Lectures on
Field Theory and Ramification Theory

Sudhir R. Ghorpade
Department of Mathematics
Indian Institute of Technology, Bombay
Powai, Mumbai 400 076, India
E-Mail: srg@math.iitb.ernet.in

Instructional School on Algebraic Number Theory
(Sponsored by the National Board for Higher Mathematics)
Department of Mathematics, University of Bombay
December 27, 1994 – January 14, 1995

Contents

Chapter 1

Field Extensions

1.1 Basic Facts

Let us begin with a quick review of the basic facts regarding field extensions and Galois groups. For more details, consult the notes [4] or any of the standard texts such as Lang [7] or Jacobson [6].

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 iff 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.

1. L/K is finite $\iff$ L/K is algebraic and finitely generated.

2. 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 $K(\alpha)$.

3. 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.

4. 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.

5. (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

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

such extension is separable and thus saying that it is Galois amounts to saying that it is finite and normal.

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.

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

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

3. 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 $L_{i+1} \cap (L_1 L_2 \ldots L_i) = K$. Then show that the Galois group of $L_1 L_2 \ldots L_r$ is isomorphic to $G_1 \times G_2 \times \ldots \times G_r$.

Exercise 1.3: Suppose L/K is Galois and $\mathrm{Gal}(L/K)$ can be written as a direct product $G_1 \times \ldots \times G_r$. Let L_i be the fixed field of the subgroup $G_1 \times \ldots G_{i-1} \times \{1\} \times G_{i+1} \times \ldots \times G_r$ of G. Show that L_i/K is Galois with $\mathrm{Gal}(L_i/K) \simeq G_i$, and $L_{i+1} \cap (L_1 L_2 \ldots L_i) = K$, and $L_1 L_2 \ldots L_r = L$.

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 $1, \zeta, \zeta^2, \ldots, \zeta^{n-1}$; 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 $j(\sigma\tau) = j(\sigma)j(\tau)(\mathrm{mod}\ n)$. Because 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.

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 let 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

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

[2]The structure of this group is well–known from Elementary Number Theory. To begin with, if $n = p_1^{e_1} \dots p_g^{e_g}$ is the factorization of n as a product of powers of distinct primes, then by Chinese Remainder Theorem, we have $(\mathbb{Z}/n\mathbb{Z})^\times \simeq (\mathbb{Z}/p_1^{e_1}\mathbb{Z})^\times \times \dots \times (\mathbb{Z}/p_g^{e_g}\mathbb{Z})^\times$. 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, [1] or [5] for details.

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

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

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

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

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 $\mathbb{F}_q$ 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

[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.

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*.

1.3 Cyclic Extensions

In this section, we shall see that if K is a reasonably big field, then cyclic extensions of K have a very neat structure. This will be done using a famous result of Hilbert, known as Hilbert Theorem 90, which characterizes elements in cyclic extensions of norm 1 or of trace 0. This result of Hilbert or more precisely, a cohomological version of it, is of prime importance in Class Field Theory.

To begin with, let us recall the notions of norm and trace. 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 $\Phi(X) = X^n + a_1X^{n-1} + \ldots + a_n$ 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.

1. $\mathrm{Tr}_{L/K}$ is a K–linear map of $L \to K$. For $a \in K$, $\mathrm{Tr}(a) = na$.
2. $N_{L/K}$ is a multiplicative map of $L \to K$ (i.e., $N(\alpha\beta) = N(\alpha)N(\beta)$ for $\alpha, \beta \in L$). For $a \in K$, $N(a) = a^n$.
3. 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
$$\mathrm{Tr}_{L/K}(\alpha) = \sum_{\sigma \in \mathrm{Gal}(L/K)} \sigma(\alpha) \qquad \text{and} \qquad N_{L/K}(\alpha) = \prod_{\sigma \in \mathrm{Gal}(L/K)} \sigma(\alpha).$$
4. 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 3 above 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
$$\mathrm{Tr}_{L/K}(\alpha) = \alpha^{(1)} + \alpha^{(2)} + \ldots + \alpha^{(n)} \qquad \text{and} \qquad N_{L/K}(\alpha) = \alpha^{(1)}\alpha^{(2)} \ldots \alpha^{(n)}.$$

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, the reader may consult [4], [12], or [14].

Remark: 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.

Now suppose L/K is a Galois extension. For any $\alpha \in K$ and any $\sigma \in \mathrm{Gal}(L/K)$, the elements α and $\sigma(\alpha)$ clearly have the same norm as well as the same trace. In other words, $N_{L/K}(\alpha/\sigma(\alpha)) = 1$ and $\mathrm{Tr}_{L/K}(\alpha - \sigma(\alpha)) = 0$. The result of Hilbert we talked about, which was ninetieth in the sequence of 169 theorems in his "Zahlbericht", says that the converse is true if L/K happens to be a cyclic extension. More precisely, we have the following.

Hilbert Theorem 90. *Let L/K be a cyclic extension of degree n and σ be a generator of $\mathrm{Gal}(L/K)$. Then for any $\beta \in L$, we have:*

(i) $N(\beta) = 1$ *iff* $\beta = \alpha/\sigma(\alpha)$ *for some* $\alpha \in L$.

(ii) $\mathrm{Tr}(\beta) = 0$ *iff* $\beta = \alpha - \sigma(\alpha)$ *for some* $\alpha \in L$.

To prove this result, we will use the following lemma due to Artin, which is a sleek reformulation of a classical result of Dedekind.

