Graduate Texts in Mathematics

Steven Roman

Field Theory

Springer Science+Business Media, LLC

Graduate Texts in Mathematics 158

Graduate Texts in Mathematics

1 TAKEUTI/ZARING. Introduction to Axiomatic Set Theory. 2nd ed.
2 OXTOBY. Measure and Category. 2nd ed.
3 SCHAEFFER. Topological Vector Spaces.
4 HILTON/STAMMBACH. A Course in Homological Algebra.
5 MAC LANE. Categories for the Working Mathematician.
6 HUGHES/PIPER. Projective Planes.
7 SERRE. A Course in Arithmetic.
8 TAKEUTI/ZARING. Axiomatic Set Theory.
9 HUMPHREYS. Introduction to Lie Algebras and Representation Theory.
10 COHEN. A Course in Simple Homotopy Theory.
11 CONWAY. Functions of One Complex Variable. 2nd ed.
12 BEALS. Advanced Mathematical Analysis.
13 ANDERSON/FULLER. Rings and Categories of Modules. 2nd ed.
14 GOLUBITSKY/GUILEMIN. Stable Mappings and Their Singularities.
15 BERBERIAN. Lectures in Functional Analysis and Operator Theory.
16 WINTER. The Structure of Fields.
17 ROSENBLATT. Random Processes. 2nd ed.
18 HALMOS. Measure Theory.
19 HALMOS. A Hilbert Space Problem Book. 2nd ed.
20 HUSEMOLLER. Fibre Bundles. 3rd ed.
21 HUMPHREYS. Linear Algebraic Groups.
22 BARNES/MACK. An Algebraic Introduction to Mathematical Logic.
23 GREUB. Linear Algebra. 4th ed.
24 HOLMES. Geometric Functional Analysis and Its Applications.
25 HEWITT/STROMBERG. Real and Abstract Analysis.
26 MANES. Algebraic Theories.
27 KELLEY. General Topology.
28 ZARISKI/SAMUEL. Commutative Algebra. Vol.I.
29 ZARISKI/SAMUEL. Commutative Algebra. Vol.II.
30 JACOBSON. Lectures in Abstract Algebra I. Basic Concepts.
31 JACOBSON. Lectures in Abstract Algebra II. Linear Algebra.
32 JACOBSON. Lectures in Abstract Algebra III. Theory of Fields and Galois Theory.
33 HIRSCH. Differential Topology.
34 SPITZER. Principles of Random Walk. 2nd ed.
35 WERMER. Banach Algebras and Several Complex Variables. 2nd ed.
36 KELLEY/NAMIOKA et al. Linear Topological Spaces.
37 MONK. Mathematical Logic.
38 GRAUERT/FRITZSCHE. Several Complex Variables.
39 ARVESON. An Invitation to C^*-Algebras.
40 KEMENY/SNELL/KNAPP. Denumerable Markov Chains. 2nd ed.
41 APOSTOL. Modular Functions and Dirichlet Series in Number Theory. 2nd ed.
42 SERRE. Linear Representations of Finite Groups.
43 GILLMAN/JERISON. Rings of Continuous Functions.
44 KENDIG. Elementary Algebraic Geometry.
45 LOÈVE. Probability Theory I. 4th ed.
46 LOÈVE. Probability Theory II. 4th ed.
47 MOISE. Geometric Topology in Dimensions 2 and 3.
48 SACHS/WU. General Relativity for Mathematicians.
49 GRUENBERG/WEIR. Linear Geometry. 2nd ed.
50 EDWARDS. Fermat's Last Theorem.
51 KLINGENBERG. A Course in Differential Geometry.
52 HARTSHORNE. Algebraic Geometry.
53 MANIN. A Course in Mathematical Logic.
54 GRAVER/WATKINS. Combinatorics with Emphasis on the Theory of Graphs.
55 BROWN/PEARCY. Introduction to Operator Theory I: Elements of Functional Analysis.
56 MASSEY. Algebraic Topology: An Introduction.
57 CROWELL/FOX. Introduction to Knot Theory.
58 KOBLITZ. p-adic Numbers, p-adic Analysis, and Zeta-Functions. 2nd ed.
59 LANG. Cyclotomic Fields.
60 ARNOLD. Mathematical Methods in Classical Mechanics. 2nd ed.
61 WHITEHEAD. Elements of Homotopy Theory.
62 KARGAPOLOV/MERLZJAKOV. Fundamentals of the Theory of Groups.
63 BOLLOBAS. Graph Theory.
64 EDWARDS. Fourier Series. Vol. I. 2nd ed.

continued after index

Steven Roman

Field Theory

Springer Science+Business Media, LLC

Steven Roman
Department of Mathematics
California State University
Fullerton, CA 92637
USA

Mathematics Subject Classifications (1991): 12-01

With 8 Illustrations.

Library of Congress Cataloging-in-Publication Data
Roman, Steven.
Field theory / Steven Roman.
p. cm. — (Graduate texts in mathematics ; 158)
Includes bibliographical references and indexes.

1. Algebraic fields. 2. Galois theory. 3. Polynomials.
I. Title. II. Series.
QA247.R598 1995
512'.3—dc20 94-36400

Printed on acid-free paper.

Originally published by Springer-Verlag New York, Inc., in 1995

Production managed by Hal Henglein; manufacturing supervised by Genieve Shaw.
Camera-ready copy prepared by the author using EXP®

9 8 7 6 5 4 3 2 1

ISBN 978-0-387-94408-1 ISBN 978-1-4612-2516-4 (eBook)
DOI 10.1007/978-1-4612-2516-4

To Donna

Preface

This book presents the basic theory of fields, starting more or less from the beginning. It is suitable for a graduate course in field theory, or independent study. The reader is expected to have absorbed a serious undergraduate course in abstract algebra, not so much for the material it contains but for the oft-mentioned *mathematical maturity* it provides.

The book begins with a preliminary chapter (Chapter 0), which is designed to be quickly scanned or skipped and used as a reference if needed. The remainder of the book is divided into three parts.

Part 1, entitled *Basic Theory*, begins with a chapter on polynomials. Chapter 2 is devoted to various types of field extensions. In Chapter 3, we treat algebraic independence, starting with the general notion of a dependence relation and concluding with Luroth's Theorem on intermediate fields of a simple transcendental extension. Chapter 4 is devoted to the notion of separability of algebraic extensions.

Part 2 of the book is entitled *Galois Theory*. Chapter 5 begins with the notion of a Galois correspondence between two partially ordered sets, and then specializes to the Galois correspondence of a field extension, concluding with a brief discussion of the Krull topology. In Chapter 6, we discuss the Galois theory of equations. In Chapter 7, we take a closer look at a finite field extension E of F as a vector space over F. The next two chapters are devoted to a fairly thorough discussion of finite fields. Möbius inversion is used in a few brief spots in these chapters, so an appendix has been included on this subject.

Part 3 of the book is entitled *The Theory of Binomials*. Chapter 10 covers the roots of unity (that is, the roots of the binomial $x^n - 1$) and includes Wedderburn's theorem (a finite division ring is a field). This

also seems like the appropriate time to discuss the question of whether a given group is the Galois group of a field extension. In Chapter 11, we characterize the splitting fields of binomials $x^n - u$, when the base field contains the n-th roots of unity. Chapter 12 is devoted to the question of solvability of a polynomial equation by radicals. (This chapter might make a convenient ending place in a graduate course.) In Chapter 13, we determine conditions that characterize the irreducibility of a binomial and describe the Galois group of a binomial. Chapter 14 briefly describes the theory of families of binomials – the so-called *Kummer theory.*

Sections marked with an asterisk are optional, in that they may be skipped without loss of continuity. The unmarked sections might be considered as forming a basic core course in field theory.

Contents

Sections marked with an asterisk are optional.

Chapter 0
Preliminaries

The purpose of this chapter is to review some basic facts that will be needed in the book. The discussion is not intended to be complete, nor are all proofs supplied. We suggest that the reader quickly skim this chapter (or skip it altogether) and use it as a reference if needed.

0.1 Lattices

Definition A **partially ordered set** (or **poset**) is a nonempty set P, together with a binary relation $\leq$ on P satisfying the following properties. For all $\alpha, \beta, \gamma \in P$,

1) (**reflexivity**) $\alpha \leq \alpha$
2) (**antisymmetry**) $\alpha \leq \beta, \beta \leq \alpha \Rightarrow \alpha = \beta$
3) (**transitivity**) $\alpha \leq \beta, \beta \leq \gamma \Rightarrow \alpha \leq \gamma$

If, in addition,

$$\alpha, \beta \in P \Rightarrow \alpha \leq \beta \text{ or } \beta \leq \alpha$$

then P is said to be **totally ordered.** □

Any subset of a poset P is also a poset under the restriction of the relation defined on P. A totally ordered subset of a poset is called a **chain.** If $S \subseteq P$ and $s \leq \alpha$ for all $s \in S$ then α is called an **upper bound** for S. A **least upper bound** for S, denoted by lub(S) or $\vee S$, is an upper bound that is less than or equal to any other upper bound. Similar statements hold for lower bounds and greatest lower bounds, the latter

denoted by glb(S), or $\wedge S$. A **maximal element** in a poset P is an element $\alpha \in P$ such that $\alpha \leq \beta$ implies $\alpha = \beta$. A **minimal element** in a poset P is an element $\gamma \in P$ such that $\beta \leq \gamma$ implies $\beta = \gamma$. **Zorn's Lemma** says that if every chain in a poset P has an upper bound in P then P has a maximal element.

Definition A **lattice** is a poset L in which every pair of elements α, $\beta \in L$ has a least upper bound, or **join**, denoted by $\alpha \vee \beta$ and a greatest lower bound, or **meet**, denoted by $\alpha \wedge \beta$. If every nonempty subset of L has a join and a meet then L is called a **complete lattice.** □

Note that any nonempty complete lattice has a greatest element, denoted by 1 and a smallest element, denoted by 0.

Definition A **sublattice** of a lattice L is a subset S of L that is closed under meets and joins. □

It is important to note that a subset S of a lattice L can be a lattice under the same order relation and yet not be a sublattice of L. As an example, consider the collection $\mathcal{S}$ of all subgroups of a group G, ordered by inclusion. Then $\mathcal{S}$ is a subset of the power set $\mathcal{P}(G)$, which is a lattice under union and intersection. But $\mathcal{S}$ is not a sublattice of $\mathcal{P}(G)$ since the union of two subgroups need not be a subgroup. On the other hand, $\mathcal{S}$ is a lattice in its own right under set inclusion, where the meet $H \wedge K$ of two subgroups is their intersection and the join $H \vee K$ is the smallest subgroup of G containing H and K.

In a complete lattice L, joins can be defined in terms of meets: $\vee T$ is the meet of all upper bounds of T. The fact that $1 \in L$ insures that T has at least one upper bound, so that the meet is not an empty one. The following theorem exploits this idea to give conditions under which a subset of a complete lattice is itself a complete lattice.

Theorem 0.1.1 Let L be a complete lattice. If $S \subseteq L$ has the properties (i) $1 \in S$ and (ii) $T \subseteq S$, $T \neq \emptyset \Rightarrow \wedge T \in S$, then S is a complete lattice.

Proof. Let $T \subseteq S$. Then $\wedge T \in S$ by assumption. Let U be the set of all upper bounds of T that lie in S. Since $1 \in S$, we have $U \neq \emptyset$. Hence, $\wedge U \in S$ and is $\vee T$. Thus, S is a complete lattice. (Note that S need not be a sublattice of L since $\wedge U$ need not equal the meet of *all* upper bounds of T in L.) ∎

0.2 Groups

Definition A **binary operation** on a set A is a map from $A \times A$ to A. □

Definition A **group** is a nonempty set G, together with a binary operation on G, denoted by juxtaposition, with the following properties:

1) (**Associativity**) $(\alpha\beta)\gamma = \alpha(\beta\gamma)$ for all $\alpha, \beta, \gamma \in G$;
2) (**Identity**) There exists an element $\epsilon \in G$ for which $\epsilon\alpha = \alpha\epsilon = \alpha$ for all $\alpha \in G$;
3) (**Inverses**) For each $\alpha \in G$, there is an element $\alpha^{-1} \in G$ for which $\alpha\alpha^{-1} = \alpha^{-1}\alpha = \epsilon$.

A group G is **abelian**, or **commutative**, if $\alpha\beta = \beta\alpha$, for all $\alpha, \beta \in G$. □

The identity element is often denoted by 1. When G is abelian, the group operation is often denoted by $+$ and the identity by 0.

