] J. Esmonde and M. Ram Murty, Problems in Algebraic Number Theory, Springer–Verlag, 2000.

[5] A. Fröhlich and M. J. Taylor, Algebraic Number Theory, Cambridge University Press, 1991.

[6] E. Hecke, Lectures on the Theory of Algebraic Numbers, Springer-Verlag, 1998.

[7] D. Hilbert, The Theory of Algebraic Number Fields, Springer-Verlag, 1998.

[8] K. Ireland and M. Rosen, A Classical Introduction to Modern Number Theory, Springer–Verlag, 1982.

[9] N. Jacobson, Basic Algebra I, 2nd Ed., W. H. Freeman, 1985.

[10] H. Koch, Algebraic Number Theory, 2nd printing, Springer–Verlag, 1997.

[11] S. Lang, Algebra, 2nd ed., Addison-Wesley, 1984.

[12] S. Lang, Algebraic Number Theory, Springer–Verlag, 1986.

[13] D. A. Marcus, Number Fields, Springer–Verlag, 1977.

[14] C. D. Olds, A. Lax and G. Davidoff, The Geometry of Numbers, Mathematical Association of America, 2000.

[15] P. Samuel, Algebraic Theory of Numbers, Hermann, 1970.

[16] H. P. F. Swinnerton-Dyer, A Brief Guide to Algebraic Number Theory, Cambridge University Press, 2001.

[17] J.-P. Serre, Local Fields, Springer–Verlag, 1979.

[18] B. L. Van der Waerden, Algebra, F. Ungar, 1949.

[19] L. C. Washington, Introduction to Cyclotomic Fields, Springer–Verlag, 1982.

[20] O. Zariski and P. Samuel, Commutative Algebra, vol. 1, Springer–Verlag, 1975.

Appendix A

Notes on Galois Theory

A.1 Preamble

These notes attempt to give an introduction to some basic aspects of Field Theory and Galois Theory. Originally, a preliminary version of a part of these notes was prepared to supplement the lectures of the author on Galois Theory and Ramification Theory at the All India Summer School in Number Theory held at Pune in June 1991. Subsequently, the first 6 sections of the Pune Notes were separated and slightly revised to form these "Notes on Galois Theory". These notes were, then, used for the pre-conference distribution to the participants of the NBHM sponsored Instructional School on Algebraic Number Theory (University of Bombay, December 1994) at the request of the organizers. A few minor revisions have taken place in the subsequent years.

The main aim of these notes has always been to provide a geodesic, yet complete, presentation starting from the definition of field extensions and concluding with the Fundamental Theorem of Galois Theory. Some additional material on separable extensions and a section on Norms and Traces is also included, and some historical comments appear as footnotes. The prerequisite for these notes is basic knowledge of Abstract Algebra and Linear Algebra not beyond the contents of usual undergraduate courses in these subjects. No formal background in Galois Theory is assumed. While a complete proof of the Fundamental Theorem of Galois Theory is given here, we do not discuss further results such as Galois' theorem on solvability of equations by radicals. An annotated list of references for Galois Theory appears at the end of Section 5. By way of references for the last section, viz., Norms and Traces, we recommend Van der Waerden's "Algebra" (F. Ungar Pub. Co., 1949) and Zariski–Samuel's "Commutative Algebra, Vol. 1" (Springer-Verlag, 1975).

It appears that over the years, these notes are often used by students primarily interested in Number Theory. Thus it may be pertinent to remark at the outset that the topics discussed in these notes are very useful in the study of Algebraic Number Theory[1]. In order to derive maximum benefit from these notes, the students are advised to attempt all the Exercises and fill the missing steps, if any, in the proofs given. The author would appreciate receiving comments, suggestions and criticism regarding these notes.

[1] In fact, questions concerning integers alone, can sometimes be answered only with the help of field extensions and certain algebraic objects associated to them. For instance, Kummer showed that the equation $X^p + Y^p = Z^p$ has no integer solution for a class of odd primes p, called regular primes, which include all odd primes less than 100 except 37, 59 and 67. Even a convenient definition of regular primes, not to mention the proof of Kummer's Theorem, involves many of the algebraic notions discussed in these lectures. Indeed, an odd prime is *regular* if it doesn't divide the class number of the cyclotomic field extension $\mathbb{Q}(\zeta_p)$ of $\mathbb{Q}$. For details, see H. Edwards' Springer monograph "Fermat's Last Theorem" (1977).

A.2 Field Extensions

Let K be a field [2]. By a *(field) extension* of K we mean a field containing K as a subfield. Let a field L be an extension of K (we usually express this by saying that L/K [read: L over K] is an extension). Then L can be considered as a vector space over K. The *degree* of L over K, denoted by $[L : K]$, is defined as

$$[L : K] = \dim_K L = \text{ the vector space dimension of } L \text{ over } K.$$

If $[L : K] < \infty$, we say that L is a *finite extension* of K or that L is *finite* over K. A subfield K of $\mathbb{C}$ such that $[K : \mathbb{Q}] < \infty$ is called an *algebraic number field* or simply a *number field.*

Lemma 1: *Finite over finite is finite. More precisely, if L/E and E/K are field extensions, then*

$$L \text{ is finite over } K \Leftrightarrow L \text{ is finite over } E \text{ and } E \text{ is finite over } K$$

and, in this case, $[L : K] = [L : E][E : K]$.

Proof: The implication "$\Rightarrow$" is obvious. The rest follows easily from the observation that if $\{u_i\}$ is an E–basis of L and $\{v_j\}$ is a K–basis of E, then $\{u_i v_j\}$ is a K–basis of L. □

Let L/K be a field extension. An element $\alpha \in L$ is said to be *algebraic* over K if it satisfies a nonzero polynomial with coefficients in K, i.e, $\exists\ 0 \neq f(X) \in K[X]$ such that $f(\alpha) = 0$. Given $\alpha \in L$ which is algebraic over K, we can find a monic polynomial in $K[X]$ of least possible degree, satisfied by α. This is unique and is called the *minimal polynomial* of α over K. It is easily seen to be irreducible and we will denote it by $\mathrm{Irr}(\alpha, K)$. Note that if $f(X)$ is any monic irreducible polynomial satisfied by α, then we must have $f(X) = \mathrm{Irr}(\alpha, K)$ and that it generates the ideal $\{g(X) \in K[X] : g(\alpha) = 0\}$ in $K[X]$.[3] The extension L of K is said to be *algebraic* if every element of L is algebraic over K.

Lemma 2: *Finite $\Rightarrow$ algebraic. That is, if L/K is a finite extension, then it is algebraic.*

Proof: For any $\alpha \in L$, there must exist a positive integer n such that $\{1, \alpha, \alpha^2, ..., \alpha^n\}$ is linearly dependent over K, thus showing that α is algebraic over K. □

Exercise 1: Show, by an example, that the converse of the above lemma is not true, in general.

We now study extensions for which the converse *is* true.

Definition: Given elements $\alpha_1, \ldots, \alpha_n$ in an extension L of a field K, we define

$$K[\alpha_1, \ldots, \alpha_n] = \text{the smallest subring of } L \text{ containing } K \text{ and } \alpha_1, \ldots, \alpha_n$$
$$K(\alpha_1, \ldots, \alpha_n) = \text{the smallest subfield of } L \text{ containing } K \text{ and } \alpha_1, \ldots, \alpha_n.$$

Note that $K[\alpha_1, \ldots, \alpha_n]$ precisely consists of elements of the form $f(\alpha_1, \ldots, \alpha_n)$ where $f(X_1, \ldots, X_n)$ varies over $K[X_1, \ldots, X_n]$ (= the ring of polynomials in the n variables $X_1, \ldots, X_n$ with coefficients in K) whereas $K(\alpha_1, \ldots, \alpha_n)$ precisely consists of elements of the form $\frac{f(\alpha_1, \ldots, \alpha_n)}{g(\alpha_1, \ldots, \alpha_n)}$ where $f(X_1, \ldots, X_n), g(X_1, \ldots, X_n)$ vary over $K[X_1, \ldots, X_n]$ with $g(\alpha_1, \ldots, \alpha_n) \neq 0$. Also note that $K(\alpha_1, \ldots, \alpha_n)$ is the quotient field of $K[\alpha_1, \ldots, \alpha_n]$ in L.

Definition: An extension L of K is said to be *finitely generated* over K if there exist $\alpha_1, \ldots, \alpha_n$ in L such that $L = K(\alpha_1, \ldots, \alpha_n)$. We say that L is a *simple* extension of K if $L = K(\alpha)$ for some $\alpha \in L$.

For simple extensions, the converse to Lemma 2 is true. In fact, we can say much more.

Lemma 3: *Let α be an element in an overfield L of a field K. Then:*

$$K(\alpha)/K \text{ is algebraic } \Leftrightarrow \alpha \text{ is algebraic over } K \Leftrightarrow K[\alpha] = K(\alpha) \Leftrightarrow [K(\alpha) : K] < \infty.$$

[2] Fields are usually denoted by K or k since the German word for field is Körper. Much of Modern Field Theory was created by the German mathematician E. Steinitz; see his paper "Algebraische Theorie der Körper", Crelle Journal (1910), pp. 167–308, for an original exposition.

[3] It may be instructive to verify the observations made in the last few statements. General Hint: Use the Division Algorithm in $K[X]$.

Moreover, if α is algebraic over K and $f(X) = \mathrm{Irr}(\alpha, K)$, then there exists an isomorphism of $K(\alpha)$ onto $K[X]/(f(X))$ which maps α to $\overline{X}$, the residue class of X, and the elements of K to their residue classes.

Proof: Without loss of generality, we can and will assume that $\alpha \neq 0$. The first assertion trivially implies the second. Now, the map $\varphi : K[X] \to L$ defined by $f(X) \mapsto f(\alpha)$ is clearly a ring homomorphism whose image is $K[\alpha]$. If α is algebraic over K, then the kernel of φ is a nonzero prime ideal in $K[X]$ and is hence a maximal ideal (prove!). So $K[\alpha] \simeq K[X]/\ker\varphi$ is a field containing K and α. Therefore $K[\alpha] = K(\alpha)$. Next, if $K[\alpha] = K(\alpha)$, we can write $\alpha^{-1} = a_0 + a_1\alpha + \cdots + a_r\alpha^r$ for some $a_0, \ldots, a_r \in K$ with $a_r \neq 0$, which shows that α^{r+1} lies in the K–linear span of $1, \alpha, \alpha^2, \ldots, \alpha^r$, and consequently so does α^{r+j} for any $j \geq 1$. And since $1, \alpha, \alpha^2, \ldots$ clearly span $K[\alpha] = K(\alpha)$, it follows that $[K(\alpha) : K] \leq r + 1 < \infty$. If $[K(\alpha) : K] < \infty$, Lemma 2 shows that $K(\alpha)$ is algebraic over K. Moreover, if α is algebraic over K and $f(X) = \mathrm{Irr}(\alpha, K)$, then, as noted earlier, $\ker\varphi$ is generated by $f(X)$, from which we get the desired isomorphism between $K(\alpha)$ and $K[X]/(f(X))$. □

Exercise 2: If α is algebraic over K, then show that $[K(\alpha) : K]$ equals the degree of $\mathrm{Irr}(\alpha, K)$.

Exercise 3: Try to give a more constructive proof of the fact that if α is algebraic over K, then $K[\alpha] = K(\alpha)$ by showing that for any $g(X) \in K[X]$ with $g(\alpha) \neq 0$, we can find $h(X) \in K[X]$ such that $g(\alpha)^{-1} = h(\alpha)$.

The following lemma gives necessary and sufficient conditions for the converse to Lemma 2.

Lemma 4: *Let L be an extension of a field K. Then:*

$$L \text{ is finite over } K \Leftrightarrow L \text{ is algebraic and finitely generated over } K.$$

Proof: If L is finite over K, then it is algebraic, and if $u_1, \ldots, u_n$ is a K–basis of L, then clearly $L = K(u_1, \ldots, u_n)$. Conversely, if $L = K(\alpha_1, \ldots, \alpha_n)$ for some $\alpha_1, \ldots, \alpha_n \in K$, then using Lemmas 1 and 3 and induction on n, it is seen that L is finite over K. □

Let us obtain some useful consequences of the above lemma.

Lemma 5: *Algebraic over algebraic is algebraic. More precisely, if L/E and E/K are field extensions, then:*

$$L \text{ is algebraic over } K \Leftrightarrow L \text{ is algebraic over } E \text{ and } E \text{ is algebraic over } K$$

Proof: The implication "⇒" is obvious. To prove the other one, take any $\alpha \in L$. Find $b_0, b_1, \ldots, b_n \in E$, not all zero, such that $b_0 + b_1\alpha + \cdots + b_n\alpha^n = 0$. Then α is algebraic over $K(b_0, b_1, \ldots, b_n)$, and $K(b_0, b_1, \ldots, b_n) \subseteq E$ is algebraic over K. Hence, in view of Lemmas 1, 3 and 4, we see that

$$\begin{aligned} [K(\alpha) : K] &\leq [K(b_0, b_1, \ldots, b_n, \alpha) : K] \\ &= [K(b_0, b_1, \ldots, b_n, \alpha) : K(b_0, b_1, \ldots, b_n)][K(b_0, b_1, \ldots, b_n) : K] \\ &< \infty \end{aligned}$$

which shows that α is algebraic over K. □

Lemma 6: *Let L be an extension of a field K and let*

$$E = \{\alpha \in L : \alpha \text{ is algebraic over } K\}.$$

Then E is a subfield of L containing K.

Proof: Clearly $K \subseteq E \subseteq L$. Given any $\alpha, \beta \in E$, by Lemma 3, we see that

$$[K(\alpha, \beta) : K] = [K(\alpha, \beta) : K(\alpha)][K(\alpha) : K] < \infty$$

and therefore every element of $K(\alpha, \beta)$ is algebraic over K. So $\alpha + \beta, \alpha - \beta, \alpha\beta \in E$ and if $\beta \neq 0$, then $\frac{\alpha}{\beta} \in E$, and hence E is a subfield of L. □

Exercise 4: Given elements α, β, algebraic over a field K, can you explicitly find polynomials in $K[X]$ satisfied by $\alpha + \beta$, $\alpha\beta$? Find, for instance, a polynomial, preferably irreducible, satisfied by $\sqrt{2} + \sqrt{3}$.