Lemma. *Let $\sigma_1, \ldots, \sigma_n$ be distinct homomorphisms of a group G into the multiplicative group k^* of a field k. Then they are linearly independent over k.*

Proof: Induct on n. The case of $n = 1$ is obvious. Suppose $n > 1$ and $a_1\sigma_1 + \ldots + a_n\sigma_n = 0$ for some $a_1, \ldots, a_n \in k$. We may assume that $a_i \neq 0$ for all i because otherwise the induction hypothesis applies. Now since $\sigma_1 \neq \sigma_2$, there is some $\alpha \in G$ such that $\sigma_1(\alpha) \neq \sigma_2(\alpha)$. From the above equation, we see that for any $x \in G$, we have $a_1\sigma_1(x) + \ldots + a_n\sigma_n(x) = 0$. Multiplying throughout by $\sigma_1(\alpha)$ we get $a_1\sigma_1(\alpha)\sigma_1(x) + \ldots + a_n\sigma_1(\alpha)\sigma_n(x) = 0$ while replacing x by αx and using the fact that σ_i are homomorphisms, we get $a_1\sigma_1(\alpha)\sigma_1(x) + \ldots + a_n\sigma_n(\alpha)\sigma_n(x) = 0$. Subtracting the first equation from the last, we find that $b_2\sigma_2(x) + \ldots + b_n\sigma_n(x) = 0$, where $b_i = a_i(\sigma_i(\alpha) - \sigma_1(\alpha))$ and $b_2 \neq 0$. But this contradicts the induction hypothesis. □

Remark: In the above result, G could have been any monoid which isn't necessarily a group. Homomorphisms of $G \to k^*$ are usually called the *characters* of G in k.

Proof of Hilbert Theorem 90. The "if" part is easy and its proof has already been indicated. Suppose $\beta \in L$ is such that $N(\beta) = 1$. Let us put

$$a_0 = 1,\ a_1 = \beta,\ a_2 = \beta\sigma(\beta),\ \ldots,\ a_{n-1} = \beta\sigma(\beta)\ldots\sigma^{n-2}(\beta).$$

Then these are nonzero elements of L such that $\beta\sigma(a_i) = a_{i+1}$ for $0 \leq i < n-1$ and $\beta\sigma(a_{n-1}) = N(\beta) = 1 = a_0$. Consider the homomorphisms $\mathrm{id}, \sigma, \sigma^2, \ldots, \sigma^{n-1}$. These are clearly distinct maps of $L^* \to L^*$. Therefore, by the lemma above, there exists some $x \in L^*$ such that $a_0x + a_1\sigma(x) +$

$a_2\sigma^2(x) + \ldots + a_{n-1}\sigma^{n-1}(x) \neq 0$. If we let α denote this nonzero element, then we readily see that $\beta\sigma(\alpha) = \alpha$. Thus $\beta = \alpha/\sigma(\alpha)$.

To prove the additive version of Hilbert Theorem 90, let us again consider only the nontrivial part. Thus let $\beta \in L$ be such that $\mathrm{Tr}(\beta) = 0$. This time, let us put

$$b_0 = 0,\ b_1 = \beta,\ b_2 = \beta + \sigma(\beta),\ \ldots,\ b_{n-1} = \beta + \sigma(\beta) + \ldots + \sigma^{n-2}(\beta).$$

Then we have $\beta + \sigma(b_i) = b_{i+1}$ for $0 \leq i < n-1$ and $\beta + \sigma(b_{n-1}) = \mathrm{Tr}(\beta) = 0 = b_0$. Using the Lemma above, we can find some $x \in L^*$ such that $\mathrm{Tr}(x) = x + \sigma(x) + \ldots + \sigma^{n-1}(x) \neq 0$. Now if we take $\alpha = \frac{1}{\mathrm{Tr}(x)}\left[b_1\sigma(x) + b_2\sigma^2(x) + \ldots + b_{n-1}\sigma^{n-1}(x)\right]$, then we see that $\beta + \sigma(\alpha) = \alpha$. This completes the proof. □

Exercise 1.7: Let d be a squarefree positive integer. Show that a pair (x, y) of integers is a solution of the Pell's equation $X^2 - dY^2 = 1$ iff $x + y\sqrt{d} = \frac{a+b\sqrt{d}}{a-b\sqrt{d}}$ for some integers a and b.

Now let K be a field and n be a positive integer. Assume that the characteristic of K is either zero or relatively prime to n. Also assume that K contains all the n^{th} root of unity. Thus $\mu_n = \mu_n(K)$ is a cyclic group of order n.

Consider the polynomial $X^n - a$ in $K[X]$, where a is some nonzero element of K. Suppose α is a root of this polynomial, then all other roots are of the form $\omega\alpha$, where $\omega \in \mu_n$. Thus $K(\alpha)$ contains all the roots of $X^n - a$. Moreover, these roots are distinct since 0 is the only root of the derivative nX^{n-1} of $X^n - a$. Therefore $K(\alpha)/K$ is a Galois extension. Let G denote the Galois group of $K(\alpha)/K$. Any $\sigma \in G$ must map α to $\omega\alpha$ for a uniquely determined $\omega = \omega_\sigma \in \mu_n$. The map $\sigma \to \omega_\sigma = \sigma(\alpha)/\alpha$ is clearly seen to be an injective homomorphism of $G \to \mu_n$. Therefore G is a cyclic group of order d, where d is a divisor of n. If σ is a generator of G, then $\sigma(\alpha) = \omega\alpha$, where $\omega \in \mu_n$ must be a primitive d^{th} root of unity in K. Consequently, $\sigma(\alpha^d) = (\omega\alpha)^d = \alpha^d$, and thus $\alpha^d \in K$. It follows that the minimal polynomial of α over K is $X^d - \alpha^d$. In particular, if $X^n - a$ is irreducible, then its Galois group is the cyclic group of order n.

To summarise the above discussion, we may say that if $X^n - 1$ can be solved in K, then any equation of the form $X^n - a$, has a cyclic Galois group. We show below that the converse is also true.