Definition A **subgroup** S of a group G is a subset of G that is a group in its own right, using the restriction of the operation defined on G. We denote the fact that S is a subgroup of G by writing $S < G$. □

Let G be a group. Since G is a subgroup of itself and since the intersection of subgroups of G is a subgroup of G, Theorem 0.1.1 implies that the set of subgroups of G forms a complete lattice, where $H \wedge J = H \cap J$ and $H \vee J$ is the smallest subgroup of G containing both H and J. We denote this lattice by $\mathcal{S}(G)$.

A group G is **finite** if it contains only a finite number of elements. The cardinality of a finite group G is called its **order** and is denoted by $|G|$ or $o(G)$. If $\alpha \in G$, and if $\alpha^k = \epsilon$ for some integer k, we say that k is an **exponent** of α. The smallest positive exponent for $\alpha \in G$ is called the **order** of α and is denoted by $o(\alpha)$. An integer m for which $\alpha^m = 1$ for all $\alpha \in G$ is called an **exponent** of G. (Note: Some authors use the term exponent of G to refer to the *smallest* positive exponent of G.)

Theorem 0.2.1 Let G be a group and let $\alpha \in G$. Then k is an exponent of α if and only if k is a multiple of $o(\alpha)$. Similarly, the exponents of G are precisely the multiples of the smallest positive exponent of G. □

While the smallest positive exponent of an element $\alpha \in G$ is the order of the cyclic subgroup $\langle\alpha\rangle = \{\alpha^n \mid n \in \mathbb{Z}\}$, this does not extend to groups in general, that is, the smallest positive exponent of G may be smaller than the order of G. (Example: $\mathbb{Z}_2 \times \mathbb{Z}_2$ has exponent 2 but order 4.) We next characterize the smallest positive exponent for finite abelian groups.

Theorem 0.2.2 Let G be a finite abelian group.

1) If m is the maximum order of all elements in G then $\alpha^m = 1$ for all $\alpha \in G$. Thus, the smallest positive exponent of G is equal to the maximum order of all elements of G.
2) The smallest positive exponent of G is equal to $o(G)$ if and only if G is cyclic.

Proof. Let α have maximum order m among all the elements in G. Suppose that $\beta^m \neq 1$ for some $\beta \in G$ and let $o(\beta) = k < m$. It follows that $k \nmid m$ and so there exists a prime p for which $p^u \mid k$ but $p^u \nmid m$. Let $v < u$ be the largest integer for which $p^v \mid m$. Consider the elements

$$\alpha' = \alpha^{p^v} \text{ and } \beta' = \beta^{k/p^u}$$

Since $o(\alpha') = m/p^v$ and $o(\beta') = p^u$ and since $(m/p^v, p^u) = 1$, it follows that

$$o(\alpha'\beta') = o(\alpha')o(\beta') = mp^{u-v} > m$$

in contradiction to the maximality of m. Thus, all elements $\beta \in G$ satisfy $\beta^m = 1$. Clearly, $m = o(\alpha)$ is the smallest such positive integer and part 1) is proved. Part 2) follows easily from part 1), since a finite group G is cyclic if and only if it has an element of order $o(G)$. ∎

Let $H < G$. We may define an equivalence relation on G by saying that $\alpha \sim \beta$ if $\beta^{-1}\alpha \in H$ (or equivalently $\alpha^{-1}\beta \in H$). The equivalence classes are the **left cosets** $\alpha H = \{\alpha h \mid h \in H\}$ of H in G. Thus, the distinct left cosets of H form a partition of G. Similarly, the distinct **right cosets** $H\alpha$ form a partition of G. It is not hard to see that all cosets of H have the same cardinality and that there are the same number of left cosets of H in G as right cosets. (This is easy when G is finite. Otherwise, consider the map $\alpha H \mapsto H\alpha^{-1}$.)

Definition The **index** of H in G, denoted by (G:H), is the cardinality of the set G/H of all distinct left cosets of H in G. If G is finite then $(G:H) = |G|/|H|$. □

Theorem 0.2.3 Let G be a finite group.

1) (**Lagrange**) The order of any subgroup of G divides the order of G.
2) The order of any element of G divides the order of G.
3) (**Converse of Lagrange's Theorem for Finite Abelian Groups**) If A is a finite *abelian* group and if $k \mid o(A)$ then A has a subgroup of order k. □

Normal Subgroups

Definition A subgroup H of G is **normal** in G, written $H \triangleleft G$, if $\alpha H \alpha^{-1} = H$ for all $\alpha \in G$. □

Definition A group G is **simple** if it has no normal subgroups other than $\{1\}$ and G. □

Theorem 0.2.4 The following are equivalent for a subgroup H of G.

1) $H \triangleleft G$.
2) $\alpha H = H\alpha$ for all $\alpha \in G$.
3) For all $\alpha \in G$, there exists a $\beta \in G$ such that $\alpha H = H\beta$.
4) $\alpha H \alpha^{-1} \subseteq H$ for all $\alpha \in G$.
5) $\alpha\beta \in H \Rightarrow \beta\alpha \in H$ for all $\alpha, \beta \in G$. □

Theorem 0.2.5 Any subgroup H of a group G of index 2 is normal. □

Theorem 0.2.6 If G is a group and $\{H_i\}$ is a collection of normal subgroups of G then $\cap H_i$ and $\vee H_i$ are normal subgroups of G. Hence, the collection of normal subgroups of G is a complete sublattice of the complete lattice $\mathcal{L}(G)$ of all subgroups of G. □

Theorem 0.2.7 If $H < G$ then the set G/H of all right cosets of H in G forms a group under the operation $(\alpha H)(\beta H) = \alpha\beta H$ if and only if $H \triangleleft G$. The group G/H is called the **quotient group** (or **factor group**) of H in G. The order of G/H is (G:H). □

Euler's Formula

If α and β are integers, not both zero, then an integer δ is called a **greatest common divisor** (**gcd**) of α and β if (i) $\delta \mid \alpha$ and $\delta \mid \beta$ and (ii) if $\gamma \mid \alpha$ and $\gamma \mid \beta$ then $\gamma \mid \delta$. Note that if δ is a gcd of α and β, then so is $-\delta$. It is customary to denote a gcd of α and β by (α,β) or $\gcd(\alpha,\beta)$.

If $(\alpha,\beta) = 1$, then α and β are **relatively prime.** The **Euler phi function** ϕ is defined by letting $\phi(n)$ be the number of positive integers less than or equal to n that are relatively prime to n. The Euler phi function is *multiplicative*, that is,

$$\phi(mn) = \phi(m)\phi(n), \quad \text{when } (m,n) = 1$$

It also satisfies

$$\phi(p^n) = p^{n-1}(p-1), \qquad p \text{ prime}, n > 0$$

These two properties completely determine ϕ.

Two integers α and β are **congruent modulo n**, written $\alpha \equiv \beta \bmod n$, if $\alpha - \beta$ is divisible by n. Let $\mathbb{Z}_n$ denote the ring of integers $\{0,\ldots,n-1\}$ under addition and multiplication modulo n.

Theorem 0.2.8 (Euler's Theorem) If $\alpha, n \in \mathbb{Z}$ and $(\alpha,n) = 1$, then

$$\alpha^{\phi(n)} \equiv 1 \bmod n$$

Proof. We first show that the set $G = \{\beta \in \mathbb{Z}_n \mid (\beta,n) = 1\}$ is a group of order $\phi(n)$ under multiplication modulo n. Clearly, $\beta,\gamma \in G$ imply $\beta\gamma \in G$. Also, if $\beta \in G$, then there exists $a, b \in \mathbb{Z}$ such that $a\beta + bn = 1$ and so $a\beta \equiv 1 \bmod n$. Thus, $a \bmod n$ is the inverse of $\beta \in G$. Since G is a group of order $\phi(n)$, we deduce that $\alpha^{\phi(n)} \equiv 1 \bmod n$, for all $\alpha \in G$. If $\alpha \notin G$, then there exists an $\alpha' \in G$ for which $\alpha' \equiv \alpha \bmod n$. Since $(\alpha,n) = 1$ if and only if $(\alpha',n) = 1$, we have

$$\alpha^{\phi(n)} \equiv (\alpha')^{\phi(n)} \equiv 1 \bmod n \qquad \blacksquare$$

Corollary 0.2.9 (Fermat's Theorem) If p is a prime not dividing the integer α, then

$$\alpha^{p} \equiv \alpha \bmod p \qquad \square$$

Cyclic Groups

If G is a group and $\alpha \in G$, then the set of all powers of α

$$\langle\alpha\rangle = \{\alpha^n \mid n \in \mathbb{Z}\}$$

is a subgroup of G, called the **cyclic subgroup generated by α**. A group G is **cyclic** if it has the form $G = \langle\alpha\rangle$, for some $\alpha \in G$. In this case, we say that α **generates** G.

Theorem 0.2.10 Every subgroup of a cyclic group is cyclic. A finite abelian group G is cyclic if and only if its smallest positive exponent is equal to $o(G)$. $\square$

The following theorem contains some key results about finite cyclic groups.

Theorem 0.2.11 Let $G = \langle\alpha\rangle$ be a cyclic group of order n.

1) For $1 \leq k < n$,

$$o(\alpha^k) = \frac{n}{(n,k)}$$

In particular, α^k generates $G = \langle\alpha\rangle$ if and only if $(n,k) = 1$.

2) If $d \mid n$, then

$$o(\alpha^k) = d \iff k = r\frac{n}{d}, \text{ where } (r,d) = 1$$

Thus the elements of G of order $d \mid n$ are the elements of the form $\alpha^{rn/d}$, where $0 \leq r < d$ and r is relatively prime to d.

3) For each $d \mid n$, the group G has exactly one subgroup H_d of order d and $\phi(d)$ elements of order d, all of which lie in H_d.

Proof. To prove part 1), we first observe that if $d = (k,n)$ then $d = ak + bn$ for some integers a and b. Hence,

$$\alpha^d = (\alpha^k)^a \in \langle\alpha^k\rangle$$

whence $\langle\alpha^d\rangle \subseteq \langle\alpha^k\rangle$. But the reverse inclusion holds since $d \mid k$ and so $\langle\alpha^k\rangle = \langle\alpha^d\rangle$. Since $d \mid n$, it is clear that

$$o(\alpha^k) = o(\alpha^d) = \frac{n}{d} = \frac{n}{(n,k)}$$

To prove part 2), we let $d \mid n$ and solve the equation

$$\frac{n}{(n,k)} = d$$

Rearranging gives

$$n = d(n,k) = (dn,dk)$$

Setting $r = k/(n,k)$, we get $dk = n[k/(n,k)] = nr$ and so

$$n = (dn,rn) = n(d,r)$$

which holds if and only if $(d,r) = 1$.

For part 3), it follows from part 2) that all of the $\phi(d)$ elements of G of order d lie in the subgroup $H_d = \langle\alpha^{n/d}\rangle$. Moreover, if H is a subgroup of G of order d then, being cyclic, it must contain an element β of order d. But $\beta \in H_d$ and so $H = \langle\beta\rangle = H_d$. ∎

Counting the elements in a cyclic group of order n gives the following corollary.

Corollary 0.2.12 For any positive integer n,

$$n = \sum_{d \mid n} \phi(d)$$ □

Homomorphisms

Definition Let G and H be groups. A map ψ:G→H is called a **group homomorphism** if $\psi(\alpha\beta) = (\psi\alpha)(\psi\beta)$. A surjective homomorphism is an **epimorphism**, an injective homomorphism is a **monomorphism** and a bijective homomorphism is an **isomorphism**. If ψ:G→H is an isomorphism, we say that G and H are **isomorphic** and write $G \simeq H$. □

If ψ is a homomorphism then $\psi\epsilon = \epsilon$ and $\psi\alpha^{-1} = (\psi\alpha)^{-1}$. The **kernel** of a homomorphism ψ:G→H,

$$ker\,\psi = \{\alpha \in G \mid \psi\alpha = \epsilon\}$$

is a normal subgroup of G. Conversely, any normal subgroup H of G is the kernel of a homomorphism. For we may define the **natural projection** π:G→G/H by $\pi\alpha = \alpha H$. This is easily seen to be an epimorphism with kernel H.

Let f:S→T be a function from a set S to a set T. Let $\mathcal{P}(S)$ and $\mathcal{P}(T)$ be the power sets of S and T, respectively. We define the **induced map** f:$\mathcal{P}(S)$→$\mathcal{P}(T)$ by $f(U) = \{f(u) \mid u \in U\}$ and the **induced inverse map** by $f^{-1}(V) = \{s \in S \mid f(s) \in V\}$. (It is customary to denote the induced maps by the same notation as the original map.) Note that f is surjective if and only if its induced map is surjective, and this holds if and only if the induced inverse map is injective. A similar statement holds with the words surjective and injective reversed.