A.3 Splitting Fields and Normal Extensions

Galois Theory, at least in its original version, has to do with roots of polynomial equations. This motivates much of what is done in this section.

Let K be a field. By a *root* of a polynomial $f(X) \in K[X]$ we mean an element α in an overfield of K such that $f(\alpha) = 0$. It is easy to see that a nonzero polynomial in $K[X]$ of degree n has at most n roots (Verify!). The following lemma, usually attributed to Kronecker, shows, by a method not unlike witchcraft, that roots can always be found.

Lemma 7: *Let $f(X) \in K[X]$ be a nonconstant polynomial of degree n. Then there exists an extension E of K such that $[E : K] \leq n$ and $f(X)$ has a root in E.*

Proof: Let $g(X)$ be a monic irreducible factor of $f(X)$. Then $(g(X))$, the ideal generated by $g(X)$ in $K[X]$, is a maximal ideal and hence $E = K[X]/(g(X))$ is a field. Let $\sigma : K[X] \to E$ be the canonical homomorphism which maps an element in $K[X]$ to its residue class modulo $(g(X))$. Note that $\sigma|_K$ is injective and hence K may be regarded as a subfield of E. Let $\alpha = \sigma(X)$. Then $g(\alpha) = g(\sigma(X)) = \sigma(g(X)) = 0$. Hence, $f(\alpha) = 0$. By Lemma 3 and Exercise 2, $[E : K] = \deg g(X) \leq n$. □

Remark: The above proof, though common in many texts, is slightly imprecise. To be pedantic, an actual extension E of K as in the statement of Lemma 6 can be constructed by putting $E = (\sigma(K[X])\backslash\sigma(K)) \cup K$, where σ is as in the above proof, and by defining field operations on E in an obvious manner. Note that we then have $E \simeq \sigma(K[X])$.

To study the roots of a polynomial $f(X) \in K[X]$, it seems natural to be in a nice set containing all the roots of $f(X)$ and which, in some sense, is the smallest such. This is afforded by the following.

Definition: Let $f(X) \in K[X]$ be a nonconstant polynomial. By a *splitting field* of $f(X)$ over K we mean an extension L of K such that $f(X)$ splits into linear factors in L and L is generated over K by the roots of $f(X)$ in L, i.e.,

(i) $f(X) = c(X - \alpha_1) \ldots (X - \alpha_n)$ for some $c \in K$ and $\alpha_1, \ldots, \alpha_n \in L$.

(ii) $L = K(\alpha_1, \ldots, \alpha_n)$.

Lemma 8: *Given any nonconstant polynomial $f(X) \in K[X]$ of degree n, there exists a splitting field L of $f(X)$ over K such that $[L : K] \leq n!$.*

Proof: Induct on n. If $n = 1$, then $L = K$ does the job. For $n > 1$, by Lemma 7, we can find an extension E of K such that $[E : K] \leq n$ and $f(X) = (X - \alpha)g(X)$ for some $\alpha \in E$ and $g(X) \in E[X]$. Since $\deg g(X) = n - 1 \geq 1$, a splitting field, say L, of $g(X)$ over E exists. Clearly, L is also a splitting field of $f(X)$ over K; moreover, $[L : K] = [L : E][E : K] \leq (n - 1)!n = n!$. □

Notation: Given any fields K and K', a homomorphism $\sigma : K \to K'$, and a polynomial $f(X) \in K[X]$, by $f^\sigma(X)$ we denote the corresponding polynomial in $K'[X]$, i.e., if $f(X) = \sum a_i X^i$ then $f^\sigma(X) = \sum \sigma(a_i) X^i$. Note that $f(X) \mapsto f^\sigma(X)$ gives a homomorphism of $K[X] \to K'[X]$ which is an isomorphism if σ is an isomorphism.

The following lemma will help us prove that a splitting field is unique up to isomorphism.

Lemma 9: *Let K and K' be fields and $\sigma : K \to K'$ be an isomorphism. Let $g(X) \in K[X]$ be an irreducible polynomial and let α and α' be roots of $g(X)$ and $g^\sigma(X)$ in some extensions of K and K' respectively. Then there exists an isomorphism $\eta : K(\alpha) \to K'(\alpha')$ such that $\eta|_K = \sigma$ and $\eta(\alpha) = \alpha'$.*

Proof: Clearly σ gives an isomorphism of $K[X]$ onto $K'[X]$, which, in turn, induces an isomorphism of $K[X]/(g(X))$ onto $K'[X]/(g^\sigma(X))$. By Lemma 3, we get an isomorphism of $K(\alpha)$ onto the former and of $K'(\alpha')$ onto the latter. By suitably composing these maps, we obtain an isomorphism $\eta : K(\alpha) \to K'(\alpha')$ such that $\eta|_K = \sigma$ and $\eta(\alpha) = \alpha'$. □

Note: A field has no proper ideals. This means that a homomorphism of a field (into a ring) is either injective or maps everything to 0. If L is an extension of K, by a *K–homomorphism* of L we mean a homomorphism $\sigma : L \to L'$, where L' is some extension of K, which is identity on K, i.e., $\sigma(c) = c$ $\forall\, c \in K$. Observe that a K–homomorphism is always injective.[4] Also observe that, a K–homomorphism

[4]Indeed, $1 \in K$ and $\sigma(1) = 1 \neq 0$.

$\sigma : L \to L'$, where L' is an extension of L, is an automorphism (= isomorphism onto itself) of L provided $\sigma(L) \subseteq L$ [since $\sigma(L)$ and L have the same vector space dimension over K].

Before proving the uniqueness of splitting fields, let us deduce an important consequence of the above lemma.

Corollary: *Let α be algebraic over K and $f(X) = \mathrm{Irr}(\alpha, K)$. Let L be any extension of K containing a splitting field of $f(X)$. Then the number of K–homomorphisms of $K(\alpha)$ to L is equal to the number of distinct roots of $f(X)$; in particular, this number is $\leq [K(\alpha) : K]$ with equality holding if and only if all roots of $f(X)$ are distinct.*

Proof: Let $\alpha_1, \ldots, \alpha_r \in L$ be all possible distinct roots of $f(X)$. By Lemma 9, there exist K–isomorphisms $\eta_i : K(\alpha) \to K(\alpha_i)$ such that $\eta_i(\alpha) = \alpha_i$ $(1 \leq i \leq r)$. Moreover, if $\sigma : K \to L$ is any K–homomorphism, then $f^\sigma(X) = f(X)$, and hence $\sigma(\alpha) = \alpha_i$ for some i, which shows that $\sigma = \eta_i$. The inequality $r \leq [K(\alpha) : K]$ follows from Exercise 2. □

Lemma 10: *Let K and K' be fields and $\sigma : K \to K'$ be an isomorphism. Let $f(X) \in K[X]$ be any nonconstant polynomial and let L and L' be splitting fields of $f(X)$ and $f^\sigma(X)$ over K and K' respectively. Then there exists an isomorphism $\tau : L \to L'$ such that $\tau|_K = \sigma$. Moreover, the number of such isomorphisms is $\leq [L : K]$.*

Proof: Let $n = \deg f(X) = \deg f^\sigma(X) \geq 1$. We proceed by induction on n. If $n = 1$, we must have $L = K$ and $L' = K'$, so the assertion follows with $\tau = \sigma$. Suppose $n > 1$. Let $g(X)$ be a monic irreducible factor of $f(X)$. Let α and α' be roots of $g(X)$ and $g^\sigma(X)$ in L and L' respectively. By Lemma 9, we can find a K–isomorphism $\eta : K(\alpha) \to K(\alpha')$ such that $\eta|_K = \sigma$ and $\eta(\alpha) = \alpha'$. Now write $f(X) = (X - \alpha)h(X)$ for some $h(X) \in K(\alpha)[X]$ and note that L and L' are splitting fields of $h(X)$ and $h^\sigma(X)$ over $K(\alpha)$ and $K'(\alpha)$ respectively. Using the induction hypothesis, we get the desired isomorphism, and, in view of the above Corollary, also the desired inequality. □

Taking $K = K'$ and σ to be the identity map in the above Lemma, we get

Corollary: *If $f(X) \in K[X]$ is a nonconstant polynomial, then any two splitting fields of $f(X)$ over K are K–isomorphic.* □

A notion closely related to splitting fields is defined below.

Definition: An extension L of K such that whenever an irreducible polynomial in $K[X]$ has a root in L it has all its roots in L, is called a *normal extension.*

And here is the connection.

Lemma 11: *Let L/K be a finite extension. Then the following statements are equivalent.*

(1) L is a normal extension of K.

(2) L is a splitting field of a polynomial in $K[X]$.

(3) Any K–homomorphism $\sigma : L \to L'$, where L' is any extension of L, is an automorphism of L.

Proof: (1) ⇒ (2): Since L/K is finite, we can write $L = K(\alpha_1, \ldots, \alpha_n)$ for some $\alpha_1, \ldots, \alpha_n \in L$. Let $f_i(X) = \mathrm{Irr}(\alpha_i, K)$ and $f(X) = \prod_{i=1}^n f_i(X)$. Then, by our hypothesis, all the roots of $f(X)$ are in L. Also L is clearly generated (over K) by these roots.

(2) ⇒ (3): Let $L = K(\alpha_1, \ldots, \alpha_n)$ be a splitting field of some $f(X) \in K[X]$ where $\alpha_1, \ldots, \alpha_n$ are the roots of $f(X)$ in L. If $\sigma : L \to L'$ is any K–homomorphism, then $f^\sigma(X) = f(X)$ and hence $\sigma(\alpha_i)$ must be a root of $f(X)$. Since σ is injective, it permutes the roots of $f(X)$, and therefore $\sigma(L) = L$.

(3) ⇒ (1): Let $f(X)$ be any irreducible polynomial having a root $\alpha \in L$. Let β be any other root of $f(X)$. Let L' be a splitting field of $f(X)$ over L so that $\beta \in L'$. By Lemma 9, there exists a K–isomorphism $\eta : K(\alpha) \to K(\beta)$ such that $\eta(\alpha) = \beta$. By Lemma 10, η can be extended to a K–isomorphism $\tau : L' \to L'$. Let $\sigma = \tau|_L$. Then, by our hypothesis, $\beta = \sigma(\alpha) \in L$. □

Remark: The above lemma also holds for infinite algebraic extensions provided in (2) we replace "a polynomial" by "a family of polynomials". Verify!

Example: The usual formula for the roots of a quadratic equation shows that an extension of degree 2 is always normal. Extensions of $\mathbb{Q}$ of degree 2 are called *quadratic fields.* If ω is a "primitive n–th root

of unity" (i.e., $\omega^n = 1$ and $\omega^m \neq 1$ for $1 \leq m < n$), then $\mathbb{Q}(\omega)$ is a normal extension of $\mathbb{Q}$ (prove!); it is called the *cyclotomic field* of the n–th roots of unity.

Exercise 5: Prove that if an extension L/K is normal and E is a subfield of L containing K, then L/E is also normal.

Exercise 6: Show, by an example, that normal over normal need not be normal.

Exercise 7: Show that if L/K is any finite extension, then we can find a *least normal extension* of K containing L (as a subfield), i.e., an extension N of L such that N/K is normal, and no proper subfield of N containing L is normal over K; note that any such N is finite over K. Show that any two least normal extensions of K containing L are K–isomorphic.

A.4 Separable Extensions

Let K be a field. An irreducible polynomial in $K[X]$ is said to be *separable* if all its roots (in its splitting field) are distinct. An element α, which is algebraic over K, is said to be *separable* if $\mathrm{Irr}(\alpha, K)$ is a separable polynomial. An algebraic extension L of K is called *separable* if every element of L is separable over K.

Assuming an extension to be separable can lead to nice consequences such as the following

Lemma 12 (Primitive Element Theorem): *Finite separable extensions are simple.*

Proof: Let L/K be a finite separable extension. If K is finite, then so is L, and using the well-known fact that the multiplicative group of the nonzero elements of a finite field is cyclic,[5] we can find $\theta \in L$ which generates $N = L \setminus \{0\}$; clearly $L = K(\theta)$, and thus L/K is simple. Now assume that K is infinite. Obviously L is finitely generated over K and so it suffices to show that if $L = K(\alpha, \beta)$, then we can find a "primitive element" $\theta \in L$ so that $L = K(\theta)$. Let $f(X) = \mathrm{Irr}(\alpha, K)$ and $g(X) = \mathrm{Irr}(\beta, K)$. Suppose $\alpha_1, \ldots, \alpha_m$ and $\beta_1, \ldots, \beta_n$ are the roots of $f(X)$ and $g(X)$ respectively with $\alpha_1 = \alpha$ and $\beta_1 = \beta$. By hypothesis, $\alpha_i \neq \alpha_j$ and $\beta_i \neq \beta_j$ for all $i \neq j$. Since K is infinite, we can find an element $c \in K$ such that

$$c \neq \frac{\alpha_i - \alpha_j}{\beta_r - \beta_s} \quad \text{for all choices of } i, j, r, s \text{ such that } 1 \leq i, j \leq m,\ 1 \leq r, s \leq n \text{ and } r \neq s.$$

Let $\theta = \alpha + c\beta$ and $h(X) = f(\theta - cX)$. Clearly $h(X) \in K(\theta)[X]$ and $h(\beta) = 0$. Also $h(\beta_j) \neq 0$ for $j \geq 2$ lest $c = \frac{\alpha_i - \alpha}{\beta - \beta_j}$ for some $i \geq 1$. It follows that the GCD of $g(X)$ and $h(X)$ in $K(\theta)[X]$ must be $X - \beta$. Hence $\beta \in K(\theta)$, and consequently, $\alpha \in K(\theta)$. Thus $K(\theta) = K(\alpha, \beta) = L$. □

Remark: Note that the above proof actually shows that if either one of α or β is separable over K, then $K(\alpha, \beta)/K$ is simple.

To check separability, the notion of derivatives comes in handy. In Algebra, derivatives can be defined in a purely formal manner (i.e., without involving limits) as follows. Given any $f(X) \in K[X]$, let $f(X) = \sum_{i=0}^{n} a_i X^i$, with $a_i \in K$, and define the *derivative* of $f(X)$, denoted by $f'(X)$, by $f'(X) = \sum_{i=1}^{n} i a_i X^{i-1}$. The usual properties such as linearity [i.e., $(af \pm bg)' = af' \pm bg'$], product rule [i.e., $(fg)' = f'g + fg'$], can be easily checked using this definition. Now recall that an element α in an extension L of K is called a *multiple root* of $f(X) \in K[X]$ if $f(X) = (X - \alpha)^2 g(X)$ for some $g(X) \in L[X]$.