Theorem. *Let K be as above and let L/K be a cyclic extension of degree n. Then there exists $\alpha \in K$ such that $L = K(\alpha)$ and $\mathrm{Irr}(\alpha, K) = X^n - a$ for some $a \in K$.*

Proof: Let ζ be a primitive n^{th} root of unity in K. Then $N(\zeta^{-1}) = (\zeta^{-1})^n = 1$. Hence by Hilbert Theorem 90, there exists $\alpha \in L$ such that $\zeta^{-1} = \alpha/\sigma(\alpha)$, or equivalently, $\zeta = \sigma(\alpha)/\alpha$, where σ denotes a generator of $\mathrm{Gal}(L/K)$. It follows that $\sigma^i(\alpha) = \zeta^i\alpha$, and thus $\zeta^i\alpha$ are conjugates of α for $0 \leq i \leq n-1$, which are clearly distinct. Therefore, $[K(\alpha) : K] \geq n = [L : K] \geq [K(\alpha) : K]$. It follows that $L = K(\alpha)$, and $\mathrm{Irr}(\alpha, K) = \prod_{i=0}^{n-1}(X - \zeta^i\alpha) = (X^n - \alpha^n)$. This proves the theorem. □

Remark: In case $n = p = \mathrm{char}\, K$, we have an analogous result with X^p replaced by $X^p - X$. Thus the Galois group of $X^p - X - a$ is cyclic and this is the prototype of a cyclic extension of degree p. This result is known as Artin–Schreier Theorem. Its proof uses the the additive version of Hilbert Theorem 90. For cyclic extensions of degree p^m over a field of characteristic p, one has similar but more complicated result using the notion of Witt vectors. See [7] for details.

1.4 Abelian Extensions

Let us suppose n is a positive integer and K is a field whose characteristic is zero or relatively prime to n. Assume that it contains all the n^{th} roots of unity. We have seen that an equation of the form $X^n - a$ has cyclic Galois group. Now suppose we consider several such equations, say $X^n - a_1$, $X^n - a_2$, ..., $X^n - a_r$, and ask for the Galois group of their product. That means, given $a_1, a_2, \ldots, a_r \in K$, we can consider the field L obtained by adjoining to K the n^{th} roots of $a_1, a_2, \ldots, a_r$; it is clearly a Galois extension of K (is it clear to you?), and we ask how does the Galois group $\mathrm{Gal}(L/K)$ look like? Let us note that L not only contains the n^{th} roots of $a_1, \ldots, a_r$ but also of any powers of them or of finite products of such powers and of course of the n^{th} power of each element of K. Indeed L consists of the n^{th} roots of any element of the subgroup, say Δ, of the multiplicative group K^* which is generated by K^{*n} and the elements $a_1, \ldots, a_r$. Thus we may write $L = K(\Delta^{1/n})$. To come back to the question about the Galois group of L/K, we see right away from the example of biquadratic extensions (Exercise 1.1) that it can't be a cyclic group. But it seems natural to expect it to be a direct product of cyclic groups. This is indeed the case. And to see that is quite easy. As in the previous section, we have a natural homomorphism of the Galois group into the r–fold direct product $\mu_n \times \mu_n \times \ldots \times \mu_n$, which is injective. Thus at any rate, the said Galois group is abelian. Now we know that any finite abelian group is the direct product of cyclic groups. So it seems reasonable that any finite abelian group is the Galois group of equations of the type above. This we shall now prove.

A Galois extension L/K is said to be of *exponent* n if $\sigma^n = 1$, for all $\sigma \in \mathrm{Gal}(L/K)$. By a *Kummer extension* of K we mean a field extension L of K of the form $L = K(\Delta^{1/n})$, where Δ is a subgroup of K^* containing the group K^{*n} of n^{th} powers such that Δ/K^{*n} is finitely generated (or equivalently, finite!). As outlined above, a Kummer extension is an abelian extension of exponent n. Conversely, we have the following.

Theorem. *If L/K is an abelian extension of exponent n, then $L = K(\Delta^{1/n})$, where $\Delta = L^{*n} \cap K^*$.*

Proof: Let $\Delta = L^{*n} \cap K^*$. Clearly, $K(\Delta^{1/n}) \subseteq L$. Let $G = \mathrm{Gal}(L/K)$. Since G is a finite abelian group, we can write $G = G_1 \times G_2 \times \ldots \times G_r$, where $G_1, \ldots, G_r$ are cyclic groups. Moreover, since $\sigma^n = 1$ for all $\sigma \in G$, the order of G_i must divide n, for each i. Let L_i be the fixed field of $G_1 \times \ldots \times G_{i-1} \times \{1\} \times G_{i+1} \times \ldots \times G_r$. Then from Exercise 1.3, we know that L_i/K is Galois with Galois group G_i. Now using the result about cyclic extensions proved in the last section, we see that $L_i = K(\alpha_i)$, where α_i is a nonzero element of L_i such that $\alpha_i^n \in K$. Clearly $L_i \subseteq K(\Delta^{1/n})$. Since L is the compositum of $L_1, \ldots, L_r$, it follows that $L \subseteq K(\Delta^{1/n})$. □

Thus we see that abelian extensions of K of exponent n are precisely the Kummer extensions obtained by adjoining n^{th} roots of elements of a subgroup Δ of K^* such that $K^{*n} \subseteq \Delta$ and Δ/K^{*n} is finite. As we shall see in a moment, this correspondence between subgroups Δ of the type above and Kummer extensions $K(\Delta^{1/n})/K$ of exponent n is actually one-to-one and inclusion preserving. Moreover, the degree of the Kummer extension $K(\Delta^{1/n})/K$ is precisely the index of K^{*n} in Δ. To state this in a "natural" fashion we need the notion of dual group, which is briefly reviewed below.

Let G be an abelian group of exponent n. By a *dual group* of G we mean the group $G^* = \mathrm{Hom}(G, C_n)$ of all group homomorphisms of G into a cyclic group C_n of order n. In these notes,

G will usually be the Galois group of an abelian extension of K of exponent n and we take C_n to be the group $\mu_n = \mu_n(K)$ of n^{th} roots of unity in K. The construction of dual groups preserves direct products and has the property that if G is a finite abelian group, then G^* is isomorphic to G [this is usually proved by reducing to the case of cyclic groups via the Structure Theorem for finite abelian groups; try!]. For more on dual groups, see Chapter 1, §11 of [7].

