Notes on Galois Theory

Sudhir R. Ghorpade

Department of Mathematics, Indian Institute of Technology, Bombay 400 076

E-mail : srg@math.iitb.ac.in

October 1994

Contents

1 Preamble **2**

2 Field Extensions **3**

3 Splitting Fields and Normal Extensions **6**

4 Separable Extensions **9**

5 Galois Theory **11**

6 Norms and Traces **16**

---

1 Preamble

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

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

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

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

2 Field Extensions

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

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

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

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

$$L \; is \; finite \; over \; K \Leftrightarrow L \; is \; finite \; over \; E \; and \; E \; is \; finite \; over \; K$$

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

Let us obtain some useful consequences of the above lemma.

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

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

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

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

which shows that α is algebraic over K. □

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

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

Then E is a subfield of L containing K.

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

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

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

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

3 Splitting Fields and Normal Extensions

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

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

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

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

Remark: The above proof, though common in many texts, is slightly imprecise. To be pedantic, an actual extension E of K as in the statement of Lemma 6 can be constructed by putting

$$E = (\sigma(K[X])\backslash\sigma(K)) \cup K$$

where σ is as in the above proof, and by defining field operations on E in an obvious manner. Note that we then have $E \simeq \sigma(K[X])$.

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

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

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

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

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

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

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

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

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

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

Note: A field has no proper ideals. This means that a homomorphism of a field (into a ring) is either injective or maps everything to 0. If L is an extension of K, by a *K–homomorphism* of L we mean a homomorphism $\sigma : L \to L'$, where L' is some extension of K, which is identity on K, i.e., $\sigma(c) = c \ \forall\, c \in K$. Observe that a K–homomorphism is always injective.[4] Also observe that, when L/K is finite, a K–homomorphism $\sigma : L \to L$ is necessarily an automorphism (= isomorphism onto itself) of L [because $\sigma(L)$ is a subspace of L and the vector space dimension over K of L and $\sigma(L)$ is the same].

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

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

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

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

Proof: Let $n = \deg f(X) = \deg f^\sigma(X) \geq 1$. We proceed by induction on n. If $n = 1$, we

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

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

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

Corollary: *Any two splitting fields over K of a nonconstant polynomial in $K[X]$ are K–isomorphic.* □

A notion closely related to splitting fields is defined below.

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

And here is the connection.

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

(1) L is a normal extension of K.

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

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

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

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

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

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

Example: The usual formula for the roots of a quadratic equation shows that an extension of degree 2 is always normal. Extensions of $\mathbb{Q}$ of degree 2 are called *quadratic fields*. If ω is a "primitive n–th root of unity" (i.e., $\omega^n = 1$ and $\omega^m \neq 1$ for $1 \leq m < n$), then $\mathbb{Q}(\omega)$ is a normal extension of $\mathbb{Q}$ (prove!); it is called the *cyclotomic field* of the n–th roots of unity.

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

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

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

4 Separable Extensions

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

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

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

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

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

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

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

To check separability, the notion of derivatives comes in handy. In Algebra, derivatives can be defined in a purely formal manner (i.e., without involving limits) as follows. Given

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

any $f(X) \in K[X]$, let $f(X) = \sum_{i=0}^{n} a_i X^i$, with $a_i \in K$, and define the *derivative* of $f(X)$, denoted by $f'(X)$, by $f'(X) = \sum_{i=1}^{n} i a_i X^{i-1}$. The usual properties such as linearity [i.e., $(af \pm bg)' = af' \pm bg'$], product rule [i.e., $(fg)' = f'g + fg'$], can be easily checked using this definition. Now recall that an element α in an extension L of K is called a *multiple root* of $f(X) \in K[X]$ if $f(X) = (X - \alpha)^2 g(X)$ for some $g(X) \in L[X]$.

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

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

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

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

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

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

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

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

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

Exercise 11: Prove that a finite field is perfect.

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

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

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

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

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

5 Galois Theory

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

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

Definitions: Let L/K be a field extension.