Lemma 13: *Let $f(X)$ be an irreducible polynomial in $K[X]$. Then*

$$f(X) \text{ has a multiple root } \Leftrightarrow f'(X) = 0.$$

Proof: If α is a multiple root of $f(X)$, then, by the product rule, $f'(\alpha) = 0$. But $f(X)$, being irreducible, is a polynomial of the least degree satisfied by α, which contradicts the fact that $\deg f'(X) < \deg f(X)$ unless $f'(X) = 0$. Conversely if $f'(X) = 0$, then any root of $f(X)$ is a multiple root. □

[5] A proof of this fact may be taken as an exercise. A hint is to take the maximum order, say m, of the elements of the multiplicative group, and note that the order of every element divides m whereas the equation $X^m = 1$ has at most m solutions in the field.

Exercise 8: Let $\mathbb{Z}/p\mathbb{Z}$ be the field of residue classes of integers modulo a prime number p. Let $q = p^n$ and $\mathbb{F}_q$ denote the splitting field of $X^q - X$ over $\mathbb{Z}/p\mathbb{Z}$. Show that $\mathbb{F}_q$ is a finite field containing q elements and that it is a separable and normal extension of $\mathbb{Z}/p\mathbb{Z}$.[6]

Exercise 9: Let F be a finite field. Show that $|F|$, the cardinality of F, must equal p^n for some prime p, and that F is isomorphic to $\mathbb{F}_{p^n}$.

Definition: A field K is said to be *perfect* if either $\mathrm{char}(K)$, the characteristic of K, is 0, or $\mathrm{char}(K) = p \neq 0$ and $K = K^p$, i.e., for any $\alpha \in K$, there exists $\beta \in K$ such that $\alpha = \beta^p$.

Lemma 14: *Any algebraic extension of a perfect field is separable.*

Proof: Let K be a perfect field and L be an extension of K. Let $\alpha \in L$ and $\mathrm{Irr}(\alpha, K) = f(X) = \sum_{i=0}^{n} a_i X^i$. If α is not separable, then $f(X)$ has multiple roots and hence $f'(X) = \sum_{i=1}^{n} i a_i X^{i-1} = 0$. In case $\mathrm{char}(K) = 0$, we get $a_i = 0$ for all $i \geq 1$, which is a contradiction. In case $\mathrm{char}(K) = p \neq 0$, we have $a_i = 0$ if $p \not| i$. Since K is perfect, we can find $b_i \in K$ such that $a_i = b_i^p$, and thus $f(X) = g(X)^p$ where $g(X) = \sum_{p|i} b_i X^{i/p} \in K[X]$, which contradicts the irreducibility of $f(X)$. □

Exercise 10: Prove that the converse of Lemma 14 is also true. That is, if K is a field such that every algebraic extension of K is separable, then K is perfect.

Exercise 11: Prove that a finite field is perfect.

Exercise 12: Show that not everything is perfect! More precisely, let k be a field of characteristic $p \neq 0$, and $K = k(t)$ be the field of rational functions in an indeterminate t over k. Let L be an algebraic extension of K containing a root of $X^p - t$. Show that L is not separable over K. In particular, inseparable (= not separable) extensions and imperfect (= not perfect) fields do exist.

Exercise 13: Let L/K be a finite extension of degree n. Show that L/K is separable if and only if there are n distinct K–homomorphisms of L into N, for any normal extension N/K containing L as a subfield. [Hint: Use Lemma 12 and the Corollary to Lemma 9]. Further show that if L/K is separable and E is a subfield of L containing K, then each K–homomorphism of E into N has exactly $[L : E]$ distinct extensions to L.

Exercise 14: Show that separable over separable is separable. More precisely, if L/E and E/K are algebraic extensions, then show that L/K is separable iff both L/E and E/K are separable. [Hint: For the nontrivial implication, reduce to the case of finite extensions and use Exercise 13]. Deduce that if $\alpha_1, \ldots, \alpha_n$ are algebraic and separable over a field K, then $K(\alpha_1, \ldots, \alpha_n)$ is a separable extension of K. Further deduce that if L/K is a finite separable extension and N is a least normal extension of K containing L, then N/K is also a finite separable extension [in this case N is called a *least Galois extension* of K containing L].

In Number Theory, the fields occurring are algebraic extensions of $\mathbb{Q}$ or $\mathbb{Z}/p\mathbb{Z}$, and thus, in view of Lemma 14 and Exercise 11, we only have to deal with separable extensions.

A.5 Galois Theory

Let K be a field. Given any polynomial $f(X) \in K[X]$ having distinct roots, the splitting field L of $f(X)$ over K is a finite, normal and separable extension. The essence of Galois theory lies in the association of a group G, known as Galois group, to such a polynomial or more generally, to an extension L/K with the above properties. Intrinsic properties of the polynomial $f(X)$ (or the extension L/K) are nicely captured in this group. A main result of Galois Theory establishes a one–to–one correspondence between the subgroups of G and the subfields of L containing K. This enabled Galois to obtain his celebrated results in Theory of Equations.[7]

[6]Finite fields are often called *Galois fields*, and $\mathbb{F}_q$ is sometimes denoted by $GF(q)$; these fields were first studied by E. Galois in a paper, published in 1830, entitled "Sur la theorié des nomberes".

[7]Galois showed that the equation $f(X) = 0$ is solvable by radicals (like the quadratic equation) if and only if G, the Galois group of $f(X)$, is a solvable group. The Galois group of a general equation of degree n turns out to be S_n, which is not solvable for $n \geq 5$, and thus general equations of degree 5 or more cannot be solved by radicals. For details, see any of the references given at the end of this section. It may be worth noting that

To describe the Galois group and the said correspondence, let us begin with some

Definitions: Let L/K be a field extension.

(1) The *Galois group* of L/K, denoted by $\mathrm{Gal}(L/K)$, is defined by

$$\mathrm{Gal}(L/K) = \text{the group of all } K\text{–automorphisms of } L$$

(2) L/K is said to be a *Galois extension* if it is finite, normal and separable.[8]

(3) For a subgroup H of $\mathrm{Gal}(L/K)$, the *fixed field* of H, denoted by L^H, is defined by

$$L^H = \{\alpha \in L : \sigma(\alpha) = \alpha \text{ for all } \sigma \in H\}.$$

Note that $\mathrm{Gal}(L/K)$ is indeed a group (with composition of maps as the group operation) and that L^H is a subfield of L containing K. Also note that if L/K is a Galois extension, then for any subfield E of L containing K, L/E is also a Galois extension (cf. Exercise 5) and $\mathrm{Gal}(L/E)$ is a subgroup of $\mathrm{Gal}(L/K)$.

Theorem 1 (Fundamental Theorem of Galois Theory): *Let L/K be a Galois extension. Then $\mathrm{Gal}(L/K)$ is a finite group of order $[L : K]$, and there is a bijection between the subfields E of L containing K and the subgroups H of $\mathrm{Gal}(L/K)$, given by*

$$E \mapsto \mathrm{Gal}(L/E) \quad \textit{with the inverse given by} \quad H \mapsto L^H.$$

In particular, K is the fixed field of $\mathrm{Gal}(L/K)$.

Note that this bijection is inclusion–reversing. It also has additional nice properties which can be deduced from the above Theorem.

Corollary (Supplement to the Fundamental Theorem of Galois Theory): *Let L/K be a Galois extension and E be a subfield of L containing K. Then E/K is a finite separable extension, and*

$$E/K \textit{ is a normal extension} \Leftrightarrow \mathrm{Gal}(L/E) \textit{ is a normal subgroup of } \mathrm{Gal}(L/K)$$

and, in this case,

$$\mathrm{Gal}(E/K) \textit{ is isomorphic to the quotient group } \frac{\mathrm{Gal}(L/K)}{\mathrm{Gal}(L/E)}.$$

A proof of the above Theorem will be given by piecing together the following lemmas.

Lemma 15: *Let L/E be a Galois extension. Then $\mathrm{Gal}(L/E)$ is a finite group of order $[L : E]$ and E is its fixed field.*

Proof: By Primitive Element Theorem, $L = E(\alpha)$ for some $\alpha \in L$. Now $\mathrm{Irr}(\alpha, E)$ is of degree $n = [L : E]$ and, since L/E is normal and separable, it has n distinct roots in L. By Corollary to Lemma 9, we see that there are exactly n distinct E–automorphisms of L, i.e, $|\mathrm{Gal}(L/E)| = n$. If β is in the fixed field of $\mathrm{Gal}(L/E)$ and $\beta \notin E$, then we can find $\beta' \in L$ such that $\beta' \neq \beta$ and β' is a root of $\mathrm{Irr}(\beta, E)$. By Lemma 9, there exists an E–isomorphism $\eta : E(\beta) \to E(\beta')$ with $\eta(\beta) = \beta'$, and, by Lemma 10, this can be extended to an E–automorphism $\sigma : L \to L$. Now $\sigma \in \mathrm{Gal}(L/E)$ and $\sigma(\beta) = \beta' \neq \beta$, which contradicts the assumption on β. □

The following result is a key step in the proof of the above Theorem.

Lemma 16: *Let L/K be a field extension and H be a finite subgroup of $\mathrm{Gal}(L/K)$. Then L/L^H is a Galois extension and $\mathrm{Gal}(L/L^H) = H$.*

Evariste Galois, the inventor of Galois theory, did his work at a very early age. He was born in October 1811, and he died twenty years and seven months later in a duel.

[8] It may be noted that by a Galois extension, some authors mean an extension which is algebraic, normal, and separable, i.e., they don't require it to be finite.

Proof: Let $\alpha \in L$ and $H = \{\sigma_1, \ldots, \sigma_n\}$ where $\sigma_1, \ldots, \sigma_n$ are distinct elements so arranged that $\{\sigma(\alpha) : \sigma \in H\} = \{\sigma_1(\alpha), \ldots, \sigma_m(\alpha)\}$ for some $m \leq n$. Notice that $\sigma_1(\alpha), \ldots, \sigma_m(\alpha)$ are distinct and for any $\tau \in H$, we have

$$\{\tau\sigma_1(\alpha), \ldots, \tau\sigma_m(\alpha)\} = \{\tau\sigma(\alpha) : \sigma \in H\} = \{\sigma_1(\alpha), \ldots, \sigma_m(\alpha)\}.$$

Consider the polynomial

$$f(X) = \prod_{i=1}^{m}(X - \sigma_i(\alpha)) \quad \text{and note that } f^{\tau}(X) = \prod_{i=1}^{m}(X - \tau\sigma_i(\alpha)) = \prod_{i=1}^{m}(X - \sigma_i(\alpha)) = f(X).$$

So every $\tau \in H$ fixes the coefficients of $f(X)$, and hence $f(X) \in L^H[X]$. Also $f(\alpha) = 0$ and if $g(X) = \mathrm{Irr}(\alpha, L^H)$, then $g(\sigma_i(\alpha)) = \sigma_i(g(\alpha)) = 0$ for all $i = 1, \ldots, m$. Thus $\deg g(X) \geq \deg f(X)$, and, since $g(X)$ is the minimal polynomial of α over L^H, we have $g(X) = f(X)$. Therefore α is algebraic and separable over L^H, and moreover, $[L^H(\alpha) : L^H] = m \leq n = |H|$. Now choose $\alpha \in L$ such that $[L^H(\alpha) : L^H]$ is maximal. Then we must have $L = L^H(\alpha)$. To see this, assume the contrary. Then we can find $\beta \in L$ such that $\beta \notin L^H$ and we note that, by Lemma 1, $[L^H(\alpha, \beta) : L^H] > [L^H(\alpha) : L^H]$ and that, by Lemma 12, $L^H(\alpha, \beta)$ is a simple extension of L^H. But this contradicts the maximality of $[L^H(\alpha) : L^H]$. Hence $L = L^H(\alpha)$ and thus L/L^H is a Galois extension. Moreover, $H \subseteq \mathrm{Gal}(L/L^H)$ and, in view of Lemma 15, we have $\mathrm{Gal}(L/L^H) = [L : L^H] = \deg \mathrm{Irr}(\alpha, L^H) \leq |H|$. Therefore $H = \mathrm{Gal}(L/L^H)$. □

Remark: Note that the subfield K did not play any role in the above proof. In fact, we could have taken H to be any finite group of automorphisms of L.

Proof of the Fundamental Theorem of Galois Theory: Let L/K be a Galois extension. From Lemma 15, it follows that the composite of the maps given by $E \mapsto \mathrm{Gal}(L/E)$ and $H \mapsto L^H$ is identity, i.e., $\mathrm{Gal}(L/E)$ is a subgroup of $\mathrm{Gal}(L/K)$ and $L^{\mathrm{Gal}(L/E)} = E$. From Lemma 16, it follows that the other composite is identity, i.e., L^H is a subfield of L containing K, L/L^H is a Galois extension, and $\mathrm{Gal}(L/L^H) = H$. Thus we have a bijection as desired. □

Proof of the Supplement to FTGT: Let L/K be a Galois extension and E be a subfield of L containing K. The finiteness and separability of E/K is obvious. For any $\sigma \in \mathrm{Gal}(L/K)$, $\sigma(E)$ is a subfield of L containing K, and it is easy to see that

$$\mathrm{Gal}(L/\sigma(E)) = \sigma\mathrm{Gal}(L/E)\sigma^{-1}.$$

From Lemma 11, it follows that

$$E/K \text{ is a normal extension } \Leftrightarrow \ \sigma(E) = E \text{ for all } \sigma \in \mathrm{Gal}(L/K).$$

Consequently, if E/K is a normal extension, then $\mathrm{Gal}(L/E)$ is a normal subgroup of $\mathrm{Gal}(L/K)$. To prove the converse, note that for any $\sigma \in \mathrm{Gal}(L/K)$, by Lemma 15, we have that

$$\text{the fixed field of } \mathrm{Gal}(L/E) = E \ \text{ and } \ \text{the fixed field of } \sigma\mathrm{Gal}(L/E)\sigma^{-1} = \sigma(E).$$

Therefore if $\mathrm{Gal}(L/E)$ is a normal subgroup of $\mathrm{Gal}(L/K)$, we have $\sigma(E) = E$ for any $\sigma \in \mathrm{Gal}(L/K)$, and hence E/K is normal. In the case E/K is normal, it is Galois, and the map $\sigma \mapsto \sigma|_E$ defines a group homomorphism of $\mathrm{Gal}(L/K)$ into $\mathrm{Gal}(E/K)$. By Lemma 10, any K–automorphism of E can be extended to a K–automorphism of L, which shows that this group homomorphism is surjective. Hence $\mathrm{Gal}(E/K)$ is isomorphic to the quotient group $\mathrm{Gal}(L/K)/\mathrm{Gal}(L/E)$. □

Remark: Let $f(X) \in K[X]$ be a nonconstant polynomial of degree n having distinct roots $\alpha_1, \ldots, \alpha_n$. Let $L = K(\alpha_1, \ldots, \alpha_n)$ be the splitting field of $f(X)$ over K. Then $\mathrm{Gal}(L/K)$ is called the Galois group of $f(X)$ over K, and may be denoted by G_f. Note that a K–automorphism of L gives a permutation of the n roots $\alpha_1, \ldots, \alpha_n$, which uniquely determines this automorphism. Thus G_f can be considered as a subgroup of S_n, the group of all permutations of n symbols. A more concrete definition of G_f, which doesn't involve automorphisms, is as follows.

$$G_f = \{\sigma \in S_n : \Phi(\alpha_{\sigma(1)}, \ldots, \alpha_{\sigma(n)}) = 0 \text{ for all } \Phi \in K[X_1, \ldots, X_n] \text{ with } \Phi(\alpha_1, \ldots, \alpha_n) = 0\}.$$

Exercise 15: Let $f(X)$ and G_f be as in the above Remark. Prove that $f(X)$ is irreducible if and only if G_f is transitive. [A subgroup H of S_n is said to be *transitive* if for any $i, j \in \{1, \ldots, n\}$, there exists $\sigma \in H$ such that $\sigma(i) = j$.]