Theorem. *With K and n as above and μ_n denoting the group of n^{th} roots of unity in K, we have the following.*

(i) Given any subgroup Δ of K^* such that $K^{*n} \subseteq \Delta$ and Δ/K^{*n} is finite, we have a canonical isomorphism of the dual group $G^* = \text{Hom}(G, \mu_n)$ of $G = \text{Gal}(K(\Delta^{1/n})/K)$ with the factor group Δ/K^{*n}. It is given by $a \mapsto \chi_a$, where for $a \in \Delta$, $\chi_a(\sigma) = \sigma(\alpha)/\alpha$, where α is an element of $K(\Delta^{1/n})$ such that $\alpha^n = a$. In particular, we have $[K(\Delta^{1/n}) : K] = |\Delta/K^{*n}|$.

(ii) The map $\Delta \mapsto K(\Delta^{1/n})$ sets up an inclusion preserving bijection from the set of subgroups Δ of K^* such that $K^{*n} \subseteq \Delta$ and Δ/K^{*n} is finite onto the set of Kummer extensions $K(\Delta^{1/n})/K$ of exponent n.

Proof: Let Δ be as in (i), $L = K(\Delta^{1/n})$ and $G = \text{Gal}(L/K)$. In view of the previous result, we see that $\Delta = L^{*n} \cap K^*$. To prove (i), first let us note that the map $a \mapsto \chi_a$ is well-defined. Fix $a \in \Delta$ and $\sigma \in G$. Now if α is such that $\alpha^n = a$, then we must have $\sigma(\alpha) = \zeta\alpha$ for some $\zeta \in \mu_n$ and thus $\sigma(\alpha)/\alpha$ is in μ_n; moreover, $\zeta = \sigma(\alpha)/\alpha$ is independent of the choice of α. Also if $a \equiv b (\text{mod } K^{*n})$, then we clearly have $\chi_a(\sigma) = \chi_b(\sigma)$. Thus this map is defined on the factor group Δ/K^{*n}. Next, with α as above, we have

$$\chi_a = 1 \iff \sigma(\alpha) = \alpha \text{ for all } \sigma \in G \iff \alpha \in K^* \iff a \in K^{*n}.$$

This shows that the map $a \mapsto \chi_a$ of $\Delta/K^{*n} \to G^*$ is injective. To prove its surjectivity, let χ be any element of G^*. As before, we can write $G = G_1 G_2 \dots G_r \simeq G_1 \times \dots \times G_r$, where $G_1, \dots, G_r$ are cyclic subgroups of G and the order of each of them divides n. If L_i is the fixed field of $G_1 \dots G_{i-1} G_{i+1} \dots G_r$, then we know that L_i/K is a cyclic extension with Galois group G_i. Let σ_i be the generator of G_i. If the order of G_i is d_i, then, $\chi(\sigma_i)$ is a primitive $d_i{}^{\text{th}}$ root of unity in K, and so its norm (w.r.t. L_i/K) is 1. Therefore, by Hilbert Theorem 90, there exists $\alpha_i \in L_i$ such that $\chi(\sigma_i) = \sigma_i(\alpha_i)/\alpha_i$. It is clear that $\alpha_i^n \in K^*$. Let $\alpha = \alpha_1 \alpha_2 \dots \alpha_r$ and $a = \alpha^n$. Then $\alpha \in L$ and $a \in K^* \cap L^{*n} = \Delta$. We claim that $\chi = \chi_a$. To see this, let σ be any element of G. Then we can uniquely write $\sigma = \sigma_1^{j_1} \sigma_2^{j_2} \dots \sigma_r^{j_r}$ for some nonnegative integers $j_1, j_2, \dots, j_r$. We clearly have

$$\chi(\sigma) = \chi(\sigma_1^{j_1})\chi(\sigma_2^{j_2}) \dots \chi(\sigma_r^{j_r}) = \frac{\sigma_1^{j_1}(\alpha_1)}{\alpha_1} \cdot \frac{\sigma_2^{j_2}(\alpha_2)}{\alpha_2} \cdots \frac{\sigma_r^{j_r}(\alpha_r)}{\alpha_r} = \frac{\sigma(\alpha)}{\alpha}$$

where the last equality uses the fact that L_i is the fixed field of $G_1 \dots G_{i-1} G_{i+1} \dots G_r$. Thus we have proved the surjectivity and the isomorphism between G^* and Δ/K^{*n} is established.

To prove (ii), let us first note that by previous theorem, the map $\Delta \mapsto K(\Delta^{1/n})$ is surjective. The remaining assertions will follow if we show that for any subgroups Δ_1 and Δ_2 of K^* containing K^{*n} and such that the index of K^{*n} in Δ_i is finite, we have:

$$\Delta_1 \subseteq \Delta_2 \iff K(\Delta_1^{1/n}) \subseteq K(\Delta_2^{1/n}).$$

The implication "⇒" is of course obvious. Suppose we have $K(\Delta_1^{1/n}) \subseteq K(\Delta_2^{1/n})$. Let $b \in \Delta_1$. Consider the group Δ_3 generated by Δ_2 and b. Since $K(b^{1/n}) \subseteq K(\Delta_2^{1/n})$, it follows that $K(\Delta_2^{1/n}) = K(\Delta_3^{1/n})$. By (i) above, $|\Delta_2/K^{*n}| = |\Delta_3/K^{*n}|$. Also since $\Delta_2 \subseteq \Delta_3$, this implies that $\Delta_2 = \Delta_3$. Thus $b \in \Delta_2$. So we have proved that $\Delta_1 \subseteq \Delta_2$. This completes the proof. □

Remark: The results in this section are collectively referred to as Kummer Theory (of abelian extensions). Analogues of the above result also hold in the case of infinite extensions where we drop the assumption that Δ/K^{*n} is finite. For the case of infinite extensions, see [9]. In case of abelian extensions of exponent p of a field of characteristic p, we have results similar to Artin–Schreier Theorem. As before, see [7] for this.