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

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

[7]Galois showed that the equation $f(X) = 0$ is solvable by radicals (like the quadratic equation) if and only if G, the Galois group of $f(X)$, is a solvable group. The Galois group of a general equation of degree n turns out to be S_n, which is not solvable for $n \geq 5$, and thus general equations of degree 5 or more cannot be solved by radicals. For details, see any of the references given at the end of this section. It may be worth noting that Evariste Galois, the inventor of Galois theory, did his work at a very early age. He was born in October 1811, and he died twenty years and seven months later in a duel.

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

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

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

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

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

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

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

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

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

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

and, in this case,

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

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

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

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

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

an E–automorphism $\sigma : L \to L$. Now $\sigma \in \mathrm{Gal}(L/E)$ and $\sigma(\beta) = \beta' \neq \beta$, which contradicts the assumption on β. $\square$

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

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

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

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

Consider the polynomial

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

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

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

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

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

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

From Lemma 11, it follows that

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

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

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

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

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

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

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

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

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

Exercise 17: Let E and F be subfields of a field L and K be a subfield of $E \cap F$. Let EF denote the smallest subfield of L containing E and F (this looks like $\{\sum \alpha_i\beta_i : \alpha_i \in E, \ \beta_i \in$

[9]The term 'abelian' is derived from the name of the Norwegian mathematician N. H. Abel who proved, around 1829, that a certain class of equations is always solvable by radicals. In the modern terminology, this is precisely the class of equations whose Galois group is commutative. The usage of 'abelian' seems to have been initiated by L. Kronecker who, in 1853, announced that *the roots of every abelian equation with integer*

$F\}$, and is called the *compositum* of E and F). Show that if E/K is Galois, then so is EF/F, and that $\sigma \mapsto \sigma|_E$ is an injective homomorphism of $\mathrm{Gal}(EF/F)$ into $\mathrm{Gal}(E/K)$ which is an isomorphism if $K = E \cap F$. Also show that if E/K and F/K are Galois and $K = E \cap F$, then $\mathrm{Gal}(EF/K) \simeq \mathrm{Gal}(E/K) \times \mathrm{Gal}(F/K)$. In particular, if $\mathrm{Gal}(E/K)$ and $\mathrm{Gal}(F/K)$ are abelian, then so is $\mathrm{Gal}(EF/K)$, and thus one can talk of the *maximal abelian extension* of K in L.

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

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

Annotated List of Reference for Galois Theory

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

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

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

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

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

coefficients can be represented as rational functions of roots of unity, a result which is nowadays known as the Kronecker–Weber Theorem and is usually expressed as: *every abelian extension of* $\mathbb{Q}$ *is contained in a cyclotomic field*. In an 1870 paper, Kronecker formally defined "abstract abelian groups" and proved what is now known as the Structure Theorem for Finite Abelian Groups. To get an idea of Abel's work on solvability by radicals, see Van der Waerden's enchanting book "A History of Algebra", Springer (1985).

[10] It is not difficult to see that the answer is Yes if G is an abelian group. For recent work on this problem, see the article by B. Matzat in the MSRI Proceedings on "Galois groups over $\mathbb{Q}$" published by Springer (1988) or his german book "Konstruktive Galoistheorie", Springer LNM 1284 (1987).

[5] T. Hungerford, *Algebra*, Springer GTM 73, 1980 (Ch. V).

a useful reference; contains a treatment applying also to infinite extensions.

[6] N. Jacobson, *Basic Algebra I*, 2nd Ed., W. H. Freeman, 1985 (Ch. IV).

the introduction to the chapter is highly readable and informative; the 2nd Ed. has a valuable section on mod p reduction.

[7] S. Lang, *Algebra*, 2nd Ed., Addison–Wesley, 1984 (Ch. VII, VIII).

a neat exposition of the elements of Galois theory as well as more advanced material; contains a good collection of exercises.

[8] TIFR Mathematical Pamphlet on *Galois Theory*, No. 3, 1965.

short, self–contained, neat, and thorough; seek elsewhere for motivation and history.