Exercise 16: Let F be a finite field containing q elements and E be a finite extension of F. Show that E/F is a Galois extension and that $\mathrm{Gal}(E/F)$ is cyclic; in fact, the "Frobenius map" $\alpha \mapsto \alpha^q$ defines an F–automorphism of E, which generates $\mathrm{Gal}(E/F)$.

Definition: A Galois extension L/K is said to be *abelian* (resp: *cyclic*) if its Galois group $\mathrm{Gal}(L/K)$ is abelian[9] (resp: cyclic).

Exercise 17: Let E and F be subfields of a field L and K be a subfield of $E \cap F$. Let EF denote the smallest subfield of L containing E and F (this looks like $\{\sum \alpha_i \beta_i : \alpha_i \in E,\ \beta_i \in F\}$, and is called the *compositum* of E and F). Show that if E/K is Galois, then so is EF/F, and that $\sigma \mapsto \sigma|_E$ is an injective homomorphism of $\mathrm{Gal}(EF/F)$ into $\mathrm{Gal}(E/K)$ which is an isomorphism if $K = E \cap F$. Also show that if E/K and F/K are Galois and $K = E \cap F$, then $\mathrm{Gal}(EF/K) \simeq \mathrm{Gal}(E/K) \times \mathrm{Gal}(F/K)$. In particular, if $\mathrm{Gal}(E/K)$ and $\mathrm{Gal}(F/K)$ are abelian, then so is $\mathrm{Gal}(EF/K)$, and thus one can talk of the *maximal abelian extension* of K in L.

Exercise 18: Let L/K be a Galois extension and $G = \mathrm{Gal}(L/K)$. Let H be the commutator subgroup of G, i.e, the subgroup generated by the elements $\sigma\tau\sigma^{-1}\tau^{-1}$ as σ, τ vary over elements of G. Show that H is a normal subgroup of G and the fixed field L^H is an abelian extension of K with $\mathrm{Gal}(L^H/K)$ isomorphic to the 'abelianization' of G, viz., G/H. Further show that L^H is, in fact, the maximal abelian extension of K contained in L.

There is more to Galois Theory than what has been discussed so far. Our objectives being limited, we haven't said anything about computing the Galois group of a given polynomial or a given extension. No general method is known. There are, however, various techniques which sometimes help in determining the Galois group. It may be mentioned that one of the major open problems in the area, called the Inverse Problem of Galois Theory or the Construction Problem of Number Theory, is whether any finite group G is the Galois group of some (normal) extension of $\mathbb{Q}$.[10] As an aid for further studies, we give below a list of relevant books with some (highly subjective) remarks.

Annotated List of References for Galois Theory

Books on Galois Theory, or Abstract Algebra in general, seem quite abundant these days. We will mention only a few.

[1] E. Artin, *Galois Theory*, 2nd Ed., Notre Dame Press, 1956.
a classic little text on which most of the modern treatments of Galois theory are based.

[2] M. Artin, *Algebra*, Prentice Hall Inc., 1991 (Ch. 14).
a novel text on Algebra with a friendly introduction to the rudiments of Galois Theory.

[3] H. Edwards, *Galois Theory*, Springer GTM 101, 1984.
a historically guided treatment; contains a translation of Galois' original memoirs.

[4] I. Herstein, *Topics in Algebra*, 2nd Ed., John Wiley, 1975 (Ch. V).
elementary and rather verbose; well–suited for an undergraduate course.

[9] The term 'abelian' is derived from the name of the Norwegian mathematician N. H. Abel who proved, around 1829, that a certain class of equations is always solvable by radicals. In the modern terminology, this is precisely the class of equations whose Galois group is commutative. The usage of 'abelian' seems to have been initiated by L. Kronecker who, in 1853, announced that *the roots of every abelian equation with integer coefficients can be represented as rational functions of roots of unity*, a result which is nowadays known as the Kronecker–Weber Theorem and is usually expressed as: *every abelian extension of $\mathbb{Q}$ is contained in a cyclotomic field.* In an 1870 paper, Kronecker formally defined "abstract abelian groups" and proved what is now known as the Structure Theorem for Finite Abelian Groups. To get an idea of Abel's work on solvability by radicals, see Van der Waerden's enchanting book "A History of Algebra", Springer (1985), or the article 'Niels Hendrick Abel and the equations of fifth degree' by M. Rosen in the *American Math. Monthly*, Vol. 102 (1995), pp. 495–505.

[10] It is not difficult to see that the answer is Yes if G is an abelian group. For recent work on this problem, see the article by B. Matzat in the MSRI Proceedings on "Galois groups over $\mathbb{Q}$" published by Springer (1988) or the book " Groups as Galois groups" by H. Völklein (Cambridge University Press, 1996).

[5] T. Hungerford, *Algebra*, Springer GTM 73, 1980 (Ch. V).
a useful reference; contains a treatment applying also to infinite extensions.
[6] N. Jacobson, *Basic Algebra I*, 2nd Ed., W. H. Freeman, 1985 (Ch. IV).
the introduction to the chapter is highly readable and informative; the 2nd Ed. has a valuable section on mod p reduction.
[7] S. Lang, *Algebra*, 2nd Ed., Addison–Wesley, 1984 (Ch. VII, VIII).
a neat exposition of the elements of Galois theory as well as more advanced material; contains a good collection of exercises.
[8] TIFR Mathematical Pamphlet on *Galois Theory*, No. 3, 1965.
short, self–contained, neat, and thorough; seek elsewhere for motivation and history.

A.6 Norms and Traces

In the study of finite field extensions L/K, a useful passage from L to K is provided by the functions called Norm and Trace. These notions can be used in defining the so called discriminant, which plays an important role in Number Theory.

Definition: Let L/K be a finite extension of degree n and α be any element of L. Let (a_{ij}) be an $n \times n$ matrix, with entries in K, corresponding to the K–linear transformation $x \mapsto \alpha x$ of L into itself, i.e., for some K–basis $\{u_1, \ldots, u_n\}$ of L, we have

$$\alpha u_i = \sum_{j=1}^{n} a_{ij} u_j \quad i = 1, \ldots, n.$$

The *trace* of α w.r.t. L/K, denoted by $\mathrm{Tr}_{L/K}(\alpha)$ or simply $\mathrm{Tr}(\alpha)$, is defined by

$$\mathrm{Tr}(\alpha) = \sum_{i=1}^{n} a_{ii}.$$

The *norm* of α w.r.t. L/K, denoted by $N_{L/K}(\alpha)$ or simply $N(\alpha)$, is defined by

$$N(\alpha) = \det(a_{ij}).$$

We also define the *field polynomial* of α w.r.t. L/K [11] to be the polynomial $\Phi(X) \in K[X]$ given by

$$\Phi(X) = \det(X\delta_{ij} - a_{ij}) \quad \text{[where } \delta_{ij} \text{ is the Kronecker delta]}.$$

Note that $\mathrm{Tr}_{L/K}(\alpha)$, $N_{L/K}(\alpha)$, and $\Phi(X)$ are independent of the choice of a K–basis of L, and depend only upon the extension L/K and the element α.

Lemma 17: *Let L/K be a finite extension of degree n and $\alpha \in L$. Then:*
(1) $\mathrm{Tr}_{L/K}$ is a K–linear map, i.e.,

$$\mathrm{Tr}_{L/K}(a\alpha + b\beta) = a\mathrm{Tr}_{L/K}(\alpha) + b\mathrm{Tr}_{L/K}(\beta) \quad \forall\, a, b \in K,\ \alpha, \beta \in L.$$

(2) $N_{L/K}$ is multiplicative, i.e.,

$$N_{L/K}(\alpha\beta) = N_{L/K}(\alpha) N_{L/K}(\beta) \quad \forall\, \alpha, \beta \in L.$$

(3) For any $a \in K$, we have

$$\mathrm{Tr}_{L/K}(a) = na \quad \textit{and} \quad N_{L/K}(a) = a^n.$$

[11] this is sometimes called the *characteristic polynomial* of α w.r.t. L/K; indeed, it is the characteristic polynomial of the matrix (a_{ij}) [or the corresponding linear transformation] in the sense of Linear Algebra.

Proof: Assertions (1) and (2) follow from the fact that $(aa_{ij} + bb_{ij})$ and $(\sum_{k=1}^{n} b_{ik}a_{kj})$ are $n \times n$ matrices corresponding to the K–linear transformations $x \mapsto (a\alpha + b\beta)x$ and $x \mapsto (\alpha\beta)x$, where (a_{ij}) and $b_{(ij)}$ are $n \times n$ matrices corresponding to the K–linear transformations $x \mapsto \alpha x$ and $x \mapsto \beta x$. Moreover, for any $a \in K$, $(a\delta_{ij})$ is a matrix corresponding to the K–linear transformation $x \mapsto ax$, and hence we get (3). □

Note that a field polynomial is monic of degree equal to the degree of the corresponding extension. Its relation to the trace and the norm is given in the following

Lemma 18: *Let L/K be a finite extension of degree n and $\alpha \in L$. Let $\Phi(X) = X^n + a_1X^{n-1} + \cdots + a_n$ be the field polynomial of α w.r.t. L/K. Then $\mathrm{Tr}_{L/K}(\alpha) = -a_1$ and $N_{L/K}(\alpha) = (-1)^n a_n$.*

Proof: Let a_{ij} be a matrix corresponding to the K–linear transformation $x \mapsto \alpha x$ of L into itself. Expanding $\det(X\delta_{ij} - a_{ij})$, it is easily seen that the coefficient of X^{n-1} is $-(a_{11} + \cdots + a_{nn})$ and the constant coefficient is $(-1)^n \det(a_{ij})$. □

Lemma 19: *Let L/K be a finite extension, $\alpha \in L$, and $\Phi(X)$ be the field polynomial of α w.r.t. L/K. Suppose E is a subfield of L containing K such that $\alpha \in E$ and $\Psi(X)$ is the field polynomial of α w.r.t. E/K. Then*

$$\Phi(X) = \Psi(X)^{[L:E]}$$

and, in particular,

$$\mathrm{Tr}_{L/K}(\alpha) = [L : E]\left(\mathrm{Tr}_{E/K}(\alpha)\right) \quad \textit{and} \quad N_{L/K}(\alpha) = \left(N_{L/E}(\alpha)\right)^{[L:E]}.$$

Proof: Let $\{u_1, \ldots u_r\}$ be an E–basis of L and $\{v_1, \ldots, v_s\}$ be a K–basis of E. Then $\{u_iv_j : 1 \le i \le r,\ 1 \le j \le s\}$, ordered lexicographically (say), is a K–basis of L. If (a_{jl}) is the $s \times s$ matrix such that

$$\alpha v_j = \sum_{l=1}^{s} a_{jl}v_l \quad j = 1, \ldots, s$$

then, for $1 \le i \le r$ and $1 \le j \le s$, we have

$$\alpha(u_iv_j) = \sum_{l=1}^{s} a_{jl}(u_iv_l) = \sum_{\substack{1 \le k \le r \\ 1 \le l \le s}} a_{jl}\delta_{ik}(u_kv_l).$$

Now $(a_{jl}\delta_{ik})$ [where (i, j) and (k, l) vary, in a lexicographic order, over the set $\{1, \ldots, r\} \times \{1, \ldots, s\}$] is the $rs \times rs$ matrix corresponding to the K–linear transformation $x \mapsto \alpha x$ of L into itself. The $rs \times rs$ identity matrix can be represented as $(\delta_{ik}\delta_{jl})$, and so

$$\Phi(X) = \det\left(X\delta_{ik}\delta_{jl} - a_{jl}\delta_{ik}\right) = \det\left(\delta_{ik}[X\delta_{jl} - a_{jl}]\right) = \left[\det\left(X\delta_{jl} - a_{jl}\right)\right]^r.$$

Thus $\Phi(X) = \Psi(X)^{[L:E]}$. The rest is evident. □

Corollary: *Let L/K be a finite extension and $\alpha \in L$. Then the field polynomial $\Phi(X)$ of α w.r.t. L/K is a power of the minimal polynomial of α over K. In fact, $\Phi(X) = [\mathrm{Irr}(\alpha, K)]^{[L:K(\alpha)]}$.*

Proof: Let $\Psi(X)$ be the field polynomial of α w.r.t. $K(\alpha)/K$. Then $\Psi(X)$ is a monic polynomial in $K[X]$ with $\Psi(\alpha) = 0$ and $\deg \Psi(X) = [K(\alpha) : K] = \deg \mathrm{Irr}(\alpha, K)$. Hence $\Psi(X) = \mathrm{Irr}(\alpha, K)$. Our assertion now follows from the previous Lemma. □

Remark: The field polynomial is usually easy to compute and, in view of the above results, it often helps in finding the minimal polynomial.