1.5 Discriminant

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.] Let us note that, as remarked earlier, 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. *If $\alpha_1, \ldots, \alpha_n \in L$ are such that $D_{L/K}(\alpha_1, \ldots, \alpha_n) \neq 0$, 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. *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

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

and so the result follows. □

Remarks: 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. *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

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

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

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 [14].

Remark: Classically, the discriminant of a polynomial, say $g(X) = a_0X^m + a_1X^{m-1} + \ldots + a_m$, is defined to be the "resultant" $\mathrm{Res}(g(X), g'(X))$ of the polynomial and its derivative. In turn, the *resultant* $\mathrm{Res}(\phi, \psi)$ of two polynomials, say $\phi(X) = b_0X^r + b_1X^{r-1} + \ldots + b_r$ and $\psi(X) = c_0X^s + c_1X^{s-1} + \ldots + c_s$ is defined to be the determinant of the $(r+s) \times (r+s)$ matrix whose (i,j)–th entry, for $1 \leq j \leq r+s$, is b_{j-i} if $1 \leq i \leq r$ and is c_{j+r-i} if $r+1 \leq i \leq r+s$. Here, we have used the convention that $b_i = 0$ if either $i < 0$ or $i > r$ and $c_j = 0$ if either $j < 0$ or $j > s$. The resultant of two polynomials in one variable X is actually the result of elimination of X between them. One shows that if $\phi(X) = b_0 \prod_{i=1}^{r}(X - \alpha_i)$ and $\psi(X) = c_0 \prod_{j=1}^{s}(X - \beta_j)$, then

$$\mathrm{Res}(\phi, \psi) = b_0^s \prod_i \psi(\alpha_i) = (-1)^{rs} c_0^r \prod_j \phi(\beta_j) = b_0^s c_0^r \prod_i \prod_j (\alpha_i - \beta_j).$$

It follows that $\mathrm{Res}(\phi, \psi) = 0$ iff either $b_0 = 0 = c_0$ or ϕ and ψ have a common root. In particular, for a polynomial $g(X)$ as above, assuming $a_0 \neq 0$, we have that $g(X)$ has a multiple root iff its (classical) discriminant $\mathrm{Disc}_X g(X)$ is zero. Now the above formulae readily imply that in the situation of the previous Theorem, we have $\mathrm{Disc}_X f(X) = (-1)^{n(n-1)/2} D_{K(\alpha)/K}(1, \alpha, \ldots, \alpha^{n-1})$, and thus we see that the classical and the modern notions of discriminant are essentially the same. For more on resultant et al, see [12].

Now let us review a few basic facts concerning integral extensions in order to prove an important consequence of the above Corollary.

Let B be a ring[4] and A be a subring of B. An element $x \in B$ is said to be *integral* over A if it satisfies a monic polynomial with coefficients 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. It can be shown that the elements of B which are integral over A form a subring, say C, of B. If $C = A$, 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. Basic example of an integrally closed ring is $\mathbb{Z}$, the ring of integers. (Verify!) If K is a number field, then the elements of K which are integral over $\mathbb{Z}$ form an integrally closed ring, which is denoted by $\mathcal{O}_K$ and called the *ring of integers of K*.

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

(i) If an element α (in some extension 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.

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

(ii) If A is integrally closed, 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 integrally closed, 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 $X^n + a_1X^{n-1} + \ldots + a_n \in K[X]$, 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 elements of 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 §1.2 follows from (ii) above. We are now ready to prove the following important result.

Finiteness Theorem: *Let A be an integrally closed 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. □

We will derive a useful consequence of this when A is a PID using the following lemma.

Lemma: *Let A be a PID and M be a finite A–module generated by n elements. Then every submodule N of M is generated by n elements.*

Proof: We prove by induction on n. If $n = 1$, then $M = Ax$, and letting α to be a generator of the ideal $\{a \in A : ax \in N\}$ of A, and $y = \alpha x$, we see that $N = Ay$. Assume that $n > 1$ and that the assertion holds for smaller values of n. Suppose $M = Ax_1 + \ldots + Ax_n$. We let $M_1 = Ax_2 + \ldots Ax_n$ and note that, by induction hypothesis, we can find $y_2, \ldots, y_n \in N$ such that $N \cap M_1 = Ay_2 + \ldots + Ay_n$. We have

$$N/(N \cap M_1) \simeq (N + M_1)/M_1 \subseteq M/M_1.$$

Now M/M_1 is clearly isomorphic to a submodule of Ax_1, and hence so is $M/(N \cap M_1)$. By the case $n = 1$, it follows that there exists $y_1 \in N$ such that $\bar{y}_1 = y_1 + (N \cap M_1)$ generates $N/(N \cap M_1)$ as an A–module. Consequently, $N = Ay_1 + Ay_2 + \ldots + Ay_n$, as desired. □

Corollary: *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 $B = Ay_1 + \ldots + Ay_n$.* □

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 number field. If $\{\alpha_1, \ldots, \alpha_n\}$ is an integral basis of a number field K, then by (iii) in the Proposition above, we see that $D_{L/K}(\alpha_1, \ldots, \alpha_n)$ is an integer. Further, if $\{u_1, \ldots, u_n\}$ is any $\mathbb{Q}$–basis of K which is contained in $\mathcal{O}_K$, 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, then clearly $d = \pm 1$. It follows that any two integral bases have the same discriminant, and among all bases of K contained in $\mathcal{O}_K$, the discriminant of an integral basis has the least absolute value.

Remark: The last observation can be used to give an alternate proof of the existence of an integral basis. Namely, 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 [5] for a proof along these lines.