6 Norms and Traces

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

and, in particular,

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

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

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

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

$$\alpha(u_i v_j) = \sum_{l=1}^{s} a_{jl}(u_i v_l) = \sum_{\substack{1 \leq k \leq r \\ 1 \leq l \leq s}} a_{jl}\delta_{ik}(u_k v_l).$$

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

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

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

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

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

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

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

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

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

Let L/K be a finite separable extension of degree n, $\alpha \in L$, and N be a normal extension of K containing L [such N exists by Exercise 7; it can, for example, be the least Galois extension of K containing L]. By Lemma 12 and the Corollary to Lemma 9, we see that there exist exactly n distinct K–isomorphisms $\sigma_1, \ldots, \sigma_n$ of L into N. Clearly, $\sigma_i(\alpha)$ and α are conjugates over K for each i with $1 \leq i \leq n$. The n elements $\sigma_1(\alpha), \ldots, \sigma_n(\alpha)$ will be called the *conjugates of α w.r.t. L/K*; these are uniquely determined provided we fix our N. Note that these n elements need not be distinct; in fact, the number of distinct conjugates among these is $[K(\alpha) : K]$ and each of these is repeated exactly $[L : K(\alpha)]$ times. (This follows from Exercise 12. Verify!)

Lemma 20: *Let L/K be a finite separable extension of degree n and $\alpha \in L$. Fix a normal extension N of K containing L. Then:*

(1) $\mathrm{Tr}_{L/K}(\alpha)$ *is the sum of all conjugates of* α *w.r.t.* L/K*. In particular, if* L/K *is Galois, then*

$$\mathrm{Tr}_{L/K}(\alpha) = \sum_{\sigma \in \mathrm{Gal}(L/K)} \sigma(\alpha).$$

(2) $N_{L/K}(\alpha)$ *is the product of all conjugates of* α *w.r.t.* L/K*. In particular, if* L/K *is Galois, then*

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

Proof: Let $r = [L : K(\alpha)]$ and $s = [K(\alpha) : K]$. If $\tau_1, \ldots, \tau_r$ are the distinct K–homomorphisms of $K(\alpha)$ into N, then $\tau_1(\alpha), \ldots, \tau_s(\alpha)$ are precisely the distinct conjugates of α w.r.t. L/K and the minimal polynomial of α over K factors as

$$\mathrm{Irr}(\alpha, K) = \prod_{j=1}^{s} (X - \tau_j(\alpha))$$

Now the conjugates $\sigma_1(\alpha), \ldots, \sigma_n(\alpha)$ of α w.r.t. K are nothing but $\tau_1(\alpha), \ldots, \tau_s(\alpha)$ each repeated r times. Hence, by the Corollary to Lemma 19, we see that

$$\Phi(X) = \prod_{i=1}^{n} (X - \sigma_i(\alpha))$$

where $\Phi(X)$ denotes the field polynomial of α w.r.t. L/K. In view of Lemma 18, the above identity readily implies (1) and (2). □

Remark: In the above Lemma and the discussion preceding that, we could have replaced N by an algebraic closure[12] of K (assumed to contain L). Fixing an algebraic closure $\overline{K}$ of K, one can define $\mathrm{Gal}(L/K)$, for any separable extension L/K with $L \subseteq \overline{K}$, to be the set of all K–homomorphisms of L into $\overline{K}$. With this convention, the displayed identities for the trace and norm in Lemma 20 remain valid for any finite separable extension L/K. Our definition of $\mathrm{Gal}(L/K)$ applies only to Galois extensions but it has the advantage that we don't have to talk about algebraic closures, and that we can legitimately call it the Galois *group*.

Exercise 19: Let L/K be a finite separable extension and E be a subfield of L containing K. Prove the following transitivity properties of the trace and norm.

$$\mathrm{Tr}_{L/K} = \mathrm{Tr}_{E/K} \circ \mathrm{Tr}_{L/E} \quad \text{and} \quad N_{L/K} = N_{E/K} \circ N_{L/E}.$$

[12]By an *algebraic closure* of a field K we mean an algebraic extension $\overline{K}$ of K such that every nonconstant polynomial in $\overline{K}[X]$ has a root in $\overline{K}$. It can be shown that every field K has an algebraic closure with the property that any algebraic extension of K is isomorphic to some subfield of it; further any two algebraic closures of K are K–isomorphic. For details, see Lang's "Algebra".