We now proceed to give an alternative expression for the trace and norm.

Definition: Two elements α and α' in an extension of a field K are said to be *conjugates* of each other if there exists a K–isomorphism of $K(\alpha)$ onto $K(\alpha')$ which maps α to α'.

Note that, in view of Lemma 9, α and α' are conjugates over K if and only if they have the same minimal polynomial over K. Also note that α and α' are conjugates over K if and only if $\alpha' = \sigma(\alpha)$ for some K–homomorphism σ of $K(\alpha)$ into an extension of K containing α'.

Let L/K be a finite separable extension of degree n, $\alpha \in L$, and N be a normal extension of K containing L [such N exists by Exercise 7; it can, for example, be the least Galois extension of K containing L]. By Lemma 12 and the Corollary to Lemma 9, we see that there exist exactly n distinct K–isomorphisms $\sigma_1, \ldots, \sigma_n$ of L into N. Clearly, $\sigma_i(\alpha)$ and α are conjugates over K for each i with $1 \leq i \leq n$. The n elements $\sigma_1(\alpha), \ldots, \sigma_n(\alpha)$ will be called the *conjugates of α w.r.t. L/K*; these are uniquely determined provided we fix our N. Note that these n elements need not be distinct; in fact, the number of distinct conjugates among these is $[K(\alpha) : K]$ and each of these is repeated exactly $[L : K(\alpha)]$ times. (This follows from Exercise 12. Verify!)

Lemma 20: *Let L/K be a finite separable extension of degree n and $\alpha \in L$. Fix a normal extension N of K containing L. Then:*

(1) $\mathrm{Tr}_{L/K}(\alpha)$ is the sum of all conjugates of α w.r.t. L/K. In particular, if L/K is Galois, then

$$\mathrm{Tr}_{L/K}(\alpha) = \sum_{\sigma \in \mathrm{Gal}(L/K)} \sigma(\alpha).$$

(2) $N_{L/K}(\alpha)$ is the product of all conjugates of α w.r.t. L/K. In particular, if L/K is Galois, then

$$N_{L/K}(\alpha) = \prod_{\sigma \in \mathrm{Gal}(L/K)} \sigma(\alpha).$$

Proof: Let $r = [L : K(\alpha)]$ and $s = [K(\alpha) : K]$. If $\tau_1, \ldots, \tau_r$ are the distinct K–homomorphisms of $K(\alpha)$ into N, then $\tau_1(\alpha), \ldots, \tau_s(\alpha)$ are precisely the distinct conjugates of α w.r.t. L/K and the minimal polynomial of α over K factors as

$$\mathrm{Irr}(\alpha, K) = \prod_{j=1}^{s} (X - \tau_j(\alpha))$$

Now the conjugates $\sigma_1(\alpha), \ldots, \sigma_n(\alpha)$ of α w.r.t. K are nothing but $\tau_1(\alpha), \ldots, \tau_s(\alpha)$ each repeated r times. Hence, by the Corollary to Lemma 19, we see that

$$\Phi(X) = \prod_{i=1}^{n} (X - \sigma_i(\alpha))$$

where $\Phi(X)$ denotes the field polynomial of α w.r.t. L/K. In view of Lemma 18, the above identity readily implies (1) and (2). □

Remark: In the above Lemma and the discussion preceding that, we could have replaced N by an algebraic closure[12] of K (assumed to contain L). Fixing an algebraic closure $\overline{K}$ of K, one can define $\mathrm{Gal}(L/K)$, for any separable extension L/K with $L \subseteq \overline{K}$, to be the set of all K–homomorphisms of L into $\overline{K}$. With this convention, the displayed identities for the trace and norm in Lemma 20 remain valid for any finite separable extension L/K. Our definition of $\mathrm{Gal}(L/K)$ applies only to Galois extensions but it has the advantage that we don't have to talk about algebraic closures, and that we can legitimately call it the Galois *group*.

Exercise 19: Let L/K be a finite separable extension and E be a subfield of L containing K. Prove the following transitivity properties of the trace and norm.

$$\mathrm{Tr}_{L/K} = \mathrm{Tr}_{E/K} \circ \mathrm{Tr}_{L/E} \quad \text{and} \quad N_{L/K} = N_{E/K} \circ N_{L/E}.$$

[12] By an *algebraic closure* of a field K we mean an algebraic extension $\overline{K}$ of K such that every nonconstant polynomial in $\overline{K}[X]$ has a root in $\overline{K}$. It can be shown that every field K has an algebraic closure with the property that any algebraic extension of K is isomorphic to some subfield of it; further any two algebraic closures of K are K–isomorphic. For details, see Lang's "Algebra".

Appendix B

Discriminants in Algebra and Arithmetic[1]

We begin with the familiar notion of the discriminant of a quadratic and discuss how it can be extended to more general situations. We also outline some important applications of the notion of discriminant in Algebra and Arithmetic.

B.1 Discriminant in High School Algebra

Usually, we first come across discriminants in High School when we study the quadratic equation

$$aX^2 + bX + c = 0. \tag{B.1}$$

The quantity $\Delta = b^2 - 4ac$ is called the discriminant of (B.1) and it has the quintessential property:

$$\Delta = 0 \iff \text{the equation (B.1) has a repeated root.} \tag{B.2}$$

Strictly speaking, (B.2) holds if (B.1) is a genuine quadratic, i.e., if $a \neq 0$. Indeed, if $a \neq 0$ and if α, β are the roots of (B.1), then we have

$$aX^2 + bX + c = a(X - \alpha)(X - \beta) \tag{B.3}$$

or equivalently

$$\alpha + \beta = \frac{-b}{a} \quad \text{and} \quad \alpha\beta = \frac{c}{a}.$$

Thus from the simple identity $(\alpha - \beta)^2 = (\alpha + \beta)^2 - 4\alpha\beta$, it follows that

$$\Delta = a^2(\alpha - \beta)^2. \tag{B.4}$$

Note that the above expression makes it obvious that the property (B.2) holds.

We now consider the problem of suitably defining the discriminant of a general equation

$$f(X) = 0$$

where f is a polynomial of degree n, i.e.,

$$f(X) = a_0X^n + a_1X^{n-1} + \cdots + a_{n-1}X + a_n, \quad \text{with } a_0 \neq 0. \tag{B.5}$$

[1]This appendix is a *verbatim* reproduction of an article with the same title published in *Bona Mathematica*, Vol. 11, No. 2-3 (2000), pp. 43–62.

Let us assume that f is a nonconstant polynomial, i.e., $n \geq 1$. What should the discriminant of f be? Burnside and Panton (1892) answer this nicely by saying that the *discriminant* ought to be the *simplest function of the coefficients in a rational and integral form, whose vanishing expresses the condition for equal roots.* Let $\alpha_1, \ldots, \alpha_n$ denote the roots[2] of f so that

$$f(X) = a_0(X - \alpha_1)\ldots(X - \alpha_n). \tag{B.6}$$

As a first guess for the discriminant of f, it seems natural to consider an expression such as

$$V_f = \prod_{1 \leq i < j \leq n} (\alpha_i - \alpha_j).$$

This is certainly a simple function whose vanishing expresses the condition for repeated roots. But it isn't really a function of the coefficients, even in the case of a quadratic. So we take a cue from (B.4), and consider

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

Now this is a *symmetric* polynomial function in $\alpha_1, \ldots, \alpha_n$, in the sense that it is unchanged if we permute $\alpha_1, \ldots, \alpha_n$. We have a fundamental result going back to Newton which says that every symmetric polynomial can be expressed as a polynomial in the 'elementary symmetric functions'. The *elementary symmetric functions* in $\alpha_1, \ldots, \alpha_n$ are as follows.

$$\begin{aligned} e_1 &= \alpha_1 + \cdots + \alpha_n = \sum_{1 \leq i \leq n} \alpha_i \\ e_2 &= \alpha_1\alpha_2 + \cdots + \alpha_{n-1}\alpha_n = \sum_{1 \leq i < j \leq n} \alpha_i\alpha_i \\ &\vdots \\ e_n &= \alpha_1 \ldots \alpha_n. \end{aligned}$$

From (B.5) and (B.6), we see that

$$e_1 = \frac{-a_1}{a_0},\ e_2 = \frac{a_2}{a_0},\ \ldots,\ e_n = \frac{(-1)^n a_n}{a_0}. \tag{B.7}$$

Thus it follows from Newton's Theorem on symmetric functions, that any symmetric polynomial in $\alpha_1, \ldots, \alpha_n$ is a polynomial in $e_1, \ldots, e_n$, and hence it equals a polynomial in the coefficients $a_0, a_1, \ldots, a_n$ divided by some power of a_0. In the case of V_f^2, the degree in α_1 is $2(n-1)$, and since each e_i is of degree 1 in α_1, we see that the degree of V_f^2 in $e_1, \ldots, e_n$ is at most $2(n-1)$. Thus $a_0^{2n-2} V_f^2$ would be a polynomial in $a_0, a_1, \ldots, a_n$ with integral coefficients. We are now ready to make a formal definition.

Definition B.1. The *discriminant* of f, denoted by $\mathrm{Disc}(f)$, is defined by

$$\mathrm{Disc}(f) = a_0^{2n-2} \prod_{1 \leq i < j \leq n} (\alpha_i - \alpha_j)^2.$$

[2]It may be worthwhile to digress here a bit to discuss the idea of *roots* of a polynomial. If our polynomial $f(X)$ has complex coefficients (in particular, integral, rational or real coefficients), then the Fundamental Theorem of Algebra assures us that it has exactly n roots in $\mathbb{C}$, when counted with multiplicities. Recall that α is said to be a root of *multiplicity* m if $f(X) = (X - \alpha)^m g(X)$ for some polynomial $g(X)$ with $g(\alpha) \neq 0$. In case $m > 1$, we say that α is a *multiple root* or a *repeated root* of f. In general, if A is an integral domain and $f \in A[X]$ (i.e., f is a polynomial in X with coefficients in A), then for any integral domain B containing A as a subring, f has at most n roots in B. Moreover, there exists a field L containing A as a subring such that f has exactly n roots in L when counted with multiplicities. Thus abstractly speaking, by suitably enlarging the domain, if necessary, we can always consider n elements $\alpha_1, \ldots, \alpha_n$ which are the roots of f. Here each root is repeated as many times as its multiplicity.

From the definition of $\mathrm{Disc}(f)$, the following result is evident.

Theorem B.2. $\mathrm{Disc}(f) = 0 \iff f$ *has a repeated root.* □

Although our definition of $\mathrm{Disc}(f)$ meets all the basic requirements, the situation is still unsatisfactory because for any practical use of the above theorem, we should not have to find the $\mathrm{Disc}(f)$ by first finding the roots of f. In other words, it is highly desirable to have a concrete expression for $\mathrm{Disc}(f)$ purely in terms of the coefficients $a_0, a_1, \ldots, a_n$ of f. This is not so easy (try the case of $n = 3$)! But we can give a nice expression for $\mathrm{Disc}(f)$ if we know the classical notion of resultant. Let us quickly recall some basics concerning resultants. We refer to [21] for more on this topic.

Definition B.3. Given any two polynomials

$$f(X) = a_0X^n + \cdots + a_n \quad \text{and} \quad g(X) = b_0X^m + \cdots + b_m, \tag{B.8}$$

the *resultant* of $f(X)$ and $g(X)$ is defined to be the $(m+n) \times (m+n)$ determinant

$$\begin{vmatrix}
a_0 & a_1 & & \cdots\cdots & & a_n & & \\
 & a_0 & a_1 & \cdots\cdots & & a_{n-1} & a_n & \\
 & & & \cdots\cdots\cdots & \cdots\cdots & & & \\
 & & & & a_0 & a_1 & \cdots\cdots & a_n \\
b_0 & b_1 & & \cdots\cdots & & b_m & & \\
 & b_0 & b_1 & \cdots\cdots & & b_{m-1} & b_m & \\
 & & & \cdots\cdots\cdots & \cdots\cdots & & & \\
 & & & & b_0 & b_1 & \cdots\cdots & b_m
\end{vmatrix}
\begin{matrix} \left.\vphantom{\begin{matrix}a\\a\\a\\a\end{matrix}}\right\} m \text{ rows} \\ \left.\vphantom{\begin{matrix}a\\a\\a\\a\end{matrix}}\right\} n \text{ rows} \end{matrix}$$

where the blanks before a_0, b_0 and after a_n, b_m are to be filled with zeros. It is denoted by $\mathrm{Res}_X(f, g; n, m)$ or simply by $\mathrm{Res}(f, g)$.

An important fact about resultants is the following.

Theorem B.4 (Product Formula). *Let $f(X)$ and $\alpha_1, \ldots, \alpha_n$ be as in (B.5) and (B.6). Also let $g(X) = b_0X^m + b_1X^{m-1} + \cdots + b_m$ be a polynomial in X. Then*

$$\mathrm{Res}(f, g) = a_0^m \prod_{i=1}^{n} g(\alpha_i).$$

Moreover, if $b_0 \neq 0$ and if $\beta_1, \ldots, \beta_n$ are the roots of g so that $g(X) = b_0 \prod_{j=1}^{m}(X - \beta_j)$, then

$$\mathrm{Res}(f, g) = (-1)^{mn} b_0^n \prod_{j=1}^{m} f(\beta_j) = a_0^m b_0^n \prod_{i=1}^{n}\prod_{j=1}^{m}(\alpha_i - \beta_j).$$

In particular, $\mathrm{Res}(f, g) = 0$ *if and only if f and g have a common root.*

We are now ready to relate resultants to discriminants and thereby get a concrete formula for $\mathrm{Disc}(f)$ in terms of the coefficients of f.