Theorem 0.2.13 Let ψ:G→G′ be a group homomorphism.

1) a) If $H < G$ then $\psi(H) < G'$.
   b) If ψ is surjective and $H \triangleleft G$ then $\psi(H) \triangleleft G'$.
2) a) If $H' < G'$ then $\psi^{-1}(H') < G$.
   b) If $H' \triangleleft G'$ then $\psi^{-1}(H') \triangleleft G$. □

Theorem 0.2.14 (The Isomorphism Theorems) Let G be a group.

1) (**First Isomorphism Theorem**) Let ψ:G→G′ be a group homomorphism with kernel K. Then $K \triangleleft G$ and the map $\overline{\psi}$:G/K→$im\,\psi$ defined by $\overline{\psi}(\alpha K) = \psi\alpha$ is an isomorphism. Hence $G/K \simeq im\,\psi$. In particular, ψ is injective if and only if $ker\,\psi = \{\epsilon\}$.
2) (**Second Isomorphism Theorem**) If $H < G$ and $N \triangleleft G$ then $N \cap H \triangleleft H$ and

$$\frac{H}{N \cap H} \simeq \frac{NH}{N}$$

3) **(Third Isomorphism Theorem)** If $H < I \lhd J < G$ then $I/H \lhd J/H$ and

$$\frac{J/H}{I/H} \simeq \frac{J}{I}$$

Hence $(J:I) = (J/H:I/H)$. □

Theorem 0.2.15 (The Correspondence Theorem) Let $H \lhd G$ and let π be the natural projection $\pi: G \to G/H$. Thus, for any $I < G$,

$$\pi(I) = I/H = \{iH \mid i \in I\}$$

1) The induced maps π and π^{-1} define a one-to-one correspondence between the lattice of subgroups of G containing H and the lattice of subgroups of G/H.
2) π preserves index, that is, for any $H < I < J < G$, we have

$$(J:I) = (\pi(J):\pi(I))$$

3) π preserves normality, that is, if $H < I < J < G$ then $I \lhd J$ if and only if $I/H \lhd J/H$, in which case $J/I \simeq \pi(J)/\pi(I)$. □

Action of a Group on a Set

Definition Let X be a set and let G be a group. We say that G **acts on** X if there is a function $G \times X \to X$, sending (α, x) to $\alpha x \in X$, satisfying

1) $1x = x$ for all $x \in X$
2) $(\alpha\beta)x = \alpha(\beta x)$ for all $x \in X$, $\alpha, \beta \in G$.

We say that G acts **transitively** on X if for any $x, y \in X$ there exists an $\alpha \in G$ such that $\alpha x = y$. □

It follows from the definition that each $\alpha \in G$ acts as a permutation $\pi_\alpha: x \mapsto \alpha x$ of X and that the map $\alpha \mapsto \pi_\alpha$ is a group homomorphism from G to a subgroup of the group of permutations of X.

Definition Let G act on X. The **orbit** of $x \in X$ is the set

$$orb(x) = Gx = \{\alpha x \mid \alpha \in G\}$$

The **stabilizer** of x is the subgroup

$$G_x = \{\alpha \in G \mid \alpha x = x\}$$ □

Note that G acts transitively on X if and only if $orb(x) = X$ for all $x \in X$. We may define an equivalence relation on X by setting $x \sim y$ if and only if there exists an $\alpha \in G$ for which $\alpha x = y$. The equivalence classes are precisely the orbits in X, which therefore partition the set X. Since $\alpha x = \beta x$ if and only if $\beta^{-1}\alpha \in G_x$, which in turn holds if and only if $\alpha G_x = \beta G_x$, we deduce the existence of a bijection from G/G_x onto $orb(x)$.

Theorem 0.2.16 Let G act on X.

1) For any $x \in X$, $|orb(x)| = (G:G_x)$ and if X is finite then $|orb(x)| = |G|/|G_x|$.
2) If G acts transitively on X then $|X| = (G:G_x)$ for any $x \in X$ and if X is finite then $|X| = |G|/|G_x|$.
3) **(The class equation)**

$$|X| = \sum (G:G_x)$$

where the sum is taken over one representative from each distinct orbit in X. □

Example 0.2.1 One of the most important instances of a group acting on a set is the case where $X = G$ acts on itself by conjugation. To avoid obvious confusion, we denote the action of $\alpha \in G$ on $\beta \in G$ by $\overline{\alpha}\beta$. Then $\overline{\alpha}\beta = \alpha\beta\alpha^{-1}$. The orbit of $\beta \in G$ is the **conjugacy class** of β

$$orb(\beta) = \{\alpha\beta\alpha^{-1} \mid \alpha \in G\}$$

The stabilizer of $\beta \in G$ is the **centralizer** of β

$$C(\beta) = \{\alpha \in G \mid \alpha\beta = \beta\alpha\}$$

The previous theorem says that the conjugacy class of β has cardinality $(G:C(\beta))$. The class equation in this case is

$$o(G) = \sum (G:C(\beta))$$

where the sum is over one representative of each conjugacy class.

The **center** of G is the set $Z(G) = \{\beta \in G \mid \alpha\beta = \beta\alpha \text{ for all } \alpha \in G\}$. Thus Z(G) consists of those elements of G whose centralizer is equal to the entire group G, or equivalently, whose conjugacy class contains only the element itself. In other words, $\beta \in Z(C)$ if and only if $(G:C(\beta)) = 1$. We may now write the class equation in the form

$$o(G) = o(Z(G)) + \sum (G:C(\beta))$$

where the sum is taken over one representative from each conjugacy class of size greater than 1. □

Sylow Subgroups

Definition If p is a prime, then a group G is called a **p-group** if every element of G has order a power of p. □

For finite groups, if $\alpha \in G$ then $o(\alpha) \mid o(G)$. The converse does not hold in general, but we do have the following.

Theorem 0.2.17 Let G be a finite group.

1) (**Cauchy**) If $o(G)$ is divisible by a prime p then G contains an element of order p.
2) If p is a prime and $o(G)$ is divisible by p^n then G contains a subgroup of order p^n. □

Corollary 0.2.18 A finite group G is a p-group if and only if $|G| = p^n$ for some n. □

Theorem 0.2.19 (Sylow) If G has order $p^n m$ where $p \not| m$ then G has a subgroup of order p^n, called a **Sylow p-subgroup** of G. All Sylow p-subgroups are conjugate (and hence isomorphic). The number of Sylow p-subgroups of G divides $o(G)$ and is congruent to 1 mod p. Any p-subgroup of G is contained is a Sylow p-subgroup of G. □

The Symmetric Group

Definition The **symmetric group** S_n is the group of all permutations of the set $A = \{1,2,\ldots,n\}$, under composition of maps. A **transposition** is a permutation that interchanges two distinct elements of A and leaves all other elements fixed. The **alternating group** A_n is the subgroup of S_n consisting of all *even* permutations, that is, all permutations that can be written as a product of an even number of transpositions. □

Theorem 0.2.20

1) The order of S_n is n!.
2) The order of A_n is n!/2. Thus, $[S_n:A_n] = 2$ and $A_n \triangleleft S_n$.
3) A_n is the only subgroup of S_n of index 2.
4) A_n is simple (no nontrivial normal subgroups) for $n \geq 5$. □

A subgroup H of S_n is **transitive** if for any $k, j \in \{1,2,\ldots,n\}$ there is a $\sigma \in H$ for which $\sigma k = j$.

Theorem 0.2.21 If H is a transitive subgroup of S_n then $o(H)$ is a multiple of n.

Proof. The group H acts on the set $X = \{1,2,\ldots,n\}$ and Theorem 0.2.16 gives $|X| = |H|/|G_x|$, that is, $|H| = n|G_x|$. ∎

0.3 Rings

Definition A **ring** is a nonempty set R, together with two binary operations on R, called *addition* (denoted by $+$), and *multiplication* (denoted by juxtaposition), satisfying the following properties.

1) R is an abelian group under the operation $+$.
2) (**Associativity**) $(\alpha\beta)\gamma = \alpha(\beta\gamma)$ for all $\alpha, \beta, \gamma \in R$.
3) (**Distributivity**) For all $\alpha, \beta, \gamma \in R$,

$$(\alpha+\beta)\gamma = \alpha\gamma + \alpha\beta \quad \text{and} \quad \gamma(\alpha+\beta) = \gamma\alpha + \gamma\beta \qquad \square$$

Definition Let R be a ring.

1) R is called a **ring with identity** if there exists an element $1 \in R$ for which $\alpha 1 = 1\alpha = \alpha$, for all $\alpha \in R$. In a ring R with identity, an element α is called a **unit** if it has a multiplicative inverse in R, that is, if there exists a $\beta \in R$ such that $\alpha\beta = \beta\alpha = 1$.
2) R is called a **commutative ring** if multiplication is commutative, that is, if $\alpha\beta = \beta\alpha$ for all $\alpha, \beta \in R$.
3) A **zero divisor** in a commutative ring R is a nonzero element $\alpha \in R$ such that $\alpha\beta = 0$ for some $\beta \neq 0$. A commutative ring R with identity is called an **integral domain** if R contains no zero divisors.
4) A ring R with identity $1 \neq 0$ is called a **field** if the nonzero elements of R form an abelian group under multiplication. □

It is not hard to see that the set of all units in a ring with identity forms a group under multiplication. We shall have occasion to use the following example.

Example 0.3.1 Let $\mathbb{Z}_n = \{0,\ldots,n-1\}$ be the ring of integers modulo n. Then k is a unit in $\mathbb{Z}_n$ if and only if $(k,n) = 1$. This follows from the fact that $(k,n) = 1$ if and only if there exists integers a and b such that $ak + bn = 1$, that is, if and only if $ak \equiv 1 \bmod n$. The set of units of $\mathbb{Z}_n$, denoted by $\mathbb{Z}_n^*$, is a group under multiplication. □

Definition A **subring** of a ring R is a nonempty subset S of R that is a ring in its own right, using the same operations as defined on R. □

Definition A **subfield** of a field E is a nonempty subset F of E that is a field in its own right, using the same operations as defined on E. In this case, we say that E is an **extension** of F and write $F < E$ or $E > F$. □

Definition Let R and S be rings. A function ψ:R→S is a **homomorphism** if, for all $\alpha, \beta \in R$,

$$\psi(\alpha + \beta) = \psi\alpha + \psi\beta \quad \text{and} \quad \psi(\alpha\beta) = (\psi\alpha)(\psi\beta)$$

An injective homomorphism is a **monomorphism** or an **embedding**, a surjective homomorphism is an **epimorphism** and a bijective homomorphism is an **isomorphism**. A homomorphism from R into itself is an **endomorphism** and an isomorphism from R onto itself is an **automorphism**. □

Ideals

Definition A nonempty subset $\mathfrak{I}$ of a ring R is called an **ideal** if it satisfies

1) $\alpha, \beta \in \mathfrak{I}$ implies $\alpha - \beta \in \mathfrak{I}$.
2) $\alpha \in R$, $\iota \in \mathfrak{I}$ implies $\alpha\iota \in \mathfrak{I}$ and $\iota\alpha \in \mathfrak{I}$. □

If S is a nonempty subset of a ring R, then the **ideal generated** by S is defined to be the smallest ideal $\mathfrak{I}$ of R containing S. If R is a commutative ring with identity, and if $\alpha \in R$, then the ideal generated by $\{\alpha\}$ is the set

$$\langle\alpha\rangle = R\alpha = \{\rho\alpha \mid \rho \in R\}$$

Any ideal of the form $\langle\alpha\rangle$ is called a **principal ideal**.

Definition If ψ:R→S is a homomorphism, then

$$Ker\psi = \{\alpha \in R \mid \psi\alpha = 0\}$$

is an ideal of R. □

If R is a ring and $\mathfrak{I}$ is an ideal in R then for each $\alpha \in R$, we can form the **coset**

$$\alpha + \mathfrak{I} = \{\alpha + \iota \mid \iota \in \mathfrak{I}\}$$

It is easy to see that $\alpha + \mathfrak{I} = \beta + \mathfrak{I}$ if and only if $\alpha - \beta \in \mathfrak{I}$, and that any two cosets $\alpha + \mathfrak{I}$ and $\beta + \mathfrak{I}$ are either disjoint or identical. The collection of all (distinct) cosets is a ring itself, with addition and multiplication defined by

$$(a + \mathfrak{I}) + (b + \mathfrak{I}) = (a + b) + \mathfrak{I}$$

and

$$(a + \mathfrak{I})(b + \mathfrak{I}) = ab + \mathfrak{I}$$

The ring of cosets of $\mathfrak{I}$ is called a **factor ring** and is denoted by $R/\mathfrak{I}$.