The previous discussion shows that the discriminant of an integral basis of a number field K depends only on the field K. It is called the *(absolute) discriminant of* K and is denoted by d_K. In general, if A is an integrally closed domain with quotient field K, L/K is finite separable of degree n, and B is the integral closure of A in L, then instead of a single number such as d_K, one has to consider the ideal of A generated by the elements $D_{L/K}(\alpha_1, \ldots, \alpha_n)$ as $\{\alpha_1, \ldots, \alpha_n\}$ vary over all K–bases of L which are contained in B; this ideal is called the *discriminant ideal* of B/A or of L/K, and is denoted $\mathcal{D}_{B/A}$. In case A happens to be a PID (which is often the case in number theoretic applications), we can replace this ideal by a generator of it, which then plays a role analogous to d_K. Let us also note that we can consider the discriminant ideal for the extension C/k where k is a PID (in particular, k may be a field) and C is a ring which contains k as a subring and C is of free module of finite rank n over k. In this case $\mathcal{D}_{C/k}$ is defined to be the ideal of k generated by the elements $D_{C/k}(u_1, \ldots, u_r)$ as $\{u_1, \ldots, u_r\}$ vary over all k–bases of C. It may be noted that these two definitions of discriminant ideal are consistent.

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 $a_1^2 - mb_1^2 \equiv 0 (\text{mod } 4)$. Also a_1 is odd, and therefore, $m \equiv 1 (\text{mod } 4)$. It follows that if $m \not\equiv 1 (\text{mod } 4)$, 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 $m \equiv 1 (\text{mod } 4)$, the preceding observations imply that

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

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.

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

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!)

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

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

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 $\Phi_p(X) = X^{p-1} + X^{p-2} + \ldots + X + 1$ is the minimal polynomial of ζ 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

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

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

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

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 $x = c_0 + c_1\zeta + \ldots + c_{p-1}\zeta^{p-1}$ for some $c_i \in \mathbb{Q}$. We shall now show that c_i are, in fact, in $\mathbb{Z}$. To this effect, consider $(\zeta - 1)x = c_0(\zeta - 1) + c_1(\zeta^2 - \zeta) + \ldots + c_{p-1}(\zeta^p - \zeta^{p-1})$. 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 $c_1 + c_2\zeta + \ldots + c_{p-1}\zeta^{p-2}$. 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 1.8: 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: 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 [13].

Exercise 1.9: If K is either a quadratic field or a cyclotomic field, then show that $d_K \equiv 0$ or $1 (\mathrm{mod}\ 4)$.

Chapter 2

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. 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, whose results were first published in 1871. [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*). Following the ideas of Emmy Noether, it can be proved that a domain A is a Dedekind domain if and only if it satisfies any of the following equivalent conditions.

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

(2) Every nonzero ideal of A can be factored as a product of prime ideals.

(3) Fractionary ideals of A (i.e., finitely generated A–modules contained in the quotient field of A), excluding the zero ideal, form a group under multiplication.

Now in the ring of integers of a number field, a prime p of $\mathbb{Z}$ may not remain a prime. For instance in the ring of integers of $\mathbb{Q}(\sqrt{-1})$, 2 and 5 are no longer primes but 3 is. However, by the above result of Kummer–Dedekind, the ideal generated by p in this ring can be uniquely factored as a product of prime ideals. This phenomenon may be loosely described as ramification. In this chapter, we shall study some fundamental results concerning this phenomenon.

[1] 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.

2.1 Extensions of Primes

Formally, our stating point is the following result.

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.*

It may be noted that this theorem follows quickly using the Finiteness Theorem proved in §1.5 and some elementary properties of integral extensions (cf. [14]). Also note that, since $\mathbb{Z}$ is obviously a Dedekind domain, this result proves that the ring of integers of a number field is a Dedekind domain.

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

Definition. Let $\wp$ be a prime ideal of A. A prime ideal P of B is said to *lie over* $\wp$ if $P \cap A = \wp$.

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

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

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

Exercise 2.1: With $\wp$ and P_i as above, show that a prime ideal P of B lies over $\wp$ iff $P = P_i$ for some i. Also show that $\wp B \cap A = \wp = P_i^{e_i} \cap A$. Deduce that $B/\wp B$ as well as $B/P_i^{e_i}B$ can be regarded as vector spaces over the field $A/\wp$. Further show that B/P_i is a field extension of $A/\wp$ whose degree is at most n.

Definition. With $\wp$, P_i, etc. as above, the positive integer e_i is called the *ramification index* of P_i over $\wp$ and is denoted by $e(P_i/\wp)$; the field degree $[B/P_i : A/\wp]$ is called the *residue degree* (or the *residue class degree*) of P_i over $\wp$ and is denoted by $f(P_i/\wp)$. If $e_i > 1$ for some i, then we say that $\wp$ is ramified in B (or in L). Otherwise, it is said to be *unramified*. [2] The extension L/K is said to be *unramified* if every nonzero prime ideal of A is unramified in L.

Exercise 2.2: Let A, K, L, B and $\wp$ 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 $\wp$ and P' a prime of B' lying over P, then show that P' lies over $\wp$ and the following transitivity relations hold:

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

Before proving the main result of this section, let us recall some preliminary results about Dedekind domains which we shall use in the sequel. If some of these seem unfamiliar, then they are likely to be trivial, and the reader is encouraged to prove them as exercises.

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

1. If S is any multiplicatively closed subset of the Dedekind domain A such that $0 \notin S$, then the localisation $S^{-1}A$ of A at S is a Dedekind domain. Moreover, the integral closure of $S^{-1}A$ in L is $S^{-1}B$.

2. A Dedekind domain having only finitely many prime ideals is a PID.

3. A local Dedekind domain is a PID having a unique nonzero prime ideal.

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

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

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 $f_i = [B/P_i : A/\wp]$, we have

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

Proof: Let $S = A \setminus \wp$ and $A' = S^{-1}A$ be the localisation of A at $\wp$. Then $B' = S^{-1}B$ is the integral closure of A' in L, and $\wp B' = P_1'^{e_1} \ldots P_g'^{e_g}$, where $P_i' = P_i B'$. Moreover, the primes $P_1', \ldots, P_g'$ are distinct, $A'/\wp A' \simeq A/\wp$ 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 $A, B, \wp, P_i$ by $A', B', \wp', P_i'$ respectively.