Theorem B.5. *Let $f(X) = a_0X^n + a_1X^{n-1} + \cdots + a_{n-1}X + a_n$ be a nonconstant polynomial of degree n. Let $f'(X)$ be the derivative of $f(X)$, i.e., $f'(X) = na_0X^{n-1} + (n-1)a_1X^{n-2} + \cdots + a_{n-1}$. Then*

$$\mathrm{Res}(f, f') \;=\; (-1)^{\frac{n(n-1)}{2}}\, a_0\, \mathrm{Disc}(f).$$

Proof: Let $\alpha_1, \ldots, \alpha_n$ be the roots of f. Then we have

$$f(X) \;=\; a_0 \prod_{i=1}^{n}(X-\alpha_i), \quad \text{and therefore} \quad f'(X) \;=\; a_0 \sum_{i=1}^{n}\prod_{\substack{j=1\\ j\neq i}}^{n}(X-\alpha_j).$$

Hence, using Theorem B.4, we see that $\mathrm{Res}(f,f')$ equals

$$a_0^{n-1}\prod_{i=1}^{n} f'(\alpha_i) \;=\; a_0^{n-1}\prod_{i=1}^{n} a_0 \prod_{\substack{j=1\\ j\neq i}}^{n}(\alpha_i-\alpha_j) \;=\; a_0^{2n-1}\prod_{i=1}^{n}\prod_{\substack{j=1\\ j\neq i}}^{n}(\alpha_i-\alpha_j).$$

Now if in the last product, we collate together the terms of the form $(\alpha_i-\alpha_j)$ and $(\alpha_j-\alpha_i)$ so as to get the corresponding term in the expression for $\mathrm{Disc}(f)$, then the number of sign changes required would be

$$\sum_{1\le i<j\le n} 1 \;=\; \sum_{i=1}^{n}\sum_{j=i+1}^{n} 1 \;=\; \sum_{i=1}^{n}(n-i) \;=\; \frac{n(n-1)}{2}.$$

(Alternatively, the number of sign-changes is the number of 2-element subsets $\{\alpha_i,\alpha_j\}_{i<j}$ of the n-element set $\{\alpha_1,\ldots,\alpha_n\}$, and so it is $\binom{n}{2} = \frac{n(n-1)}{2}$.) Therefore, we conclude that

$$\mathrm{Res}(f,f') \;=\; a_0^{2n-1}(-1)^{\frac{n(n-1)}{2}}\prod_{i=1}^{n}\prod_{\substack{j=1\\ i<j}}^{n}(\alpha_i-\alpha_j)^2 \;=\; (-1)^{\frac{n(n-1)}{2}}\, a_0\,\mathrm{Disc}(f). \qquad \square$$

Remark. The sign factor $(-1)^{\frac{n(n-1)}{2}}$ in the above result has, curiously, been missed by several mathematicians. For example, this error occurred in the first edition of Lang's *Algebra*. In the second edition [13, p. 211], Lang mentions that Serre has pointed out to him this error and also that it occurs in van der Waerden, Samuel, and Hilbert but not in Weber. Indeed, the error occurs in van der Waerden's *Algebra* [23, p. 82], the original French edition of Samuel's *Algebraic Theory of Numbers* [17, p. 49] although not in its English translation. In the case of Hilbert, one might expect that the reference is to Hilbert's famous *Zahlbericht* (see [8, pp. 63–363] or the recent English translation [9]), but we have not been able to spot any error there. This may be because Hilbert's collected works were revised and corrected by Olga Taussky et al. On the other hand, Weber's *Textbook of Algebra*, written more than a century ago, is quite careful about the sign during the discussion of the discriminant (cf. [24, §50]).

Corollary B.6. *Let $f(X)$ and $\alpha_1,\ldots,\alpha_n$ be as in (B.5) and (B.6). Assume that $f'(X)$ is of degree $n-1$*[3] *and let $\beta_1,\ldots,\beta_{n-1}$ be the roots of $f'(X)$. Then*

$$\mathrm{Disc}(f) = (-1)^{\frac{n(n-1)}{2}} a_0^{n-2}\prod_{i=1}^{n} f'(\alpha_i) = (-1)^{\frac{n(n-1)}{2}} n^n a_0^{n-1}\prod_{j=1}^{n-1} f(\beta_j).$$

Proof: Follows easily from Theorem B.4 and Theorem B.5 by noting that $(-1)^{n(n-1)} = 1$. $\square$

Example: Consider a cubic polynomial of the form $f(X) = X^3 + pX + q$. To find $\mathrm{Disc}(f)$, we note that the roots of $f'(X) = 3X^2 + p$ are $\pm(-p/3)^{1/2}$. Therefore, by the second formula in the Corollary above, $\mathrm{Disc}(f)$ equals

$$\begin{aligned}
&(-1)^{\frac{3(2)}{2}}\, 3^3\left[(-p/3)^{3/2} + p(-p/3)^{1/2} + q\right]\left[-(-p/3)^{3/2} - p(-p/3)^{1/2} + q\right]\\
&= \;-27\left[q^2 - \left[(-p/3)+p\right]^2(-p/3)\right]\\
&= \;-27\left[q^2 + (4p^2/9)(p/3)\right]\\
&= \;-4p^3 - 27q^2.
\end{aligned}$$

[3] This is always the case if the coefficients are complex numbers or more generally, if n is not divisible by the characteristic.

More generally, if $f(X) = X^3 + aX^2 + bX + c$, then using the above method or by directly computing the resultant, it can be seen that

$$\mathrm{Disc}(f) = -4a^3c + a^2b^2 + 18abc - 4b^3 - 27c^2.$$

We leave it to the reader to verify this formula.

Exercise: Let $f(X)$ and $\alpha_1, \ldots, \alpha_n$ be as in the definition of the Discriminant. Assume that $f(X)$ is monic, i.e., $a_0 = 1$. Prove that $\mathrm{Disc}(f)$ equals the square of the Vandermonde determinant $\det\left(\alpha_i^{j-1}\right)$ corresponding to $\alpha_1, \ldots, \alpha_n$. Deduce that $\mathrm{Disc}(f)$ is also given by the determinant of the $n \times n$ matrix whose $(i,j)^{\text{th}}$ entry is the power sum symmetric function p_{i+j-2}. In other words, if for $k \geq 0$, $p_k = \alpha_1^k + \cdots + \alpha_n^k$, then show that

$$\mathrm{Disc}(f) = \begin{vmatrix} 1 & \alpha_1 & \ldots & \alpha_1^{n-1} \\ 1 & \alpha_2 & \ldots & \alpha_2^{n-1} \\ \vdots & & \ddots & \\ 1 & \alpha_n & \ldots & \alpha_n^{n-1} \end{vmatrix}^2 = \begin{vmatrix} p_0 & p_1 & \ldots & p_{n-1} \\ p_1 & p_2 & \ldots & p_n \\ \vdots & & \ddots & \\ p_{n-1} & p_n & \ldots & p_{2n-2} \end{vmatrix}.$$

B.2 Discriminant in College Algebra

In the B.Sc. and M.Sc. level courses in Algebra, where one mainly studies groups, rings, fields, etc., the notion of discriminant is encountered once again. Here, at least initially, it appears far removed from the classical or the high school algebra notion of discriminant. We will try to narrow this gap by first recalling the relevant definitions and then describing how the two seemingly different notions of discriminant are related to one another. In what follows, we will assume mild familiarity with the concepts such as rings, fields, vector spaces, and basic facts concerning them. We begin with a brief discussion of the notion of trace, and some of its properties, which are needed later. For proofs of these auxiliary results, one may refer to [6] or standard texts such as [13].

Let K be a field and L be a ring containing K as a subring. Then L is a vector space over K. We will assume that the vector space dimension of L over K is finite and denote it by $[L : K]$. A nice passage from L to K is provided by the *trace* map

$$\mathrm{Tr}_{L/K} : L \to K$$

which is defined as follows. Let $n = [L : K]$. Given any $\alpha \in L$, let t_α denote the linear transformation of $L \to L$ defined by $t_\alpha(x) = \alpha x$ for $x \in L$. Then we define $\mathrm{Tr}_{L/K}(\alpha)$, to be the trace of t_α. In other words, if $\{u_1, \ldots, u_n\}$ is a K-basis of L, and if $t_\alpha(u_j) = \sum_{i=1}^n a_{ij}u_i$ for some $a_{ij} \in K$ $(1 \leq j \leq n)$, then $\mathrm{Tr}_{L/K}(\alpha) = \sum_{i=1}^n a_{ii}$. The latter is easily seen to be independent of the choice of a basis. Some basic properties of the trace map Tr (we often drop the subscript L/K when it is clear from the context) are as follows.

(i) $\mathrm{Tr}_{L/K}$ is a K–linear map, i.e., $\mathrm{Tr}(au+bv) = a\mathrm{Tr}(u)+b\mathrm{Tr}(v)$ for all $a, b \in K$ and $u, v \in L$. Moreover, the restriction of $\mathrm{Tr}_{L/K}$ to K equals $[L : K]$ times the identity map, that is, $\mathrm{Tr}(a) = na.$ for $a \in K$.

(ii) Suppose L is a field such that $L = K(\alpha)$ for some $\alpha \in L$.[4] Let $f(X)$ be the *minimal polynomial* [5] of α over K. Assume that $f(X)$ has distinct roots, say $\alpha_1, \ldots, \alpha_n$. Then $\mathrm{Tr}(\alpha) = \alpha_1 + \cdots + \alpha_n$.

[4] By $K(\alpha)$ one denotes the smallest subfield of L containing K and α; it consists of all 'rational functions' $p(\alpha)/q(\alpha)$, where $p(X), q(X) \in K[X]$ with $q(\alpha) \neq 0$.

[5] A monic polynomial (i.e., a polynomial whose leading coefficient is 1) in $K[X]$ satisfied by α and of least possible degree is unique and is called the *minimal polynomial* of α over K. Its degree equals $[K(\alpha) : K]$. See [6], [11], [13] or [26] for more on this.

Remarks. 1. Suppose L is a field. Then K is a subfield of L and the finiteness of $[L:K] = \dim_K L$ implies that for each $\alpha \in L$, the minimal polynomial of α over K exists.[6] The roots $\alpha_1, \ldots, \alpha_d$ of this minimal polynomial are called the *conjugates* of α over K.

2. Suppose L is a field. If every $u \in L$ has distinct conjugates over K, then we say that L/K is *separable*. It can be shown that if K is any field containing rationals, then L/K is always separable. If L/K is separable (and $\dim_K L$ is finite), then the so called Primitive Element Theorem assures us that there exists some $\alpha \in L$ such that $L = K(\alpha)$; such an element α is called a *primitive element* in L.

3. Suppose L is a field such that L/K is a separable and u is any element of L. If we let d denote the degree of the minimal polynomial of u over K and $u_1, \ldots, u_d$ denote the roots of the minimal polynomial, then $n = de$, where $e = \dim_{K(u)} L$, and the n elements $u^{(1)}, \ldots, u^{(n)}$ obtained by taking each of $u_1, \ldots, u_d$ exactly e times, are called the *conjugates of u w.r.t. L/K*. We have $\mathrm{Tr}(u) = u^{(1)} + \cdots + u^{(n)}$.

Example. Consider $L = \mathbb{Q}(\sqrt{2}) = \{a + b\sqrt{2} : a, b \in \mathbb{Q}\}$. This is a field and a 2-dimensional vector space over $K = \mathbb{Q}$ with $\{1, \sqrt{2}\}$ as a basis. Given any $u = a + b\sqrt{2} \in L$, the matrix of the linear transformation t_u w.r.t. the above basis is easily seen to be

$$\begin{pmatrix} a & b \\ 2b & a \end{pmatrix}$$

and therefore $\mathrm{Tr}(u) = 2a$. Alternately, u satisfies the polynomial

$$X^2 - 2aX + (a^2 - 2b^2) = \left(X - (a + b\sqrt{2})\right)\left(X - (a - b\sqrt{2})\right)$$

and this is the minimal polynomial of u if $b \neq 0$. Therefore $a + b\sqrt{2},\ a - b\sqrt{2}$ are the conjugates of u w.r.t. L/K and the last equality in the Remark above is verified.

We are now ready to define the notion of discriminant in the set-up of the ring L containing a field K as a subring and such that $\dim_K L = n$ is finite.

Definition B.7. Given any n elements $u_1, \ldots, u_n \in L$, the *discriminant* $D_{L/K}(u_1, \ldots, u_n)$ of $u_1, \ldots, u_n$ w.r.t. L/K is defined to be the determinant of the $n \times n$ matrix $\left(\mathrm{Tr}_{L/K}(u_i u_j)\right)$.

Note that $D_{L/K}(u_1, \ldots, u_n)$ is an element of K.

Lemma B.8. *If $u_1, \ldots, u_n \in L$ are such that $D_{L/K}(u_1, \ldots, u_n) \neq 0$, then $\{u_1, \ldots, u_n\}$ is a K–basis of L.*

Proof: It suffices to show that $u_1, \ldots, u_n$ are linearly independent over K. Suppose $\sum_{i=1}^n c_i u_i = 0$ for some $c_1, \ldots, c_n \in K$. Multiplying the equation by u_j and taking the trace, we find that $\sum_{i=1}^n c_i \mathrm{Tr}(u_i u_j) = 0$. By hypothesis, the matrix $\left(\mathrm{Tr}_{L/K}(u_i u_j)\right)$ is nonsingular. Hence it follows that $c_j = 0$ for $j = 1, \ldots, n$. □

Lemma B.9. *If $\{u_1, \ldots, u_n\}$ and $\{v_1, \ldots, v_n\}$ are two K–bases of L and $u_i = \sum_{j=1}^n a_{ij} v_j,\ \ a_{ij} \in K$, then we have*

$$D_{L/K}(u_1, \ldots, u_n) = [\det(a_{ij})]^2 D_{L/K}(v_1, \ldots, v_n).$$

In particular, since (a_{ij}) is nonsingular, we have

$$D_{L/K}(u_1, \ldots, u_n) = 0 \iff D_{L/K}(v_1, \ldots, v_n) = 0.$$

[6] Indeed, since $n = \dim_K L$, the set $\{1, \alpha, \ldots, \alpha^n\}$ of $n+1$ elements must be linearly dependent over K, and thus α satisfies a nonzero polynomial of degree $\leq n$ over K. This, or any nonzero polynomial satisfied by α, can easily be made monic upon dividing by its leading coefficient.

Proof: For any $i, j \in \{1, \ldots, n\}$, we have

$$u_i u_j = \left(\sum_{k=1}^{n} a_{ik} v_k \right) u_j = \sum_{k=1}^{n} a_{ik} v_k \left(\sum_{l=1}^{n} a_{jl} v_l \right) = \sum_{k=1}^{n} \sum_{l=1}^{n} a_{ik} a_{jl} v_k v_l .$$

Taking trace of both sides, and letting A denote the matrix (a_{ij}), we see that

$$(\mathrm{Tr}(u_i u_j)) = A^{\mathrm{t}} \, (\mathrm{Tr}(v_i v_j)) \, A$$

and so the result follows. □

Remark: We shall say that the discriminant of L/K is zero (or nonzero) and write $D_{L/K} = 0$ (or $D_{L/K} \neq 0$) if for some K–basis $\{u_1, \ldots, u_n\}$ of L, the quantity $D_{L/K}(u_1, \ldots, u_n)$ is zero (or nonzero). The last lemma justifies this terminology.