Definition An ideal $\mathfrak{I}$ of a ring R is **maximal** if $\mathfrak{I} \neq R$ and if whenever $\mathfrak{I} \subseteq \mathfrak{J} \subseteq R$ for any ideal $\mathfrak{J}$, then $\mathfrak{J} = \mathfrak{I}$ or $\mathfrak{J} = R$. An ideal $\mathfrak{I}$ is **prime** if $\mathfrak{I} \neq R$ and if $\alpha\beta \in \mathfrak{I}$ implies $\alpha \in \mathfrak{I}$ or $\beta \in \mathfrak{I}$. □

It is not hard to see that a maximal ideal in a commutative ring with identity is prime. This also follows from the next theorem.

Theorem 0.3.1 Let R be a commutative ring with identity and let $\mathfrak{I}$ be an ideal of R.

1) $R/\mathfrak{I}$ is a field if and only if $\mathfrak{I}$ is maximal.
2) $R/\mathfrak{I}$ is an integral domain if and only if $\mathfrak{I}$ is prime. □

The Characteristic of a Ring

Let R be a ring and let $r \in R$. For any positive integer n, we define

$$nr = \underbrace{r + r + \cdots + r}_{n \text{ terms}}$$

The **characteristic** char(R) of a ring R is the smallest positive integer n for which $n1 = 0$ (or equivalently, $nr = 0$ for all $r \in R$), should such an integer exist. If it does not, we say that R has characteristic 0. If $\text{char}(R) = 0$ then R contains a copy of the integers $\mathbb{Z}$, in the form $\mathbb{Z} \cdot 1 = \{n1 \mid n \in \mathbb{Z}\}$. If $\text{char}(R) = r$, then R contains a copy of $\mathbb{Z}_r = \{0,1,\ldots,r-1\}$.

Theorem 0.3.2 The characteristic of an integral domain is either 0 or a prime. In particular, a finite field has prime characteristic. □

If F is a field, the intersection of all of its subfields is the smallest subfield of F and is referred to as the **prime subfield** of F.

Theorem 0.3.3 If $\mathrm{char}(F) = 0$, the prime subfield of F is isomorphic to the rational numbers $\mathbf{Q}$. If $\mathrm{char}(F) = p$ is prime, the prime field of F is isomorphic to $\mathbb{Z}_p$. □

The following result is of considerable importance for the study of fields of nonzero characteristic.

Theorem 0.3.4 Let R be a commutative ring with identity of *prime* characteristic p. If $q = p^n$ then

$$(\alpha + \beta)^q = \alpha^q + \beta^q, \qquad (\alpha - \beta)^q = \alpha^q - \beta^q$$

Proof. Since the binomial formula holds in any commutative ring with identity, we have

$$(\alpha + \beta)^p = \sum_{k=0}^{p} \binom{p}{k} \alpha^k \beta^{p-k}$$

where

$$\binom{p}{k} = \frac{p(p-1)\cdots(p-k+1)}{k!}$$

But $p \left| \binom{p}{k} \right.$ for $0 < k < p$, and so $\binom{p}{k} = 0$ in R. The binomial formula therefore reduces to

$$(\alpha + \beta)^p = \alpha^p + \beta^p$$

Repeated use of this formula gives $(\alpha + \beta)^q = \alpha^q + \beta^q$. The second formula is proved similarly. ∎

0.4 Integral Domains

Theorem 0.4.1 Let R be an integral domain. Let $\alpha, \beta \in R$.

1) We say that α **divides** β and write $\alpha \mid \beta$ if $\beta = \rho\alpha$ for some $\rho \in R$. If ρ and α are nonunits and $\beta = \rho\alpha$ then α **properly divides** β.
   a) A unit divides every element of R.
   b) $\alpha \mid \beta$ if and only if $\langle\beta\rangle \subseteq \langle\alpha\rangle$.
   c) $\alpha \mid \beta$ properly if and only if $\langle\beta\rangle \subset \langle\alpha\rangle \subset R$.
2) If $\alpha = u\beta$ for some unit u then α and β are **associates** and we write $\alpha \sim \beta$.
   a) $\alpha \sim \beta$ if and only if $\alpha \mid \beta$ and $\beta \mid \alpha$.
   b) $\alpha \sim \beta$ if and only if $\langle\alpha\rangle = \langle\beta\rangle$.
3) A nonzero element $\rho \in R$ is **irreducible** if ρ is not a unit and if ρ has no proper divisors. Thus, a nonunit ρ is irreducible if and only

if $\rho = \alpha\beta$ implies either α or β is a unit.

4) A nonzero element $\pi \in R$ is **prime** if π is not a unit and whenever $\pi \mid \alpha\beta$ then $\pi \mid \alpha$ or $\pi \mid \beta$.
   a) Every prime element is irreducible.
   b) $\pi \in R$ is prime if and only if $\langle\pi\rangle$ is a nonzero prime ideal.

5) Let α, $\beta \in R$. An element $d \in R$ is called a **greatest common divisor** (**gcd**) of α and β, written (α,β) or $\gcd(\alpha,\beta)$, if $d \mid \alpha$ and $d \mid \beta$ and if whenever $e \mid \alpha$, $e \mid \beta$ then $e \mid d$. If $\gcd(\alpha,\beta)$ is a unit, we say that α and β are **relatively prime.**
   a) The greatest common divisor of two elements, if it exists, is unique up to associate. □

Theorem 0.4.2 An integral domain R is a field if and only if it has no ideals other than the zero ideal or R itself. Any nonzero homomorphism $\sigma: F \to E$ of fields is a monomorphism. □

Theorem 0.4.3 Every finite integral domain is a field. □

If R is an integral domain, we may form the set

$$R' = \{\alpha/\beta \mid \alpha, \beta \in R, \beta \neq 0\}$$

where $\alpha/\beta = a/b$ if and only if $\alpha b = a\beta$. We define addition and multiplication on R′ in the "obvious way"

$$\frac{\alpha}{\beta} + \frac{a}{b} = \frac{\alpha b + \beta a}{\beta b}, \qquad \frac{\alpha}{\beta} \cdot \frac{a}{b} = \frac{\alpha a}{\beta b}$$

It is easy to see that these operations are well-defined and that R′ is actually a field, called the **field of quotients** of the integral domain R. It is the *smallest* field containing R, in the sense that if F is a field and $R \subseteq F$ then $R \subseteq R' \subseteq F$. The following fact will prove useful.

Theorem 0.4.4 Let R be an integral domain with field of quotients R′. Then any monomorphism $\sigma: R \to F$ from R into a field F has a unique extension to a monomorphism $\overline{\sigma}: R' \to F$.

Proof. Define $\overline{\sigma}(\alpha/\beta) = \sigma\alpha/\sigma\beta$, which makes sense since $\beta \neq 0$ implies $\sigma\beta \neq 0$. One can easily show that $\overline{\sigma}$ is well-defined. Since $\sigma\alpha/\sigma\beta = 0$ if and only if $\sigma\alpha = 0$, which in turn holds if and only if $\alpha/\beta = 0$, we see that $\overline{\sigma}$ is injective. Uniqueness is clear since $\sigma \mid_R$ (σ restricted to R) uniquely determines σ on R′. ∎

0.5 Unique Factorization Domains

Definition An integral domain R is a **unique factorization domain (ufd)** if

1) Any nonunit $r \in R$ can be written as a product $r = p_1 \cdots p_n$ where p_i is irreducible for all i. We refer to this as the **factorization property** for R.
2) This factorization is **essentially unique** in the sense that if $r = p_1 \cdots p_n = q_1 \cdots q_m$ are two factorizations into irreducible elements then $m = n$ and there is some permutation π for which $p_i \sim q_{\pi(i)}$ for all i. □

If $r \in R$ is not irreducible, then $r = st$ where s and t are nonunits. Evidently, we may continue to factor as long as at least one factor is not irreducible. An integral domain R has the factorization property precisely when this factoring process always stops after a finite number of steps.

When is an integral domain a unique factorization domain? The following answer helps explain the importance of ufd's.

Theorem 0.5.1 Let R be an integral domain for which the factorization property holds. The following conditions are equivalent and therefore imply that R is a unique factorization domain.

1) Factorization in R is essentially unique.
2) Every irreducible element of R is prime.
3) Any two elements of R (not both zero) have a greatest common divisor. □

Corollary 0.5.2 In a unique factorization domain, the concepts of prime and irreducible are equivalent. □

0.6 Principal Ideal Domains

Definition An integral domain R is called a **principal ideal domain (pid)** if every ideal of R is principal. □

Theorem 0.6.1 Every principal ideal domain is a unique factorization domain. □

We remark that the ring $\mathbb{Z}[x]$ is a ufd (as we prove in Chapter 1) but not a pid (the ideal $\langle 2,x \rangle$ is not principal) and so the converse of the previous theorem is not true.

Theorem 0.6.2 Let R be a principal ideal domain and let $\mathfrak{J}$ be an ideal of R.

1) $\mathfrak{J}$ is maximal if and only if $\mathfrak{J} = \langle \rho \rangle$ where ρ is irreducible.
2) $\mathfrak{J}$ is prime if and only if $\mathfrak{J} = \{0\}$ or $\mathfrak{J}$ is maximal.
3) The following are equivalent: (i) $R/\langle \rho \rangle$ is a field (ii) $R/\langle \rho \rangle$ is an integral domain (iii) ρ is irreducible (iv) ρ is prime. □

0.7 Euclidean Domains

Roughly speaking, a Euclidean domain is an integral domain in which we can perform "division with remainder."

Definition An integral domain R is a **Euclidean domain** if there is a function $\sigma:(R-\{0\}) \to \mathbb{N}$ with the property that given any α, $\beta \in R$, $\beta \neq 0$, there exist $q, r \in R$ satisfying

$$\alpha = q\beta + r$$

where $r = 0$ or $\sigma r < \sigma \beta$. □

Theorem 0.7.1 A Euclidean domain is a principal ideal domain (and hence also a unique factorization domain).

Proof. Let $\mathfrak{J}$ be an ideal in the Euclidean domain R and let $\alpha \in \mathfrak{J}$ be minimal with respect to the value of σ. Thus, $\sigma\alpha \leq \sigma\beta$ for all $\beta \in \mathfrak{J}$. If $s \in \mathfrak{J}$ then

$$s = r\alpha + q$$

where $q = 0$ or $\sigma q < \sigma r$. But $q = s - r\alpha \in \mathfrak{J}$ and so the latter is not possible, leaving $q = 0$ and $s \in \langle \alpha \rangle$. Hence, $\mathfrak{J} = \langle \alpha \rangle$. ∎

Theorem 0.7.2 If F is a field, then F[x] is a Euclidean domain with $\sigma(p(x)) = \textit{deg}\ p(x)$. Hence F[x] is also a principal ideal domain and a unique factorization domain.

Proof. This follows from ordinary division of polynomials; to wit, if $f(x), g(x) \in F[x]$, $g(x) \neq 0$, then there exist $q(x), r(x) \in F[x]$ such that

$$f(x) = q(x)g(x) + r(x)$$

where $\textit{deg}\ r(x) < \textit{deg}\ g(x)$. ∎

0.8 Tensor Products

Tensor products are used only in the optional Section 5.6.

Definition Let U, V and W be vector spaces over a field F. A function $f:U \times V \to W$ is **bilinear** if it is linear in both variables separately, that is, if

$$f(ru + su',v) = rf(u,v) + sf(u',v)$$

and

$$f(u,rv + sv') = rf(u,v) + sf(u,v')$$

The set of all bilinear functions from $U \times V$ to W is denoted by $\mathfrak{B}(U,V;W)$. A bilinear function $f:U \times V \to F$, with values in the base field F, is called a **bilinear form** on $U \times V$. □

Example 0.8.1

1) A *real* inner product $\langle,\rangle:V \times V \to \mathbb{R}$ is a bilinear form on $V \times V$.
2) If A is an algebra, the product map $\mu:A \times A \to A$ defined by $\mu(a,b) = ab$ is bilinear. □

We will denote the set of all linear transformations from $U \times V$ to W by $\mathfrak{L}(U \times V,W)$. There are many definitions of the tensor product. We choose a universal definition.

Theorem 0.8.1 Let U and V be vector spaces over the same field F. There exists a unique vector space $U \otimes V$ and bilinear map $t:U \times V \to U \otimes V$ with the following property. If $f:U \times V \to W$ is any bilinear function from $U \times V$ to a vector space W over F, then there is a unique *linear* transformation $\tau:U \otimes V \to W$ for which

$$\tau \circ t = f \qquad \square$$

This theorem says that to each *bilinear* function $f:U \times V \to W$, there corresponds a unique *linear* function $\tau:U \otimes V \to W$, through which f can be factored (that is, $f = \tau \circ t$). The vector space $U \otimes V$, whose existence is guaranteed by the previous theorem, is called the **tensor product** of U and V over F. We denote the image of (u,v) under the map t by $t(u,v) = u \otimes v$.