Let A be a ring (always assumed to be commutative with unity). Recall that an element α in an overring of A (i.e., a ring containing A as a subring) is said to be *integral* over A if it satisfies a monic polynomial with coefficients in A. The *integral closure* of A in an overring L is defined as the set of all the elements in L which are integral over A, and can be seen to be a subring of A. A domain is said to be *normal* or *integrally closed* if it is equal to its integral closure in its quotient field. Note that $\mathbb{Z}$ is an example of a normal domain. The integral closure of $\mathbb{Z}$ in an algebraic number field is called the *ring of (algebraic) integers* in that algebraic number field. The integral closure of $\mathbb{Z}$ in a cyclotomic field (i.e., a field obtained by adjoining to $\mathbb{Q}$ a primitive n–th root of unity) is sometimes referred to as a *ring of cyclotomic integers*.

Exercise 20: Let A be a domain, K its quotient field, and α an element in a finite separable extension L of K. Show that if α is integral over A, then so is every conjugate of α w.r.t. L/K. Deduce that if A is normal, then the field polynomial of α w.r.t. L/K and the minimal polynomial of α over K have coefficients in A, and $\mathrm{Tr}_{L/K}(\alpha)$ and $N_{L/K}(\alpha)$ are elements of A.

Remark: Given a finite extension L/K of degree n and elements $u_1, \ldots, u_n$ in L, we define the *discriminant* of $u_1, \ldots, u_n$ w.r.t. L/K, denoted by $\mathrm{Disc}_{L/K}(u_1, \ldots, u_n)$, to be $\det\left(\mathrm{Tr}_{L/K}(u_i u_j)\right)$. If $\{u_1, \ldots, u_n\}$ and $\{v_1, \ldots, v_n\}$ are any two K–bases of L and $v_i = \sum_{j=1}^{n} a_{ij} u_j$, then $\mathrm{Disc}_{L/K}(v_1, \ldots, v_n) i = [\det(a_{ij})]^2 \mathrm{Disc}_{L/K}(u_1, \ldots, u_n)$, and thus one of them vanishes iff the other does. It can be seen that the discriminant of a K–basis of L is nonzero iff L/K is separable. Now suppose L/K is separable, $L = K(\alpha)$, and $f(X) = \mathrm{Irr}(\alpha, K)$. Let $\alpha^{(1)}, \ldots, \alpha^{(n)}$ be a set of conjugates of α w.r.t. L/K. Then we have:

$$\mathrm{Disc}_{L/K}(1, \alpha, \ldots, \alpha^{n-1}) = \prod_{1 \le i < j \le n} \left(\alpha^{(i)} - \alpha^{(j)}\right)^2 = (-1)^{\frac{n(n-1)}{2}} N_{L/K}(f'(\alpha)).$$

If $f(X)$ happens to be $X^2 + bX + c$ or $X^3 + pX + q$, then we can verify that the above discriminant equals $b^2 - 4c$ or $-4p^3 - 27q^2$, as is to be expected. It may be noted that in the Theory of Equations, the classical discriminant of a quadratic, cubic, etc. is generalised to the discriminant of a polynomial of any degree, say $g(X) = a_0 X^m + a_1 X^{m-1} + \cdots + a_m$, by defining it as the "resultant" $\mathrm{Res}(g(X), g'(X))$ of the polynomial and its derivative. [13] It is not difficult to see that these two notions of discriminant aren't really different. In fact, they differ only by $(-1)^{n(n-1)/2}$.

[13] Briefly, the resultant of two polynomials in one variable X, is the result of elimination of X between them. In greater detail, if $\phi(X) = b_0 X^r + b_1 X^{r-1} + \cdots + b_r$ and $\psi(X) = c_o X^s + c_1 X^{s-1} + \cdots + c_s$ are two polynomials, then, upon letting $b_i = 0$ if either $i < 0$ or $i > r$ and $c_j = 0$ if either $j < 0$ or $j > s$, the *resultant* $\mathrm{Res}(\phi, \psi)$ is defined as the determinant of the $(r+s) \times (r+s)$ matrix whose (i,j)–th entry, for $1 \le j \le r+s$, is b_{j-i} if $1 \le i \le r$ and is c_{j+r-i} if $r+1 \le i \le r+s$. See, for example, Van der Waerden's book on Algebra for a discussion of the resultant.