We are now ready to describe the link between the two notions of discriminant considered in this and the previous section.

Theorem B.10. *Suppose L is a field and L/K is a separable. Then the discriminant of L/K is nonzero. In fact, if α is a primitive element (so that $L = K(\alpha)$ and $\{1, \alpha, \alpha^2, \ldots, \alpha^{n-1}\}$ is a K–basis of L) and $f(X)$ is its minimal polynomial, then we have*

$$D_{L/K}(1, \alpha, \alpha^2, \ldots, \alpha^{n-1}) \;=\; \prod_{i>j} (\alpha_i - \alpha_j)^2 \;=\; \mathrm{Disc}(f)$$

where $\alpha_1, \alpha_2, \ldots, \alpha_n$ denote the conjugates of α.

Proof: Since L/K is separable, the trace of any element of L equals the sum of its conjugates w.r.t. L/K. Thus if $\{u_1, \ldots, u_n\}$ is a K–basis of L and ${u_i}^{(1)}, {u_i}^{(2)}, \ldots, {u_i}^{(n)}$ denote the conjugates of u_i w.r.t. L/K, then we have $\mathrm{Tr}(u_i u_j) = \sum_{k=1}^{n} u_i^{(k)} u_j^{(k)}$. In other words, the matrix $(\mathrm{Tr}(u_i u_j))$ equals the product of the matrix $\left(u_i^{(j)} \right)$ with its transpose. Therefore

$$D_{L/K}(u_1, \ldots, u_n) \;=\; \begin{vmatrix} u_1^{(1)} & u_1^{(2)} & \ldots & u_1^{(n)} \\ u_2^{(1)} & u_2^{(2)} & \ldots & u_2^{(n)} \\ \vdots & \vdots & \ddots & \vdots \\ u_n^{(1)} & u_n^{(2)} & \ldots & u_n^{(n)} \end{vmatrix}^2 .$$

In case $u_1, u_2, \ldots, u_n$ are $1, \alpha, \ldots, \alpha^{(n-1)}$ respectively, then the determinant above is a Vandermonde determinant and the RHS becomes

$$\begin{vmatrix} 1 & 1 & \ldots & 1 \\ \alpha_1 & \alpha_2 & \ldots & \alpha_n \\ \vdots & \vdots & \ddots & \vdots \\ {\alpha_1}^{n-1} & {\alpha_2}^{n-1} & \ldots & {\alpha_n}^{n-1} \end{vmatrix}^2 = \prod_{i>j} (\alpha_i - \alpha_j)^2 \;=\; \prod_{i<j} (\alpha_i - \alpha_j)^2 .$$

Therefore, we obtain the desired formulae. Our first assertion follows from the fact that if $L = K(\alpha)$ is separable over K, then the conjugates $\alpha^{(1)}, \alpha^{(2)}, \ldots, \alpha^{(n)}$ of α w.r.t. L/K are distinct. □

Remark: The converse of the above Theorem, viz., if $D_{L/K} \neq 0$ then L/K is separable, is also true. For a proof, see [26].

B.3 Discriminant in Arithmetic

In Arithmetic, which we start learning even before entering high school, we mainly deal with numbers and their divisibility properties. A basic result is the

Fundamental Theorem of Arithmetic *Every nonzero integer can be factored as* ± 1 *times a finite product of prime numbers. Moreover, this decomposition is unique up to rearrangement of terms.*

In higher arithmetic, we are interested in knowing if such a result holds in domains more general than $\mathbb{Z}$, the ring of integers. An example of such a domain is

$$\mathbb{Z}[i] = \{a + bi : a, b \in \mathbb{Z}\}$$

This is a subring of $\mathbb{C}$, and is called the ring of *Gaussian integers*. Here i is the usual complex number whose square is -1. The notion of divisibility is easily defined in $\mathbb{Z}[i]$ or for that matter, in any ring.

Given a ring[7] A and elements $a, b \in A$, we say that b *divides* a, and write $b|a$, if $a = bc$ for some $c \in A$.

The analogue of a prime number is the so called irreducible element.

An element p in a ring A is said to be *irreducible* if $p \neq 0$, p is not a unit[8], and whenever $p = bc$ for some $b, c \in A$, either b is a unit or c is a unit.

For example, 5 is irreducible in $\mathbb{Z}$ but not in $\mathbb{Z}[i]$ since it decomposes as $5 = (2 + i)(2 - i)$. Further, the factors $2+i$ and $2-i$ can be shown to be irreducible elements which are distinct; in fact, they do not even differ by a unit. On the other hand, 3 remains prime in $\mathbb{Z}[i]$. Indeed, if $u = a + bi$ and $v = c + di$ are elements of $\mathbb{Z}[i]$ such that $3 = uv$, then by taking modulus (as complex numbers) and squaring, we have $9 = (a^2 + b^2)(c^2 + d^2)$. But the square of an integer is always $\equiv 0$ or $1 \pmod 4$, and so the sum of two squares is never $\equiv 3 \pmod 4$. Hence $a^2 + b^2 = 1$ or $c^2 + d^2 = 1$. This implies that either u or v is in $\{1, -1, i, -i\}$, i.e., either u is a unit or v is a unit. The prime 2 of $\mathbb{Z}$ is special. It splits in $\mathbb{Z}[i]$ as $2 = (1 + i)(1 - i)$ and the factors $1 \pm i$ are irreducible, but they aren't really distinct because they differ simply by a unit [indeed, $1 + i = i(1 - i)$ and so $2 = i(1 - i)^2$]. In general, a prime number p, when extended to $\mathbb{Z}[i]$

$$\begin{cases} \text{splits as a product of two distinct irreducibles} & \text{if } p \equiv 1 \pmod 4 \\ \text{remains irreducible} & \text{if } p \equiv 3 \pmod 4 \\ \text{equals unit times the square of an irreducible} & \text{if } p = 2. \end{cases}$$

Incidentally, for $p \equiv 1 \pmod 4$, the two irreducible factors in $\mathbb{Z}[i]$ must be (complex) conjugates of each other (prove!), and thus the result about the decomposition of such primes in $\mathbb{Z}[i]$ is equivalent to Fermat's Two Squares Theorem (viz., primes $\equiv 1 \pmod 4$ are sums of two squares).

The ring $\mathbb{Z}[i]$ is an example of the ring of algebraic integers (in a number field). The latter are defined as follows. A subfield K of $\mathbb{C}$, which is finite dimensional as a vector space over $\mathbb{Q}$ is called an *algebraic number field* or simply a *number field*. We call $\dim_{\mathbb{Q}} K$ the *degree* of $K/\mathbb{Q}$ and denote it by $[K : \mathbb{Q}]$. If K is a number field, then every element of K satisfies a nonzero polynomial with integer coefficients (check!). Those elements of K which satisfy a monic polynomial with integer coefficients are called (*algebraic*) *integers* in K. The set of all algebraic integers in K form a subring of K, called the ring of integers of K and denoted by $\mathcal{O}_K$.

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

1. Show that given any $u \in K$, there exists $d \in \mathbb{Z}$ such that $d \neq 0$ and $du \in \mathcal{O}_K$. Deduce that the quotient field of $\mathcal{O}_K$ is K and moreover, there exist a $\mathbb{Q}$-basis $\{u_1, \ldots, u_n\}$ of K such that $u_i \in \mathcal{O}_K$ for all $i = 1, \ldots, n$.

[7] By a ring we shall always mean a commutative ring with identity.

[8] Units in a ring A are defined to be the elements which divide 1. For example, 1, -1 are the only units in $\mathbb{Z}$.

2. Show that $\mathcal{O}_K \cap \mathbb{Q} = \mathbb{Z}$. In other words, if a rational number satisfies a monic polynomial with integer coefficients, then it must be an integer.

If $\{u_1, \ldots, u_n\}$ is a $\mathbb{Q}$-basis of K such that $\{u_1, \ldots, u_n\} \subseteq \mathcal{O}_K$, then from Exercise 2 above, we see that $D_{K/\mathbb{Q}}(u_1, \ldots, u_n)$ is an integer. Moreover, by Theorem B.10, it is a nonzero integer.

Lemma B.11. *Let $\{u_1, \ldots, u_n\} \subseteq \mathcal{O}_K$ be a $\mathbb{Q}$-basis of K with the property that $|D_{K/\mathbb{Q}}(u_1, \ldots, u_n)|$ is minimal. Then $\mathcal{O}_K = \mathbb{Z}u_1 + \cdots + \mathbb{Z}u_n$, i.e., $u \in \mathcal{O}_K$ if and only if $u = c_1u_1 + \cdots + c_nu_n$ for some $c_1, \ldots, c_n \in \mathbb{Z}$.*

Proof: It is clear that $\mathbb{Z}u_1 + \cdots + \mathbb{Z}u_n \subseteq \mathcal{O}_K$. If $u \in \mathcal{O}_K$, then we can write $u = r_1u_1 + \cdots + r_nu_n$ for some $r_1, \ldots, r_n \in \mathbb{Q}$. If $r_k \notin \mathbb{Z}$ for some k $(1 \leq k \leq n)$, then $r_k = m_k + \lambda$, where $m_k \in \mathbb{Z}$ and λ is a rational number with $0 < \lambda < 1$. Define $v_1, \ldots, v_n$ by $v_j = u_j$ if $j \neq k$ and $v_k = u - m_ku_k$. Then it is clear that $\{v_1, \ldots, v_n\} \subseteq \mathcal{O}_K$ and $\{v_1, \ldots, v_n\}$ is a $\mathbb{Q}$-basis of K. Moreover the matrix (a_{ij}) of rationals for which $v_i = \sum_{j=1}^{n} a_{ij}u_j$ for $i = 1, \ldots, n$, is the identity matrix except for the k–th row, which is given by $(r_1, \ldots, r_{k-1}, \lambda, r_{k+1}, \ldots, r_n)$. Thus in view of Lemma B.9, we see that

$$D_{K/\mathbb{Q}}(v_1, \ldots, v_n) = [\det(a_{ij})]^2 D_{K/\mathbb{Q}}(u_1, \ldots, u_n) = \lambda^2 D_{K/\mathbb{Q}}(u_1, \ldots, u_n).$$

Since $\lambda < 1$, the minimality of $|D_{K/\mathbb{Q}}(u_1, \ldots, u_n)|$ is contradicted. This proves the lemma. □

Definition B.12. A $\mathbb{Q}$-basis $u_1, \ldots, u_n$ of a number field K such that $\mathcal{O}_K = \mathbb{Z}u_1 + \cdots + \mathbb{Z}u_n$ is called an *integral basis* of K.

The above Lemma shows that every number field has an integral basis. Also, it is clear that if $\{u_1, \ldots, u_n\}$ and $\{v_1, \ldots, v_n\}$ are any two integral bases of K, then $v_i = \sum_{j=1}^{n} a_{ij}u_j$ for $j = 1, \ldots, n$, for some $n \times n$ matrix (a_{ij}) with integral entries. Moreover the inverse of (a_{ij}) is also a matrix with integral entries. Therefore, $\det(a_{ij}) = \pm 1$. Hence from Lemma B.9, it follows that any two integral bases of K have the same discriminant; it is called the *(absolute) discriminant of K* and is denoted by d_K.

The following example illustrates the computation of discriminant and determination of integral bases.

Example: Let K be a quadratic field [that is, a subfield of $\mathbb{C}$ such that $[K : \mathbb{Q}] = 2$] and $\mathcal{O}$ be its ring of integers. If α is any element of K which is not in $\mathbb{Q}$, then $1 < [\mathbb{Q}(\alpha) : \mathbb{Q}] \leq [K : \mathbb{Q}] = 2$, and hence $K = \mathbb{Q}(\alpha)$. Moreover, α satisfies a quadratic polynomial with integer coefficients, and thus $\alpha = a + b\sqrt{\Delta}$ for some $a, b \in \mathbb{Q}$ and $\Delta \in \mathbb{Z}$. Since $\alpha \notin \mathbb{Q}$, we must have $b \neq 0$ and Δ not a square. It follows that $K = \mathbb{Q}\left(\sqrt{\Delta}\right)$. Removing the extraneous square factors from Δ, if any, we can write $K = \mathbb{Q}(\sqrt{m})$, where m is a squarefree integer. We now attempt to give a more concrete description of $\mathcal{O}$. First, note that $\mathbb{Z}[\sqrt{m}] = \{r + s\sqrt{m} : r, s \in \mathbb{Z}\} \subseteq \mathcal{O}$. Let $x = a + b\sqrt{m} \in \mathcal{O}$ for some $a, b \in \mathbb{Q}$. Then the other conjugate $a - b\sqrt{m}$ of x must also be in $\mathcal{O}$. Therefore the sum of these two, i.e., $\mathrm{Tr}(x) = 2a$ and the product $a^2 - mb^2$ are both in $\mathcal{O}_K \cap \mathbb{Q} = \mathbb{Z}$. Since m is squarefree and $a^2 - mb^2 \in \mathbb{Z}$, we see that $a \in \mathbb{Z}$ if and only if $b \in \mathbb{Z}$. Thus if $a \notin \mathbb{Z}$, then we can find an odd integer a_1 such that $2a = a_1$, and relatively prime integers b_1 and c_1 with $c_1 > 1$ such that $b = \frac{b_1}{c_1}$. Now

$$\left(a_1 = 2a \in \mathbb{Z} \text{ and } a^2 - mb^2 \in \mathbb{Z}\right) \Rightarrow \left(4 | c_1^2 a_1^2 \text{ and } c_1^2 | 4mb_1^2\right) \Rightarrow c_1 = 2.$$

Hence b_1 is odd and $a_1^2 - mb_1^2 \equiv 0 (\mathrm{mod}\ 4)$. Also a_1 is odd, and therefore, $m \equiv 1 (\mathrm{mod}\ 4)$. It follows that if $m \not\equiv 1 (\mathrm{mod}\ 4)$, then $a, b \in \mathbb{Z}$, and so in this case,

$$\mathcal{O} = \mathbb{Z}[\sqrt{m}] = \{a + b\sqrt{m} : a, b \in \mathbb{Z}\} \text{ and } \{1, \sqrt{m}\} \text{ is an integral basis.}$$

In the case $m \equiv 1 (\mathrm{mod}\ 4)$, the preceding observations imply that

$$\mathcal{O} \subseteq \left\{ \frac{a_1 + b_1\sqrt{m}}{2} : a_1, b_1 \in \mathbb{Z} \text{ with } a_1 \equiv b_1 (\mathrm{mod}\ 2) \right\}$$

and, moreover, $\frac{1+\sqrt{m}}{2} \in \mathcal{O}$ since it is a root of $X^2 - X - \frac{m-1}{4}$; therefore

$$\mathcal{O} = \mathbb{Z}[\frac{1+\sqrt{m}}{2}] = \{\frac{a+b\sqrt{m}}{2} : a, b \in \mathbb{Z} \text{ with } a \equiv b (\text{mod } 2)\}$$

and consequently,

$$\{1, \frac{1+\sqrt{m}}{2}\} \text{ is an integral basis.}$$

We can now compute the discriminant of K as follows.

$$d_K = \begin{cases} \det \begin{pmatrix} 2 & 0 \\ 0 & 2m \end{pmatrix} = 4m & \text{if } m \equiv 2, 3 (\text{mod } 4) \\ \det \begin{pmatrix} 2 & 1 \\ 1 & (1+m)/2 \end{pmatrix} = m & \text{if } m \equiv 1 (\text{mod } 4). \end{cases}$$

It may be remarked that the integer $d = d_K$ determines the quadratic field K completely, and the set $\{1, \frac{d+\sqrt{d}}{2}\}$ is always an integral basis of K. (Verify!)