If $X = Im\ t = \{u \otimes v \mid u \in U,\ v \in V\}$ is the image of the tensor map t then the uniqueness statement in the theorem implies that X spans $U \otimes V$. Hence, every element of $\alpha \in U \otimes V$ is a finite sum of elements of the form $u \otimes v$

$$\alpha = \sum_{\text{finite}} a_i(u_i \otimes v_i)$$

We establish a few basic properties of the tensor product.

Theorem 0.8.2 If $\{u_1,\ldots,u_n\} \subseteq U$ is linearly independent and $\{v_1,\ldots,v_n\} \subseteq V$ then

$$\sum u_i \otimes v_i = 0 \Rightarrow v_i = 0 \text{ for all } i$$

Proof. Consider the dual vectors $\delta_i \in U^*$ to the vectors u_i, where $\delta_i u_j = \delta_{i,j}$. For linear functionals $\epsilon_i: V \to F$, we define a bilinear form $f: U \times V \to F$ by

$$f(u,v) = \sum_{j=1}^{n} \delta_j(x)\epsilon_j(y)$$

Since there exists a unique linear functional $\tau: U \otimes V \to F$ for which $\tau \circ t = f$, we have

$$0 = \tau\Big(\sum_i u_i \otimes v_i\Big) = \sum_i \tau \circ t(u_i,v_i)$$
$$= \sum_i f(u_i,v_i) = \sum_i \sum_j \delta_j(u_i)\epsilon_j(v_i) = \sum_i \epsilon_i(v_i)$$

Since the ϵ_i's are arbitrary, we deduce that $v_i = 0$ for all i. ∎

Corollary 0.8.3 If $u \neq 0$ and $v \neq 0$, then $u \otimes v \neq 0$. □

Theorem 0.8.4 Let $\mathfrak{B} = \{e_i \mid i \in I\}$ be a basis for U and $\mathfrak{C} = \{f_j \mid j \in J\}$ be a basis for V. Then the set $\mathfrak{D} = \{e_i \otimes f_j \mid i \in I, j \in J\}$ is a basis for $U \otimes V$.

Proof. To see that the $\mathfrak{D}$ is linearly independent, suppose that

$$\sum_{i,j} r_{i,j}(e_i \otimes f_j) = 0$$

This can be written

$$\sum_i e_i \otimes \Big(\sum_j r_{i,j} f_j\Big) = 0$$

Theorem 0.8.2 implies that

$$\sum_j r_{i,j} f_j = 0$$

for all i, and hence $r_{i,j} = 0$ for all i and j. To see that $\mathfrak{D}$ spans $U \otimes V$, let $u \otimes v \in U \otimes V$. Since $u = \sum_i r_i e_i$, and $v = \sum_j s_j f_j$, we have

$$u \otimes v = \sum_i r_i e_i \otimes \sum_j s_j f_j = \sum_j s_j \Big(\sum_i r_i e_i \otimes f_j\Big)$$

$$= \sum_j s_j\Big(\sum_i r_i(e_i \otimes f_j)\Big) = \sum_{i,j} r_i s_j (e_i \otimes f_j)$$

Since any vector in $U \otimes V$ is a finite sum of vectors $u \otimes v$, we deduce that $\mathfrak{D}$ spans $U \otimes V$. ∎

Corollary 0.8.5 For finite dimensional vector spaces,

$$dim(U \otimes V) = dim(U) \cdot dim(V)$$ □

Exercises

1. The relation of being associates in an integral domain is an equivalence relation.
2. Prove that the characteristic of an integral domain is either 0 or a prime, and that a finite field has prime characteristic.
3. If $char(F) = 0$, the prime subfield of F is isomorphic to the rational numbers $\mathbb{Q}$. If $char(F) = p$ is prime, the prime field of F is isomorphic to $\mathbb{Z}_p$.
4. If $F < E$ show that E and F must have the same characteristic.
5. Let F be a field of characteristic p. The map $\sigma: F \to F$ defined by $\sigma\alpha = \alpha^p$ is a homomorphism. It is called the **Frobenius map**. Show that $F \approx F^p = \{a^p \mid a \in F\}$. What if F is a finite field?
6. Consider the polynomial ring $F[x_1, x_2, \ldots]$ where $x_i^2 = x_{i-1}$. Show that the factorization process need not stop in this ring.
7. Let $R = \mathbb{Z}[\sqrt{-5}] = \{a + b\sqrt{-5} \mid a,b \in \mathbb{Z}\}$. Show that this integral domain is not a unique factorization domain by showing that $6 \in R$ has essentially two different factorizations in R. Show also that the irreducible element 2 is not prime.
8. Let R be a pid. Then an ideal $\mathfrak{I}$ of R is maximal if and only if $\mathfrak{I} = \langle p \rangle$ where p is irreducible. Also, $R/\langle p \rangle$ is a field if and only if p is irreducible.
9. Prove that $\langle x \rangle$ and $\langle 2,x \rangle$ are both prime ideals in $\mathbb{Z}[x]$ and that $\langle x \rangle$ is properly contained in $\langle 2,x \rangle$.
10. Describe the divisor chain condition in terms of principal ideals.

Part 1
Basic Theory

Chapter 1

Polynomials

In this chapter, we discuss properties of polynomials that will be needed in the sequel. Since we assume that the reader is familiar with the basic properties of polynomials, some of the present material may constitute a review.

1.1 Polynomials Over a Ring

We will be concerned in this book mainly with polynomials over a field F, but it is useful to make a few remarks about polynomials over a ring R as well. Let R[x] denote the ring of polynomials in the single variable x over R. If

$$p(x) = a_0 + a_1x + \cdots + a_nx^n$$

where $a_i \in R$ and $a_n \neq 0$ then n is called the **degree** of p(x), written *deg* p(x) and a_n is called the **leading coefficient** of p(x). A polynomial is **monic** if its leading coefficient is 1. The degree of the zero polynomial is defined to be $-\infty$.

If R is a ring, the units of R[x] are the units of R, since no polynomial of positive degree can have an inverse in R[x].

Definition Let R be a ring. A polynomial $p(x) \in R[x]$ is **irreducible** over R if whenever $p(x) = f(x)g(x)$ for $f(x), g(x) \in R[x]$, then one of f(x) or g(x) is a unit in R[x]. A polynomial that is not irreducible is said to be **reducible.** □

Many important properties that a ring R may possess carry over to the ring of polynomials R[x]. For instance, if R is an integral domain, then so is R[x] and if R is a unique factorization domain, then so is R[x]. Note, however, that the ring $\mathbb{Z}$ of integers is a principal ideal domain, but $\mathbb{Z}[x]$ is not, since the ideal $\langle 2,x \rangle$ is not principal. Nonetheless, if F is a field, F[x] is a principal ideal domain (Theorem 0.7.2).

1.2 Primitive Polynomials

We now consider polynomials over a unique factorization domain. The reader may wish to take a quick look at Section 0.5.

Definition Let $f(x) \in R[x]$ where R is a unique factorization domain. Any greatest common divisor of the coefficients of f(x) is called a **content** of f(x). A polynomial with content 1 is said to be **primitive**. We will use the notation $c(f)$ to denote a content of f(x). □

If α is a content of f(x), then β is also a content of f(x) if and only if $\beta \sim \alpha$, that is, $\beta = u\alpha$, where u is a unit in R. Since

$$c(\alpha p(x)) \sim \alpha c(p(x))$$

for all $\alpha \in R$, it follows that α is a content of f(x) if and only if $f(x) = \alpha p(x)$, where p(x) is primitive.

We can also define the content of a polynomial over R′, the field of quotients of R. To this end, if p is a prime in R, then any nonzero element $a \in R'$ has the form

$$a = p^r a_0$$

where r is an integer and p does not divide the numerator or denominator of a_0. The integer r is called the **order** of a at p, written $o_p(a)$. If $a = 0$, we set $o_p(a) = \infty$. It is easy to see that if $ab \neq 0$ then

$$o_p(ab) = o_p(a) + o_p(b)$$

If $f(x) = \sum a_i x^i$ is a nonzero polynomial in R′[x], we set

$$o_p(f) = \min_i o_p(a_i)$$

and if $f(x) = 0$, we set $o_p(f) = \infty$. Then a **content** of f(x) is defined to be

$$c(f) = u \prod p^{o_p(f)}$$

where u is any unit in R and the product is taken over all primes p for which $o_p(f) \neq 0$. Thus, content in R′ is unique up to multiplication by a unit in R.

For any $\alpha \in R'$, we have $c(\alpha p(x)) = u\alpha c(p(x))$ where u is a unit in R and so α is a content of $f(x) \in R'[x]$ if and only if

$$f(x) = \alpha p(x)$$

where p(x) is a primitive polynomial (and hence in R[x]). It follows that $f(x) \in R[x]$ if and only if its content is in R.

We now come to a key result concerning primitive polynomials.

Theorem 1.2.1 Let R be a unique factorization domain and let R′ be the field of quotients of R.

1) **(Gauss' Lemma)** If f(x) and g(x) are primitive in R[x] then so is f(x)g(x).
2) If $f(x), g(x) \in R'[x]$ then $c(fg) = uc(f)c(g)$, where u is a unit in R.
3) Let $f(x), g(x) \in R[x]$, with g(x) primitive. If $f(x) = g(x)h(x)$, where $h(x) \in R'(x)$ then, in fact, $h(x) \in R[x]$.

Proof. To prove Gauss' Lemma, suppose that fg is not primitive. Then there exists an irreducible element $r \in R$ for which $r \mid fg$. Since R is a unique factorization domain, r is also prime. Hence $\langle r \rangle$ is a prime ideal and $R[x]/\langle r \rangle$ is an integral domain. Since $r \mid fg$, we have $fg \in \langle r \rangle$ and so

$$(f + \langle r \rangle)(g + \langle r \rangle) = fg + \langle r \rangle = \langle r \rangle$$

whence $f + \langle r \rangle = \langle r \rangle$ or $g + \langle r \rangle = \langle r \rangle$, that is, $r \mid f$ or $r \mid g$. Hence, one of f or g is not primitive.

To prove part 2), observe that if c_f is a content of f(x) and c_g is a content of g(x) then $f = c_f f'$ and $g = c_g g'$, where f′ and g′ are primitive. Hence, by Gauss' Lemma

$$c(fg) = c(c_f c_g f'g') \sim c_f c_g c(f'g') = c_f c_g$$

As to part 3), we have

$$c(f) \sim c(g)c(h) \sim c(h)$$

and since $c(f) \in R$, so is c(h), whence $h(x) \in R[x]$. ∎

The previous theorem can be used to relate the irreducibility of a polynomial over a unique factorization domain R to its irreducibility over the field of quotients R′ of R. The next theorem says in loose

terms that the only difference between irreducibility over R and over R′ is how constant factors are treated.

Theorem 1.2.2 Let R be a unique factorization domain, with field of quotients R′.

1) A primitive polynomial $p(x) \in R[x]$ is irreducible over R if and only if it is irreducible over R′.
2) A polynomial $f(x) \in R[x]$ is irreducible over R if and only if it is either an irreducible element of R or a primitive polynomial that is also irreducible over R′.

Proof. To prove part 1), observe that a primitive polynomial p(x) has no constant nonunit factors and so p(x) is irreducible over R if and only if it can be written as a product of nonconstant factors over R. Hence, if p(x) is reducible over R, it is also reducible over R′. On the other hand, if p(x) is reducible over R′, then it has the form $p(x) = f(x)g(x)$, where f(x) and g(x) are nonconstant polynomials in R′[x]. Now we may write

$$p(x) = f'(x)[c(f)g(x)]$$

where f′(x) is primitive and hence, by Theorem 1.2.1, $c(f)g(x)$ is a polynomial over R. Thus f(x) is reducible over R as well.

To prove part 2), note that if f(x) is a constant, then there is nothing to prove, since the constant nonunits in R[x] are precisely the nonunits in R. On the other hand, if f(x) has positive degree, then it is irreducible over R if and only if it is both primitive and irreducible over R and this is equivalent, by part 1), to being primitive and irreducible over R′. ∎

1.3 The Division Algorithm

The familiar division algorithm for polynomials over a field F can be easily extended to polynomials over a commutative ring with identity, provided that we divide only by polynomials whose leading coefficient is a unit. We leave proof of the following to the reader.