In view of the observations above, we shall assume without loss of generality that A is a local Dedekind domain with $\wp$ as its unique nonzero prime ideal. Then, by the Corollary to the Finiteness Theorem (cf. §1.5), B is a free A–module of rank $n = [L : K]$. Write $B = Ay_1 + \ldots + Ay_n$, where $y_1, \ldots, y_n$ are some elements of B. Now for the vector space $B/\wp B$ over $A/\wp$, we clearly have

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

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

$$\sum \bar{a}_i \bar{y}_i = 0 \Rightarrow \sum a_i y_i \in \wp B \Rightarrow a_i \in \wp$$

where $a_i \in A$ and $\bar{a}_i$ denotes its residue class mod $\wp$, 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 $A/\wp$, and hence

$$\dim_{A/\wp} B/\wp B = n.$$

Now we count the same dimension by a different method. To this effect, note that $\wp B = P_1^{e_1} P_2^{e_2} \ldots P_g^{e_g}$ and, since $P_1, P_2, \ldots, P_g$ are distinct maximal ideals, $P_i^{e_i}$ and $P_j^{e_j}$ are comaximal[3] for all $i \neq j$.

[3]Two ideals I and J in a ring R are said to be *comaximal* if $I + J = R$.

Hence, by Chinese Remainder Theorem[4], we get an isomorphism (of rings as well as of $(A/\wp)$–vector spaces)

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

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

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

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 $A/\wp$–homomorphism, and it is clearly bijective. So

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

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

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

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

[4]Recall that (a version of) the Chinese Remainder Theorem states that if $I_1, \ldots, I_n$ are pairwise comaximal ideals in a ring R (i.e., $I_i + I_j = R$ for all $i \neq j$), then 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 $R/I_1 I_2 \ldots I_n$ onto the direct sum $R/I_1 \oplus R/I_2 \oplus \ldots \oplus R/I_n$. Equivalently, for any $x_1, \ldots, x_n \in R$, there exists $x \in R$ such that $x \equiv x_j (\mathrm{mod}\ I_j)$ for $1 \leq j \leq n$.

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. During the discussion in §1.5 of the example of 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 $(\zeta^i - 1)/(\zeta - 1) = 1 + \zeta + \ldots + \zeta^{i-1} \in \mathbb{Z}[\zeta]$ and its inverse $(\zeta-1)/(\zeta^i-1) = (\zeta^i j - 1)/(\zeta^i - 1)$ 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. A nonzero prime ideal $\wp$ of A is said to be *totally ramified* in L (or in B) if $\wp B = P^n$ for some prime ideal P of B.

2.2 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 $\wp$ in A, we let $\bar{A}$, denote the residue field $A/\wp$; for any polynomial $p(X) \in A[X]$, by $\bar{p}(X)$ we denote its reduction mod $\wp$, i.e., the polynomial in $\bar{A}[X]$ whose coefficients are the $\wp$–residues of the corresponding coefficients of $p(X)$.

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. Let $\wp$ 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 $\wp$ is $\bar{p}_i(X)$. Then the primes in B lying over $\wp$ are precisely given by $P_1, \dots, P_g$ where $P_i = \wp B + p_i(\alpha)B$. Moreover,

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

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

Proof: Fix some i with $1 \leq i \leq g$. 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 $\wp$, 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 $\wp A[X] + p_i(X)A[X]$. 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 $\wp B + p_i(\alpha)B$. Since $\bar{p}_i(X)$ is irreducible in $\bar{A}[X]$, $\ker \varphi_i$ is a prime ideal in B which contains $\wp$. It is therefore a maximal ideal in B lying over $\wp$. Also $\bar{A}$ is a field and

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

Now suppose P is any maximal ideal of B lying over $\wp$. Since

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

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

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

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

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

Since $P_i = \wp B + p_i(\alpha)B$, we have

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

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

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

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. □

2.3 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[5]. Let $\bar{f}(X) \in \mathbb{Z}/p\mathbb{Z}[X]$ denote the

[5]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.

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 in view of the Remark preceding Hilbert Theorem 90 in §1.3, 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. *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 $\wp$ be a nonzero prime ideal of A. Assume that the field $A/\wp$ is perfect (which means that every algebraic extension of this field is separable)*[6]*. Then we have:*

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

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 localisations $A' = S^{-1}A$ and $B' = S^{-1}B$ where $S = A \setminus \wp$, then it is readily seen that $\mathcal{D}_{B'/A'} = \mathcal{D}_{B/A}A'$ and $\wp$ ramifies in L iff $\wp' = \wp A'$ 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 $\wp$ is its unique maximal ideal.

Let $\wp B = P_1^{e_1} P_2^{e_2} \cdots P_g^{e_g}$, 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 the Theorem in §2.1, we have $\wp B \cap A = \wp = P_i^{e_i} \cap A$, and we have an isomorphism of $A/\wp$–vector spaces

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

Let us set $\bar{A} = A/\wp$ and $\bar{B} = B/\wp B$. 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

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

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

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

[6]This assumption would always be satisfied in number theoretic applications since $A/\wp$ would usually be a finite field.

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 $\wp$ 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 $D_{L/K}(\alpha_1, \ldots, \alpha_n) \in \wp B$. It follows that $\mathcal{D}_{B/A} \subseteq \wp B \cap A = \wp$.

To prove the converse, assume that $\wp \supseteq \mathcal{D}_{B/A}$. Suppose, if possible, $\wp$ 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 $\mathcal{D}_{B/A} \subseteq \wp$. It follows that $\wp$ must be a ramified prime.

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

Corollary. *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.* □

Remark: A related result in connection with the above Corollary is that if K is any number field other than $\mathbb{Q}$, then $|d_K| > 1$. Consequently, there exists at least one rational prime which ramifies in K. The proof of this result, due to Minkowski, is rather involved. See [8] for details.