In general, the unique factorization property is not true in the ring of integers of a number field; in other words, the Fundamental Theorem of Arithmetic may not hold there. For example, if $K = \mathbb{Q}(\sqrt{-5})$, then from the example above, we have $\mathcal{O}_K = \mathbb{Z}[\sqrt{-5}]$, and for the number 6, we have two different factorizations:

$$6 = 3 \cdot 2 = (1 + \sqrt{-5})(1 - \sqrt{-5}).$$

It is not difficult to see that the factors $2, 3, 1 + \sqrt{-5}$ and $1 - \sqrt{-5}$ are irreducible and genuinely distinct (i.e., no two differ by a unit) in $\mathcal{O}_K = \mathbb{Z}[\sqrt{-5}]$. Around 1844, the German mathematician E. Kummer was studying arithmetic in the ring $\mathbb{Z}[\zeta]$ of cyclotomic integers[9] while trying to prove Fermat's Last Theorem[10]. Kummer realized that the unique factorization may not always hold in rings of cyclotomic integers. Instead of giving up the problem, he continued to delve deeper and made a remarkable discovery! He showed that the unique factorization property can be salvaged if we replace numbers by what he called ideal numbers. Another German mathematician R. Dedekind simplified and extended Kummer's work by using ideals in place of ideal numbers.[11] Dedekind's results were first published in 1871.[12] In effect, Dedekind showed that if K is a number field, then every nonzero ideal of $\mathcal{O}_K$ factors as a finite product of prime ideals, and this factorization is unique up to rearrangement of terms. Integral domains with this property are now known as *Dedekind domains*.

At any rate, if K is a number field and p is a prime number, then, thanks to the abovementioned result of Kummer-Dedekind-Kronecker, the extended ideal $p\mathcal{O}_K$ can be factored uniquely as

$$p\mathcal{O}_K = P_1^{e_1} P_2^{e_2} \cdots P_h^{e_h}$$

[9] If $\zeta = \zeta_n$ is a primitive n–th root of unity (e.g., $\zeta = e^{2\pi i/n} = \cos(2\pi/n) + i\sin(2\pi/n)$), then $\mathbb{Q}(\zeta)$ is a number field, called a *cyclotomic field* and its ring of integers is $\mathbb{Z}[\zeta] = \{a_0 + a_1\zeta + \cdots + a_{n-1}\zeta^{n-1} : a_0, a_1, \ldots, a_n \in \mathbb{Z}\}$, which is called the ring of cyclotomic integers.

[10] Fermat's Last Theorem (FLT) is the famous assertion of P. Fermat that the equation $x^n + y^n = z^n$ has no solution in nonzero integers, if $n \geq 3$. It is natural to consider the ring of cyclotomic integers here because the existence of a solution (x, y, z) yields a factorization $x^n = (y - z)(y - \zeta z) \ldots (y - \zeta^{n-1} z)$ in $\mathbb{Z}[\zeta]$ and to proceed further, it would be useful to know if the unique factorization property is valid in $\mathbb{Z}[\zeta]$. In a sense, Kummer didn't succeed in proving FLT (though he settled it for several values of n) because of the failure of unique factorization in $\mathbb{Z}[\zeta]$. Recently, in 1994 FLT has been proved by A. Wiles partly in collaboration with R. Taylor.

[11] In fact, the concept of an ideal of a ring was thus born in the work of Kummer and Dedekind. Note that these historical origins justify the nomenclature "ideal", which may otherwise seem obscure. Indeed, by considering ideals, the ideal situation (of unique factorization) is restored!

[12] Incidentally, another approach towards understanding and extending Kummer's work was developed by his student L. Kronecker, whose work was apparently completed in 1859 but was not published until 1882.

where $P_1, \ldots, P_h$ are distinct prime ideals of $\mathcal{O}_K$ and $e_1, \ldots, e_h$ are positive integers. The prime p is said to be *ramified* in K if $e_i > 1$ for some i.

Example: If $K = \mathbb{Q}(i)$, then 2 is the only ramified prime.

In general, to understand the phenomenon of ramification, the discriminant is an indispensable tool. This may be clear from the following basic result.

Theorem B.13 (Dedekind's Discriminant Theorem). *Let K be a number field and d_K be its discriminant. Then for any prime number p, we have*

$$p \text{ is ramified in } K \iff p | d_K.$$

Example: If $K = \mathbb{Q}(\sqrt{m})$, where m is a squarefree integer, then we have calculated the discriminant d_K of K. Thus, for any prime number p, we have:

$$p \text{ is ramified in } K \iff \begin{cases} p|m & \text{if } m \equiv 1 (\text{mod } 4) \\ p|m \text{ or } p = 2 & \text{if } m \not\equiv 1 (\text{mod } 4). \end{cases}$$

In the case of the cyclotomic field $K = \mathbb{Q}(\zeta_n)$, where n is any integer > 2 and ζ_n is a primitive n–the root of unity, the discriminant turns out[13] to be

$$d_K = (-1)^{\varphi(n)/2} \frac{n^{\varphi(n)}}{\prod_{p|n} p^{\varphi(n)/(p-1)}}$$

where the product in the denominator is over all prime numbers dividing n, and $\varphi(n)$ denotes the number of positive integers $\leq n$ and relatively prime to n. Therefore,

$$p \text{ is ramified in } \mathbb{Q}(\zeta_n) \iff p | n.$$

Remarks. 1. For a proof of Dedekind's discriminant Theorem, see [7] or the books of Lang [14] or Serre [19].
2. The notions of discriminant and resultant are no doubt classical and date back more than a century. However, extensions and generalizations (to 'higher dimensions') of these notions are of much current interest. For an introduction, see the expository article [22] by Sturmfels and the references therein. At a more advanced level, there is a book [5] by Gelfand, Kapranov and Zelevinsky, and the recently published review [3] by Catanese may be a good starting point for this.
3. It may be remarked that the phenomenon of ramification or rather the absence of ramification, is closely related to certain basic notions in Topology. Briefly speaking, unramified field extensions (i.e., extensions for which no prime 'below' is ramified 'above') correspond to (topological or unbranched) coverings. Thus, saying that a field has no unramified extensions, is analogous to the condition that the corresponding topological space is simply connected. Unfortunately, in the compartmentalized courses at College and University level, such analogies are rarely highlighted. Thus we might take this opportunity to mention the following brief and rough dictionary of some basic concepts from Algebra and Topology.

Algebraic Field Extensions $\longleftrightarrow$ Branched Coverings;
Galois extensions $\longleftrightarrow$ Regular Coverings;
Galois Groups $\longleftrightarrow$ Groups of Deck transformations.

For more on Coverings Spaces in particular, and Topology, in general, we recommend the classic text of Seifert and Threlfall [18] or the more recent book of Massey [15]. The first appendix in [16] also gives a nice and quick summary of the basics of covering spaces.

[13] For a proof of the discriminant formula for cyclotomic fields, one may refer to [25].

4. It is a nontrivial result of Minkowski that for any number field K other than $\mathbb{Q}$, we have $|d_K| > 1$. This means that there exists at least one prime number p which is ramified in K. Thus, we might say that $\mathbb{Q}$ is simply connected! Analogous result holds when $\mathbb{Q}$ is replaced by the field $\mathbb{C}(X)$ of rational functions in one variable with complex coefficients. This time, the topological analogue is the more familiar result that the Riemann sphere or the extended complex plane is simply connected.

5. The study of ramification (and hence of discriminants) is of basic importance in some advanced developments in Algebraic Number Theory, which go under the name of Class Field Theory. This is a fascinating topic, and to learn more about it, see [2] or [14]. It may also be worthwhile and interesting to see Hilbert's *Zahlbericht*, which was meant as a report to the German Mathematical Society on the status of Algebraic Number Theory in 1895. This report contained several original contributions by Hilbert and perhaps started the subject of Class Field Theory. The *Zahlbericht* is now available in English [9].

6. The relation with ramification is perhaps the most important application of discriminant in Number Theory. However, the classical discriminant $\Delta = b^2 - 4ac$ of a quadratic also comes up in the following important and classical question.

Given an integer Δ, what are the possible binary quadratic forms $ax^2 + bxy + cy^2$ with integer coefficients a, b, c, for which $\Delta = b^2 - 4ac$? Can we classify them?

This was studied by Legendre and Gauss, and the notions of class number and genera were developed by Gauss for classifying binary quadratic forms with a given discriminant. For an exposition of the basics of this theory, one may consult the texts of Baker [1] or Flath [4]. For a beautiful introduction to some modern developments motivated by this problem, we refer to Serre's Singapore lecture [20].

7. The discriminant also makes an unexpected appearance in questions related to the generalization of the so called Waring's problem. For example, it is shown in [12] that if K is a number field and n, k are integers with $n \geq k \geq 2$, then every $n \times n$ matrix over $\mathcal{O}_K$ is a sum of k-th powers of matrices over $\mathcal{O}_K$ if and only if the discriminant d_K of K is coprime to k. Moreover, when this condition is met, seven powers always suffice.

Acknowledgments

This article is an expanded version of a lecture delivered at S. P. College, Pune on February 19, 2000. This formed a sequel to a lecture by Prof. Balwant Singh on Resultants (cf. [21]). The author would like to thank the S. P. College for its invitation, and also thank Prof. S. A. Katre for a number of useful suggestions on a preliminary version of this article.

References

[1] A. Baker, A Concise Introduction to the Theory of Numbers, Cambridge University Press, 1984.

[2] J. W. S. Cassels and A. Fröhlich (eds.), Algebraic Number Theory, Academic Press, 1967.

[3] F. Catanese, Review of [5], *Bull. Amer. Math. Soc.*, Vol. 37 (2000), 183–198.

[4] D. E. Flath, Introduction to Number Theory, John Wiley & Sons, 1989.

[5] I. M. Gelfand, M. M. Kapranov and A. V. Zelevinsky, Discriminants, Resultants and Multidimensional Determinants, Birkhäuser, 1994.

[6] S. R. Ghorpade, Notes on Galois Theory, IIT Bombay, Oct. 1994.

[7] S. R. Ghorpade, Field Theory and Ramification Theory, Instructional School on Algebraic Number Theory, Bombay Univ., Dec. 1994.

[8] D. Hilbert, Gesammelte Abhandlungen, Band I: Zahlentheorie, 2nd Ed., Springer– Verlag, 1970.

[9] D. Hilbert, The Theory of Algebraic Number Fields, Springer-Verlag, 1998.

[10] K. Ireland and M. Rosen, A Classical Introduction to Modern Number Theory, Springer–Verlag, 1982.

[11] N. Jacobson, Basic Algebra I, 2nd Ed., W. H. Freeman, 1985.

[12] S. A. Katre and S. A. Khule, Matrices over orders in algebraic number fields as sums of k-th powers, *Proc. Amer. Math. Soc.*, Vol. 128, No. 3 (2000), 671–675.

[13] S. Lang, Algebra, 2nd ed., Addison-Wesley, 1984.

[14] S. Lang, Algebraic Number Theory, Springer–Verlag, 1986.

[15] W. S. Massey, A Basic Course in Algebraic Topology, Springer-Verlag, 1991.

[16] D. Rolfsen, Knots and Links, Publish or Perish Inc., 1990.

[17] P. Samuel, Theorie Algebrique des Nombres, Hermann, 1967. [An English translation was published by Houghton Miffin in 1970, while a corrected French edition was published by Hermann in 1971.]

[18] H. Seifert and W. Threlfall, A Textbook of Algebraic Topology, Academic Press, 1980.

[19] J.-P. Serre, Local Fields, Springer–Verlag, 1979.

[20] J.-P. Serre, $\Delta = b^2 - 4ac$, *Math. Medley*, Singapore Math. Society, Vol. 13 (1985), 1–13. (See also: Œuvres, Collected Papers, Vol. IV: 1985–1998, Springer–Verlag, 2000; or the appendix of [4].)

[21] B. Singh, Resultants, *Bona Mathematica*, Vol. 11, No. 1 (2000), 11–21.

[22] B. Sturmfels, Introduction to resultants, Proc. Symp. Appl. Math., Vol. 53, pp. 25–39, American Math. Society, 1998.

[23] B. L. van der Waerden, Algebra, Vol. 1, F. Ungar, 1949. [Reprinted by Springer-Verlag in 1991.]

[24] H. Weber, Lehrbuch der Algebra, Band I, Viehweg, 1895.

[25] L. C. Washington, Introduction to Cyclotomic Fields, Springer–Verlag, 1982. [Second Ed., Springer-Verlag, 1997.]

[26] O. Zariski and P. Samuel, Commutative Algebra, Vol. 1, D. Van Nostrand, 1958. [Reprinted by Springer–Verlag in 1975.]