Theorem 1.3.1 (Division algorithm) Let R be a commutative ring with identity. Let $g(x) \in R[x]$ have invertible leading coefficient. Then for any $f(x) \in R[x]$, there exist unique $q(x), r(x) \in R[x]$ such that

$$f(x) = q(x)g(x) + r(x)$$

where $deg\ r(x) < deg\ g(x)$. □

This theorem has some very important immediate consequences.

Corollary 1.3.2 Let R be a commutative ring with identity and let $f(x) \in R[x]$. Then α is a root of $f(x)$ if and only if $x - \alpha$ is a factor of $f(x)$ over R. □

Since the usual degree formula $deg\ f(x)g(x) = deg\ f(x) + deg\ g(x)$ holds when R is an integral domain, we have the following.

Corollary 1.3.3 If R is an integral domain then a nonzero polynomial $f(x) \in R[x]$ can have at most $deg\ f(x)$ roots in R. □

In the customary way, a polynomial $p(x) \in R[x]$ can be thought of as a function on R. If R is an integral domain, Corollary 1.3.3 insures that if $p(r) = 0$ for an infinite number of distinct values of $r \in R$ then $p(x)$ must be the zero polynomial. Thus, if R is *infinite*, then $p(x)$ is zero as a function if and only if it is zero as a polynomial. Note that this does not hold for finite fields, for instance, the nonzero polynomial $p(x) = x^2 - x$ is the zero function on $\mathbb{Z}_2$. This result can be extended to polynomials in more than one variable by induction and we leave the details to the reader.

A polynomial in more than one variable may have infinitely many zeros, however, and yet not be the zero polynomial. For instance $p(x,y) = x - y$ has infinitely many zeros over $\mathbb{R}$. This example notwithstanding, we do have the following useful result, which says informally that if a polynomial has a whole subfield worth of zeros, then it must be the zero polynomial.

Theorem 1.3.4 Let F be an infinite field and let L be an extension of F. Suppose that $q(x_1,\ldots,x_n)$ is a polynomial over L. If $q(a_1,\ldots,a_n) = 0$ for all $a_i \in F$ then $q(x_1,\ldots,x_n)$ is the zero polynomial.

Proof. Write

$$q(x_1,\ldots,x_n) = \sum_e \lambda_e \mathbf{x}^e$$

where $\mathbf{x}^e = x_1^{e_1}\cdots x_n^{e_n}$ and $\lambda_e \in L$. Let $\{\beta_i\}$ be a basis for L as a vector space over F. Then

$$\lambda_e = \sum_i a_{e,i}\beta_i$$

for $a_{e,i} \in F$ and so

$$q(x_1,\ldots,x_n) = \sum_e \lambda_e \mathbf{x}^e = \sum_e \sum_i a_{e,i}\beta_i \mathbf{x}^e = \sum_i \beta_i \Big(\sum_e a_{e,i}\mathbf{x}^e \Big)$$

If $b_i \in F$, we have

$$0 = q(b_1,\ldots,b_n) = \sum_i \beta_i\Big(\sum_e a_{e,i}b^e\Big)$$

and the independence of the β_i's implies that

$$\sum_e a_{e,i}b^e = 0$$

for all i. Since this holds for all $b_i \in F$, the polynomial $\sum a_{e,i}x^e$ over F must be the zero polynomial. It follows that $a_{e,i} = 0$ for all e and i, and so $\lambda_e = 0$ for all e, whence $q(x_1,\ldots,x_n) = 0$. ∎

Corollary 1.3.3 can be used to prove a fundamental fact concerning finite fields.

Corollary 1.3.5 Let F be a finite field. The multiplicative group F^* of all nonzero elements of F is cyclic.

Proof. Let $|F^*| = q-1$ and let α have maximum order $m \leq q-1$ among all the elements in F^*. Since F^* is a finite abelian group, Theorem 0.2.2 implies that $\alpha^m = 1$ for all $\alpha \in F^*$. Thus, every element of F^* is a root of the polynomial $x^m - 1$, which has at most m roots. Hence $m = q-1$, and F^* is cyclic. ∎

In defining the greatest common divisor of two polynomials, it is customary (in order to obtain uniqueness) to require that it be monic.

Definition Let f(x) and g(x) be polynomials over F. The **greatest common divisor** of f(x) and g(x), denoted by (f(x),g(x)) or gcd(f(x),g(x)), is the unique monic polynomial p(x) over F for which

1) $p(x) \mid f(x)$ and $p(x) \mid g(x)$.
2) If $r(x) \in F[x]$ and $r(x) \mid f(x)$ and $r(x) \mid g(x)$ then $r(x) \mid p(x)$. □

The existence of greatest common divisors and the fact that d(x) = gcd(f(x),g(x)) is independent of the field F, that is, d(x) lies in any field K containing the coefficients of f(x) and g(x), follow from the fact that F[x] is a principal ideal domain. In particular, the ideal $I = \langle f(x),g(x)\rangle$ of K[x] is principal and so $I = \langle p(x)\rangle$ where $p(x) \in K[x]$. Since $f(x) \in \langle p(x)\rangle$, we have $p(x) \mid f(x)$ and similarly $p(x) \mid g(x)$ over K and hence over any larger field F. Since $p(x) \in \langle f(x),g(x)\rangle$, there exist a(x), $b(x) \in K[x]$ such that $p(x) = a(x)f(x) + b(x)g(x)$. Hence, if $q(x) \mid f(x)$ and $q(x) \mid g(x)$ over F then $q(x) \mid p(x)$ over F. Thus, p(x) = gcd(f(x),g(x)).

Theorem 1.3.6 Let $f(x), g(x) \in F[x]$ and let K be the smallest subfield of F containing the coefficients of f(x) and g(x). Then there exist a(x), $b(x) \in K[x]$ such that $\gcd(f(x),g(x)) = a(x)f(x) + b(x)g(x) \in K[x]$. □

Theorem 1.3.7 Let $f(x)$, $g(x) \in F[x]$ and let $F < E$. Then $f(x)$ and $g(x)$ have a nonconstant common factor over F if and only if they have a nonconstant common factor over E.

Proof. Any common divisor $h(x)$ of $f(x)$ and $g(x)$ over E is also a divisor of $a(x)f(x) + b(x)g(x) = \gcd(f(x),g(x))$. Hence, if $h(x)$ is nonconstant, so is $\gcd(f(x),g(x))$. ∎

Definition The polynomials $f(x)$, $g(x) \in F[x]$ are **relatively prime** if $\gcd(f(x),g(x)) = 1$. In particular, $f(x)$ and $g(x)$ are relatively prime if and only if there exist polynomials $a(x)$, $b(x) \in F[x]$ for which

$$a(x)f(x) + b(x)g(x) = 1 \qquad \square$$

Corollary 1.3.8 The polynomials $f(x)$, $g(x) \in F[x]$ are relatively prime if and only if they have no common roots in any extension field E of F.

Proof. If $\gcd(f(x),g(x)) = 1$ then $a(x)f(x) + b(x)g(x) = 1$ implies that $f(x)$ and $g(x)$ have no common roots in any extension. Conversely, if $\gcd(f(x),g(x))$ is nonconstant, any of its roots is a common root of $f(x)$ and $g(x)$ in some extension. ∎

Corollary 1.3.9 If $f(x)$ and $g(x)$ are distinct monic irreducible polynomials over F then they have no common roots in any extension E of F. □

1.4 Splitting Fields

It is a fundamental fact that every nonconstant polynomial $f(x) \in F[x]$ has a root in some field.

Theorem 1.4.1 Let F be a field, and let $f(x) \in F[x]$ be a nonconstant polynomial. Then there exists an extension E of F and an $\alpha \in E$ such that $f(\alpha) = 0$.

Proof. We may assume that $f(x)$ is irreducible. Consider the field $E = F[x]/\langle f(x)\rangle$. The field F may be thought of as a subfield of E, by identifying $\alpha \in F$ with $\alpha + \langle f(x)\rangle \in E$. Then $x + \langle f(x)\rangle$ is a root of $f(x)$ in E. (We have actually shown that F can be *embedded* in a field in which $f(x)$ has a root, but this is sufficient in view of Exercise 17 of Chapter 2.) ∎

Repeated application of Theorem 1.4.1 gives the following corollary.

Corollary 1.4.2 Let $f(x) \in F[x]$. There exists an extension E of F such that f(x) factors into linear factors over E. □

If a polynomial $f(x) \in F[x]$ factors into linear factors

$$f(x) = a(x - \alpha_1)(x - \alpha_2)\cdots(x - \alpha_n)$$

over an extension field E (that is, if $a, \alpha_1, \ldots, \alpha_n \in E$), we say that f(x) **splits** in E.

Definition Let $\mathfrak{F} = \{f_i(x)\}$ be family of polynomials over a field F. A **splitting field** for $\mathfrak{F}$ is an extension field E of F with the property that each $f_i(x)$ in $\mathfrak{F}$ splits in E and that E is generated over F by the roots of the polynomials in $\mathfrak{F}$. □

Corollary 1.4.3 Every finite family of polynomials over a field F has a splitting field.

Proof. Corollary 1.4.2 implies that any single polynomial has a splitting field. If $\mathfrak{F}$ is a finite family of polynomials, then a splitting field for $\mathfrak{F}$ is a splitting field for the product of the polynomials in $\mathfrak{F}$. ∎

We will see in the next chapter that any family of polynomials has a splitting field. We will also see that any two splitting fields S_1 and S_2 for a family of polynomials over F are isomorphic by an isomorphism that fixes each element of the base field F.

1.5 The Minimal Polynomial

Let $F < E$. An element $\alpha \in E$ is said to be **algebraic** over F if there is some nonzero polynomial $f(x) \in F[x]$ for which $f(\alpha) = 0$. An element that is not algebraic over F is said to be **transcendental** over F.

If α is algebraic over F, the set

$$\mathfrak{I} = \{g(x) \in F[x] \mid g(\alpha) = 0\}$$

is a nonzero ideal in F[x] and is therefore generated by a unique *monic* polynomial p(x), called the **minimal polynomial** of α over F and denoted by $min(\alpha,F)$. The following theorem characterizes minimal polynomials in a variety of useful ways. Proof is left to the reader.

Theorem 1.5.1 Let $F < E$ and let $p(x) = min(\alpha,F)$ where $\alpha \in E$. Then among all polynomials in F[x], the polynomial p(x) is

1) the unique monic irreducible polynomial for which $p(\alpha) = 0$
2) the unique monic polynomial of smallest degree for which $p(\alpha) = 0$
3) the unique monic polynomial with the property that $f(\alpha) = 0$ if and only if $p(x) \mid f(x)$. □

Definition Let $F < E$. Then $\alpha, \beta \in E$ are said to be **conjugates** over F if they have the same minimal polynomial over F. □

1.6 Multiple Roots

Definition Let α be a root of $f(x) \in F[x]$. The **multiplicity** of α is the largest positive integer n for which $(x - \alpha)^n$ divides $f(x)$. If $n = 1$, we say that α is a **simple root** and if $n > 1$, we say that α is a **multiple root** of $f(x)$. □

Definition An irreducible polynomial $f(x) \in F[x]$ is said to be **separable** if it has no multiple roots in any extension of F. An irreducible polynomial that is not separable is **inseparable**. □

Although, as we now show, all irreducible polynomials over a field of characteristic zero or a finite field are separable, the concept of separability plays a key role in the theory of more "unusual" fields.

Theorem 1.6.1 A polynomial $f(x)$ has no multiple roots if and only if $f(x)$ and its derivative $f'(x)$ are relatively prime.

Proof. Over a splitting field E for $f(x)$, we have

$$f(x) = (x - \alpha_1)^{e_1} \cdots (x - \alpha_n)^{e_n}$$

where the α_i's are distinct. It is easy to see that $f(x)$ and $f'(x)$ have no nontrivial common factors over E if and only if $e_i = 1$ for all i. Thus, $f(x)$ has no multiple roots in E if and only if $f(x)$ and $f'(x)$ are relatively prime. ∎

Corollary 1.6.2 An irreducible polynomial $f(x)$ is separable if and only if $f'(x) \neq 0$.

Proof. Since $deg\ f'(x) < deg\ f(x)$ and $f(x)$ is irreducible, we deduce that $f(x)$ and $f'(x)$ are relatively prime if and only if $f'(x) \neq 0$. ∎

If $char(F) = 0$ then $f'(x) \neq 0$ for any nonconstant $f(x)$. Thus, we get the following corollary.

Corollary 1.6.3 All irreducible polynomials over a field of characteristic 0 are separable. □

For $\text{char}(F) = p \neq 0$, the next result says that the inseparable polynomials are precisely the polynomials of the form $g(x^{p^d})$ for some $d \geq 1$.

Corollary 1.6.4 Let $\text{char}(F) = p \neq 0$ and let $f(x) \in F[x]$ be irreducible.