2.4 Ramification in Galois Extensions

In the case of Galois extensions, the fundamental identity $\sum e_i f_i = n$, which was proved in §2.1, 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. *Let A be an integrally closed domain, K its quotient field, L a Galois extension of K, B the integral closure of A, and $\wp$ a prime ideal of A. Then the primes of B lying over $\wp$ are conjugates of each other, i.e., for any prime ideals P, Q of B such that $P \cap A = \wp = Q \cap A$, we have $Q = \sigma(P)$ for some $\sigma \in \mathrm{Gal}(L/K)$. In particular, the number of prime ideals of B lying over $\wp$ is finite, and , in fact, $\leq [L : K]$.*

Proof: We use a similar reduction as in the proof of the Theorem in §2.1. Thus we note that if $S = A \setminus \wp$, 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 $\wp A'$. 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 $\wp$ 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 the Proposition in §1.5, this lies in A and hence in $Q \cap A = \wp$. Now P is a prime ideal of B containing $\wp$, 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: *Let A be an integrally closed domain, K its quotient field, L a finite separable extension of K, B the integral closure of A in L, and $\wp$ a prime ideal in A. Then there exists only a finite number of prime ideals in B lying over $\wp$.*

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 $\wp$. 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 $\wp$. Hence, by the above Lemma, we get the desired result. □

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

$$\wp B = (P_1 P_2 \dots P_g)^e$$

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

$$efg = n.$$

Proof: Let $\wp B = P_1^{e_1} \dots P_g^{e_g}$, where $P_1, \dots, P_g$ are distinct prime ideals of B, and let $f_i = f(P_i/\wp)$ for $1 \leq i \leq g$. For any $\sigma \in \mathrm{Gal}(L/K)$, we clearly have $\sigma(\wp) = \wp$ and $\sigma(B) = B$, and hence

$\sigma(\wp B) = \wp B$. By the above Lemma, for any i with $1 \leq i \leq g$, 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: With the notation and assumptions as in the above Theorem, we see that the ramification index $e(P/\wp)$ of a prime P of B lying over $\wp$ is independent of the choice of P. Thus it is sometimes denoted by $e_\wp$. Likewise, in the case of Galois extensions, the notation $f_\wp$ and $g_\wp$ is sometimes used.

2.5 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 $\wp$ be a nonzero prime ideal of A. Let $\bar{A} = A/\wp$. Assume that $\bar{A}$ is a perfect field.[7] Let $e = e_\wp$, $f = f_\wp$. and $g = g_\wp$.

Observe that $|G| = [L : K] = efg$. Also note that if P is any prime of B lying over $\wp$, then the set primes of B lying over $\wp$ 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. Given any prime ideal P of B lying over $\wp$, 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 $\wp$. 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 $\wp$, 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 $\wp$ and it may be denoted by $D_\wp$.

Lemma. *Let P be a prime ideal of B lying over $\wp$, 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*

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

[7] 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 $\wp A_D$ 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 2.2 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 $e(P_D/\wp) = 1$ and $f(P_D/\wp) = 1$. If D is normal, then clearly K_D/K is Galois and $e(P'/\wp) = 1 = f(P'/\wp)$, for any prime P' of A_D lying over $\wp$. 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 $\wp$ 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

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

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 alternately 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. *The residue extension $\bar{B}/\bar{A}$ is normal, and the homomorphism $\epsilon : D \to \mathrm{Gal}(\bar{B}/\bar{A})$ 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 $\wp$. 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. *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*

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

In particular, we see that $\wp$ is unramified in K_T.

Proof: Since $|D| = ef$ and $[\bar{B} : \bar{A}] = f$, it follows from the previous lemma 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 $K, A, \wp$ 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 of ramification indices and residue degrees. □

Exercise 2.3: 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 2.4: 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 2.5*: 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: Let $K_\wp$ be the completion of K w.r.t. the valuation of K corresponding to $\wp$ (whose valuation ring is $A_\wp$), 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 $K_\wp$. Since $K_\wp$ is complete, there is only one prime of L_P lying over the prime (or the corresponding valuation) of $K_\wp$. 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 $L_P/K_\wp$ is precisely e, and we have $ef = [L_P : K_\wp]$. Moreover, every element of the decomposition group $D = D_P(L/K)$ extends by continuity to an $K_\wp$–automorphism of L_P, and since $|D| = ef$, it follows that $\mathrm{Gal}(L_P/K_\wp) \simeq D_P(L/K)$. 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 $\mathrm{Gal}(L_P/K_\wp) \simeq \mathrm{Gal}(\bar{B}/\bar{A}) \simeq \mathrm{Gal}(\bar{L}_P/\bar{K}_\wp)$, where $\bar{L}_P$ and $\bar{K}_\wp$ denote the residue fields of (the valuation rings of) L_P and $K_\wp$ respectively, so that the local Galois group $\mathrm{Gal}(L_P/K_\wp)$ is cyclic. For more on these matters, see [11]

2.6 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 (cf. §2.2) 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, 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.[8]

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

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

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

[8] 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, 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 §2.3.

Exercise 2.6 (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 $\mathbb{Z}[i]$. [9] 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 $n = p_1^{e_1} \dots p_h^{e_h}$ where $p_1, \dots, p_h$ are distinct primes and $e_1, \dots, e_h$ 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 which is applicable since $\mathcal{O} = \mathbb{Z}[\zeta]$). Let q be a rational prime different

[9] 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.

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., $q^f \equiv 1 (\text{mod } p)$. Moreover, if for some $l < f$, $q^l \equiv 1 (\text{mod } p)$, 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 $q^f \equiv 1 (\text{mod } p)$. 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. 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 2.7: Let p, ζ and K be as above. Let H be the unique subgroup of index 2 in the cyclic group $\text{Gal}(\mathbb{Q}(\zeta)/\mathbb{Q})$. 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 $\left(\frac{a}{p}\right) \equiv a^{\frac{p-1}{2}} (\text{mod } p)$.] 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 $\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{\frac{(p-1)}{2}\frac{(q-1)}{2}}$.

Bibliography

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

[4] S. R. Ghorpade, Notes on Galois Theory, IIT Bombay, 1994.

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

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

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

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

[9] J. Neukirch, Class Field Theory, Springer–Verlag, 1986.

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

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

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

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

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