1) If $f(x)$ is inseparable, then there exists a positive integer d such that $f(x) = q(x^{p^d})$, where $q(x)$ is separable. In this case, all roots of $f(x)$ have multiplicity p^d.

2) If $f(x) = h(x^{p^d})$ where $h(x)$ is any nonconstant polynomial and d is a positive integer, then $f(x)$ is inseparable.

Proof. For the first statement in part 1), suppose that $f(x) = \sum a_i x^i$ has a multiple root in some extension E of F. Then $f'(x) = 0$ which implies that $ia_i = 0$ for all i, which in turn implies that $p \mid i$ for all i such that $a_i \neq 0$. Hence, $f(x) = q(x^p)$. If $q(x)$ has no multiple roots, we are done. If not, then we may repeat the argument with the irreducible polynomial $q(x)$, eventually obtaining the desired result.

For part 2), if $h(x)$ is not separable, then by part 1), we have $h(x) = q(x^{p^k})$ where $q(x)$ is separable and so

$$f(x) = h(x^{p^d}) = q(x^{p^{d+k}})$$

Thus, we may suppose that $h(x)$ is separable. Let K be a field in which both $f(x)$ and $h(x)$ split. Over K, we have $h(x) = (x - \alpha_1)\cdots(x - \alpha_k)$ and so

$$f(x) = (x^{p^d} - \alpha_1)\cdots(x^{p^d} - \alpha_k)$$

where the $\alpha_i \in K$ are distinct. Since $f(x)$ splits in K, there exist roots $\beta_i \in K$ for each of the factors $x^{p^d} - \alpha_i$, and so $\alpha_i = \beta_i^{p^d}$. Hence,

$$f(x) = (x^{p^d} - \beta_1^{p^d})\cdots(x^{p^d} - \beta_k^{p^d})$$

Since $\text{char}(F) = p$,

$$f(x) = (x - \beta_1)^{p^d}\cdots(x - \beta_k)^{p^d}$$

which shows that all the roots of $f(x)$ have multiplicity p^d. This proves part 2) and also the second statement in part 1). ∎

Corollary 1.6.5 All irreducible polynomials over a finite field are separable.

Proof. Let $\text{char}(F) = p$. The field F is an extension of its prime subfield $\mathbb{Z}_p$ and if the dimension of F as a vector space over $\mathbb{Z}_p$ is n, then F has $q = p^n$ elements. Hence, the multiplicative group F^* of nonzero elements of F has order $q-1$ and so $a^q = a$ for all $a \in F$. In particular, any element of F is a p-th power of some other element of F. Thus, any polynomial of the form $q(x^p)$ satisfies

$$\begin{aligned} q(x^p) &= a_0 + a_1 x^p + \cdots + a_n x^{pn} \\ &= b_0^p + b_1^p x^p + \cdots + b_n^p x^{np} \\ &= (b_0 + b_1 x + \cdots + b_n x^n)^p \end{aligned}$$

and so is not irreducible. ∎

We should note that in infinite fields of nonzero characteristic, there are irreducible polynomials with multiple roots.

Example 1.6.1 Let F be a field of characteristic 2 and consider the field F(y) of all rational functions in the variable y. The polynomial $f(x) = x^2 - y^2$ is irreducible over the subfield $F(y^2)$, since it has no linear factors over $F(y^2)$. However, in F(y) we have $f(x) = (x-y)^2$ and so y is a double root of f(x). □

1.7 Testing for Irreducibility

We discuss two well-known methods for testing a polynomial for irreducibility.

Theorem 1.7.1 (Eisenstein's criterion) Let R be an integral domain and let $p(x) = a_0 + a_1 x + \cdots + a_n x^n \in R[x]$ have relatively prime coefficients. If there exists a prime $p \in R$ satisfying

$$p \mid a_i \text{ for } 0 \leq i < n, \quad p \nmid a_n, \quad p^2 \nmid a_0$$

then p(x) is irreducible.

Proof. Suppose that $p(x) = f(x)g(x)$ where neither factor is a unit. If $f(x) = f_0 \in R$ then f_0 divides a_i for all i, implying that $f(x) = f_0$ is a unit, which is not the case. Thus, *deg* $f(x) > 0$ and similarly *deg* $g(x) > 0$. Let

$$f(x) = f_0 + f_1 x + \cdots + f_k x^k \quad \text{and} \quad g(x) = g_0 + g_1 x + \cdots + g_m x^m$$

Since $a_0 = f_0 g_0$ and $p \mid a_0$, $p^2 \nmid a_0$ we may assume that $p \mid f_0$ and $p \nmid g_0$.

Let $0 < i < n$ be the smallest integer for which $p \not| f_i$ and consider the coefficient

$$a_i = f_0 g_i + f_1 g_{i-1} + \cdots + f_i g_0$$

We have $p \mid a_i$, $p \mid f_0 g_i, \ldots, f_{i-1} g_1$ but $p \not| f_i g_0$, a contradiction. Hence $p(x)$ is irreducible. ∎

Eisenstein's criterion can be useful as a theoretical tool.

Corollary 1.7.2 For every positive integer n, there is an irreducible polynomial $p_n(x)$ of degree n over the integers. □

A useful approach to testing for irreducibility over $\mathbb{Z}[x]$, and hence also over $\mathbb{Q}[x]$, is *localization*. For a prime p, let $\sigma: \mathbb{Z} \to \mathbb{Z}_p$ be the natural map

$$\sigma n = \bar{n} = n + \langle p \rangle$$

If $p(x) \in \mathbb{Z}[x]$ we denote $(\sigma p)(x)$ by $\bar{p}(x)$.

Theorem 1.7.3 Let $p(x) = a_0 + a_1 x + \cdots + a_n x^n \in \mathbb{Z}[x]$ be primitive. Let p be a prime that does not divide a_n. If $\bar{p}(x)$ is irreducible over $\mathbb{Z}_p$ then $p(x)$ is irreducible over $\mathbb{Z}$.

Proof. Assume that $\bar{p}(x)$ is irreducible over $\mathbb{Z}_p$ but that $p(x) = f(x)g(x)$ is the product of nonunits over $\mathbb{Z}$. Then $\bar{p}(x) = \bar{f}(x)\bar{g}(x)$. Since $a_n \not\equiv 0 \bmod p$, we have

$$deg\ \bar{f}(x) + deg\ \bar{g}(x) = deg\ \bar{p}(x) = deg\ p(x) = deg\ f(x) + deg\ g(x)$$

which implies that $deg\ \bar{f}(x) = deg\ f(x)$ and $deg\ \bar{g}(x) = deg\ g(x)$. Since $\bar{p}(x)$ is irreducible, we must have $deg\ \bar{f}(x) = 0$ or $deg\ \bar{g}(x) = 0$, implying that one of $f(x)$ or $g(x)$ is a constant (nonunit), in contradiction to the primitiveness of $p(x)$. Hence, $p(x)$ is irreducible over $\mathbb{Z}$. ∎

Exercises

1. Prove that if R is an integral domain then so is $R[x_1, \ldots, x_n]$.
2. Describe the units in $F[x]$ where F is a field.
3. Let R be an integral domain. Prove that $c(\alpha p(x)) \sim \alpha c(p(x))$ for any $p(x) \in R[x]$ and $\alpha \in R$.
4. Prove that if $n > 1$ then the ring $F[x_1, \ldots, x_n]$ is not a principal ideal domain.
5. If $f(x) \in R[x]$ where R is an integral domain with field of quotients R′, then $f(x)$ can also be viewed as a polynomial in $R'[x]$. Show

that the definition of content for $f(x) \in R[x]$ agrees with the definition of content for $f(x) \in R'[x]$.

6. Verify the division algorithm (Theorem 1.3.1) for commutative rings with identity. *Hint*: try induction on *deg* f(x).
7. Show that the condition that p(x) be primitive is essential in the first part of Theorem 1.2.2.
8. Prove Theorem 1.5.1.
9. Let *deg* $p(x) = d$. The *reciprocal polynomial* is $q(x) = x^d p(x^{-1})$. Are the irreducibility of p(x) and q(x) related? Can you deduce an alternate version of Eisenstein's criterion from this?
10. Show that if p is a prime in an integral domain R, the polynomial $p(x) = x^n - p$ is irreducible.
11. Prove that for every positive integer n there is an irreducible polynomial $p_n(x) \in \mathbb{Z}[x]$ of degree n.
12. For p prime show that $p(x) = 1 + x + x^2 + \cdots + x^{p-1}$ is irreducible over $\mathbb{Z}[x]$. *Hint*: apply Eisenstein to the polynomial p(x+1).
13. Use the idea of localization (apply the map σ) to deduce that Eisenstein's criterion implies irreducibility in $\mathbb{Z}[x]$.
14. Prove that for p prime, $x^n + px + p^2$ is irreducible over $\mathbb{Z}[x]$.
15. If R is an infinite integral domain and $p(x_1,\ldots,x_n)$ is a polynomial in several variables over R, show that $p(x_1,\ldots,x_n)$ is zero as a function if and only if it is zero as a polynomial.

If f(x) is a polynomial of degree d, we define the **reciprocal polynomial** by $f_R(x) = x^d f(x^{-1})$. Thus, if

$$f(x) = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0$$

then

$$f_R(x) = a_0 x^n + a_1 x^{n-1} + \cdots + a_{n-1}x + a_n$$

If a polynomial satisfies $f(x) = f_R(x)$, we say that f(x) is **self-reciprocal.**

16. Show that $\alpha \neq 0$ is a root of f(x) if and only if α^{-1} is a root of $f_R(x)$.
17. Show that the reciprocal of an irreducible polynomial $f(x) \neq x$ is also irreducible.
18. Show that if a polynomial f(x) is self-reciprocal and irreducible, then *deg* f(x) must be even.
19. Suppose that $f(x) = p(x)q(x)$, where p(x) and q(x) are irreducible, and f(x) is self-reciprocal. Show that either
    (i) $p(x) = \delta p_R(x)$ and $q(x) = \delta q_R(x)$ with $\delta = \pm 1$, or
    (ii) $p(x) = \alpha q_R(x)$ and $q(x) = \alpha^{-1} p_R(x)$ for some $\alpha \in GF(q)$.
    What can you say about this if *deg* p(x) is odd?
20. There is a simple (but not necessarily practical) algorithm for factoring any polynomial over $\mathbb{Q}$, due to Kronecker. In view of

Theorem 1.2.2, it suffices to consider polynomials with integer coefficients. Prove that a polynomial of degree n is completely determined by specifying $n+1$ of its values. *Hint*: Use the *Lagrange Interpolation Formula*

$$p(x) = \sum_{i=0}^{n} p(i) \left[\prod_{j \neq i} \frac{x-j}{i-j} \right]$$

Let $f(x)$ be a polynomial of degree $n > 1$ over $\mathbb{Z}$. If $f(x)$ has a nonconstant factor $p(x)$ of degree at most $n/2$, what can you say about the values $p(i)$ for $i = 0, \ldots, \lfloor n/2 \rfloor$? Construct an algorithm for factoring $f(x)$ into irreducible factors.

Chapter 2

Field Extensions

Field extensions $F < E$ can be characterized in a variety of useful ways. Some characterizations involve properties of the individual elements of the extension. For instance, an extension $F < E$ is *algebraic* if each element $\alpha \in E$ is algebraic over F. Other characterizations involve the field E as a whole. For instance, $F < E$ is *normal* if E is the splitting field for a family of polynomials over F. In this chapter, we will describe several types of extensions and study their basic properties.

2.1 The Lattice of Subfields of a Field

If E is an extension field of F, then E can be viewed as a vector space over F. The dimension of E over F is denoted by [E:F] and called the **degree** of E over F. A sequence of fields $E_1, \ldots, E_n$ for which $E_i < E_{i+1}$ is referred to as a **tower** of fields, and we write $E_1 < E_2 < \cdots < E_n$. The fact that dimension is multiplicative over towers is fundamental.

Theorem 2.1.1 Let $F < K < E$. Then

$$[E:F] = [E:K][K:F]$$

Moreover, if $A = \{\alpha_i \mid i \in I\}$ is a basis for E over K and $B = \{\beta_j \mid j \in J\}$ is a basis for K over F, then the set $C = \{\alpha_i\beta_j \mid i \in I, j \in J\}$ is a basis for E over F.

Proof. For the independence of C, if $\sum a_{i,j}\alpha_i\beta_j = 0$ then $\sum a_{i,j}\alpha_i = 0$ for all j, and the latter implies that $a_{i,j} = 0$ for all i, j. Hence, C is independent. Next, if $\gamma \in E$ then there exist $a_i \in K$ such that $\gamma = \sum a_i\alpha_i$. Since each a_i is a linear combination of the β_j's, it follows that γ is a linear combination of the products $\alpha_i\beta_j$. Hence C is a basis for E over F. ∎

If F and E are subfields of a field K, then the intersection $F \cap E$ is clearly a field. The **composite** FE of F and E is defined to be the smallest subfield of K containing both F and E. The composite FE is also equal to the intersection of all subfields of K containing E and F. More generally, the composite $\vee E_i$ of a family $\mathcal{S} = \{E_i \mid i \in I\}$ of fields, all of which are contained in a single field E, is the smallest subfield of E containing all members of the family. Note that the composite of fields is defined only when the fields are all contained in one larger field. Whenever we form a composite, it is with the tacit understanding that the relevant fields are so contained.

A **monomial** over a family $\mathcal{S} = \{E_i \mid i \in I\}$ of fields with $E_i < E$ is an element of E of the form

$$e_{i_1}e_{i_2}\cdots e_{i_n}, \quad \text{where } e_{i_k} \in E_{i_k}$$

Note that the set of all finite sums of monomials over $\mathcal{S}$ is the smallest subring R of E containing each field E_i and the set of all quotients of elements of R (the quotient field of R) is the composite $\vee E_i$. Thus, each element of $\vee E_i$ involves only a finite number of elements from the union $\bigcup E_i$ and is therefore contained in a composite of a finite number of fields from the family $\mathcal{S}$.

The collection of all subfields of a field K forms a complete lattice $\mathcal{L}$ (under set inclusion), with meet being intersection and join being composite. The zero element in $\mathcal{L}$ is the prime subfield of K and the unit element is K itself.

2.2 Distinguished Extensions

Following Lang, we will say that a class $\mathcal{C}$ of field extensions is **distinguished** provided that

D1) If $F < K < E$, then $(F < E) \in \mathcal{C}$ if and only if $(F < K) \in \mathcal{C}$ and $(K < E) \in \mathcal{C}$.

D2) If $(F < E) \in \mathcal{C}$ and $F < K$ and EK is defined, then $(K < EK) \in \mathcal{C}$.

Note that if $\mathcal{C}$ is distinguished, then

D3) If $(F < E) \in \mathcal{C}$ and $(F < K) \in \mathcal{C}$ and EK is defined, then $(F < EK) \in \mathcal{C}$. In other words, $\mathcal{C}$ is closed under taking (a finite number of) composites.

Figure 2.2.1 illustrates D1) and D2). We refer to $K < EK$ as the **lifting** of the extension $F < E$ by K.

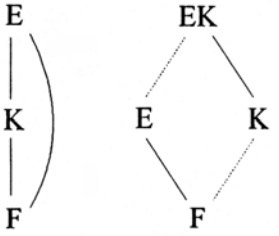

Figure 2.2.1

If a class $\mathcal{C}$ of extensions has the property that whenever $(F < E_i) \in \mathcal{C}$ for each member of a family $\{E_i\}$ of fields and if $\vee E_i$ is defined, then $(F < \vee E_i) \in \mathcal{C}$, we say that $\mathcal{C}$ is **closed under the taking of arbitrary composites.**

2.3 Finitely Generated Extensions

If S is a subset of a field E and if $F < E$, we denote the smallest subfield of E containing F and S by F(S). When $S = \{\alpha_1, \ldots, \alpha_n\}$ is a finite set, it is customary to write $F(\alpha_1, \ldots, \alpha_n)$ for F(S). Note that for $1 \leq k \leq n-1$,

$$F(\alpha_1, \ldots, \alpha_n) = [F(\alpha_1, \ldots, \alpha_k)](\alpha_{k+1}, \ldots, \alpha_n)$$

Definition Any field of the form $E = F(\alpha_1, \ldots, \alpha_n)$ is said to be **finitely generated** over F. We also say that the extension $F < E$ is finitely generated. Any extension of the form $F < F(\alpha)$ is called a **simple** extension and α is a **primitive element** in $F(\alpha)$. □

The reader may have encountered a different meaning of the term *primitive* in connection with elements of a finite field. We will discuss this alternate meaning when we discuss finite fields later in the book.

It is evident that $F(\alpha_1, \ldots, \alpha_n)$ consists of all quotients of polynomials in the α_i's:

$$F(\alpha_1, \ldots, \alpha_n) = \left\{ \frac{f(\alpha_1, \ldots, \alpha_n)}{g(\alpha_1, \ldots, \alpha_n)} \;\middle|\; g(\alpha_1, \ldots, \alpha_n) \neq 0 \right\}$$

Theorem 2.3.1 The class of all finitely generated extensions is distinguished.

Proof. For D1, let $F < K < E$. If $E = K(S)$ and $K = F(T)$ where S and T are finite, then $E = F(S \cup T)$ is finitely generated over F. Clearly, if $F < E$ is finitely generated then $K < E$ is also finitely generated by the same set of generators. However, the proof that $F < K$ is finitely generated must be postponed until we have discussed transcendental extensions in the next chapter. Statement D2 follows from the fact that if $E = F(S)$, S finite, and $F < K$ then

$$KE = K(F(S)) = K(S)$$

and so KE is finitely generated over K. ∎

2.4 Simple Extensions

Since F[x] is a principal ideal domain, the ideal $\langle p(x) \rangle$ generated by $p(x) \in F[x]$ is maximal, and the quotient ring

$$K = \frac{F[x]}{\langle p(x) \rangle}$$

is a field, if and only if p(x) is irreducible. We can use this observation to characterize simple algebraic extensions.

Theorem 2.4.1 Let $F < E$ and let $\alpha \in E$ be algebraic over F. Then $F(\alpha)$ is isomorphic to the field

$$K = \frac{F[x]}{\langle min(\alpha, F) \rangle}$$

Proof. Let $\psi: F[x] \to E$ be the evaluation (ring) homomorphism defined by $\psi(f(x)) = f(\alpha)$. The kernel of ψ is the ideal $\langle min(\alpha, F) \rangle$, and so K is isomorphic to $\psi(F[x])$, which implies that $\psi(F[x])$ is a field. Thus, we need only show that $\psi(F[x]) = F(\alpha)$. Clearly, $\psi(F[x]) \subseteq F(\alpha)$. But $\alpha = \psi(x) \in \psi(F[x])$ and $F \subseteq \psi(F[x])$ imply that $F(\alpha) \subseteq \psi(F[x])$. Hence, $\psi(F[x]) = F(\alpha)$. ∎

Let p(x) be irreducible over F. Since addition and multiplication in $K = F[x]/\langle p(x) \rangle$ is done using coset representatives and since

$$K' = \{f(x) \in F[x] \mid deg\ f(x) < deg\ p(x)\}$$

is a complete set of distinct coset representatives for K, we may identify K with K′, where addition and multiplication are performed modulo

p(x). This allows us the customary practice of thinking of F as a subfield of K. Note also that, as a vector space over F, we have *dim* K = *deg* p(x). In the symbolism of Theorem 2.4.1, we have $[F(\alpha):F] = deg\ min(\alpha,F)$.

Thus $F(\alpha)$ is the set of all polynomials in α of degree less than $d = deg\ min(\alpha,F)$, with addition and multiplication modulo $min(\alpha,F)$. It follows that the set $\{1,\alpha,\ldots,\alpha^{d-1}\}$ is a basis for $F(\alpha)$ over F.

As for simple transcendental extensions, we have the following.

Theorem 2.4.2 Let $F < E$ and let $\alpha \in E$ be transcendental over F. Then $F(\alpha)$ is isomorphic to the field of all rational functions F(x) in a single variable x.

Proof. The evaluation homomorphism $\psi:F(x)\rightarrow E$ is injective, for if $f(\alpha)/g(\alpha) = 0$ then $f(\alpha) = 0$, which implies that f(x) = 0, since otherwise α would be algebraic. Since $\psi(F(x)) = F(\alpha)$, we deduce that ψ is an isomorphism from F(x) onto $F(\alpha)$. ∎

2.5 Finite Extensions

If $F < E$ and [E:F] is finite, we say that E is a **finite extension** of F or that $F < E$ is **finite**. We have already seen that the following is true.

Theorem 2.5.1 If $F < E$ and if $\alpha \in E$ is algebraic over F then $F < F(\alpha)$ is finite, and $[F(\alpha):F] = deg\ min(\alpha,F)$. □

Theorem 2.5.2 An extension is finite if and only if it is finitely generated by algebraic elements.

Proof. If $F < E$ is finite and if $\{\alpha_1,\ldots,\alpha_n\}$ is a basis for E over F, then $E = F(\alpha_1,\ldots,\alpha_n)$ is finitely generated over F. Moreover, for each k, the infinite set of nonnegative powers of α_k cannot be linearly independent over F, it follows that α_k must be algebraic over F.

For the converse, assume that $E = F(\alpha_1,\ldots,\alpha_n)$, where each α_i is algebraic over F, and consider the tower

$$F < F(\alpha_1) < F(\alpha_1,\alpha_2) < \cdots < F(\alpha_1,\ldots,\alpha_n) = E$$

Since α_i is algebraic over $F(\alpha_1,\ldots,\alpha_{i-1})$, each extension in the tower is finite, and so E is finite over F by Theorem 2.1.1. ∎

Suppose that $E = F(\alpha_1,\ldots,\alpha_n)$ is finitely generated by algebraic elements α_i over F and consider the tower

$$F < F(\alpha_1) < F(\alpha_1,\alpha_2) < \cdots < F(\alpha_1,\ldots,\alpha_n) = E$$

Our results on simple algebraic extensions show that any element of $F(\alpha_1)$ is a polynomial in α_1 over F. Further, any element of $F(\alpha_1,\alpha_2)$ is a polynomial in α_2 over $F(\alpha_1)$, and hence a polynomial in the two variables α_1 and α_2. Continuing in this way, we conclude that E is the set of all polynomials over F in $\alpha_1,\ldots,\alpha_n$.

Theorem 2.5.3 The class of finite extensions is distinguished.

Proof. The multiplicativity of degree shows that D1 holds. For D2, let $F < E$ be finite, with basis $\{\alpha_1,\ldots,\alpha_n\}$ and let $F < K$. Thus $E = F(\alpha_1,\ldots,\alpha_n)$ where each α_i is algebraic over F and so also over K. Since $EK = K(\alpha_1,\ldots,\alpha_n)$ is finitely generated by elements algebraic over K, it is a finite extension of K. ∎

Note that if E is a splitting field for $p(x) \in F[x]$ then E is generated by a complete set of distinct roots $\alpha_1,\ldots,\alpha_n$ of p(x). Thus $E = F(\alpha_1,\ldots,\alpha_n)$ is finitely generated by algebraic elements and so is a finite extension of F, of degree at most d!, where $d = \textit{deg}\ p(x)$. This also applies to the splitting field for any finite set of polynomials over F.

Suppose that $F < E$ is finite and let $B = \{\beta_1,\ldots,\beta_n\}$ be a basis for E over F. If $F < K$, then since $EK = K(\beta_1,\ldots,\beta_n)$ and each β_i is algebraic over F, and hence also over K, it follows that EK is the set of polynomials over K in $\beta_1,\ldots,\beta_n$. However, any monomial in the β_i's is a linear combination (over F) of $\beta_1,\ldots,\beta_n$ and so EK is the set of linear combinations of $\beta_1,\ldots,\beta_n$ over K. In other words, B spans EK over K. We have proved the following, which says that a lifting cannot increase degree.

Theorem 2.5.4 If B is a basis for E over F and if $F < K$ then B spans EK over K. In particular, if $F < E$ is finite then $[EK:K] \leq [E:F]$. □

The next theorem characterizes finite simple extensions.

Theorem 2.5.5 A finite extension $F < E$ has the form $E = F(\alpha)$ for $\alpha \in E$ if and only if there are only a finite number of intermediate fields $F < K < E$ between E and F.

Proof. Suppose first that $E = F(\alpha)$, and that $p(x) = \textit{min}(\alpha,F)$. Define a map ψ that assigns to each intermediate field K the polynomial $\psi(K) = \textit{min}(\alpha,K)$. Since $p(x) \in K[x]$ and $p(\alpha) = 0$, we have $\psi(K) \mid p(x)$. But a monic polynomial has only a finite number of monic divisors. Hence, the range of ψ is finite and therefore it is sufficient to show that ψ is injective. Let K be an intermediate field, let S be the set of coefficients

of $\psi(K)$ and consider the tower $F(S) < K < F(\alpha)$. Since $\psi(K)$ is a monic irreducible polynomial over $F(S)$ and is satisfied by α, we have $\psi(K) = min(\alpha,F(S))$. Hence, $[F(\alpha):K] = deg\ \psi(K) = [F(\alpha):F(S)]$, which implies that $[K:F(S)] = 1$, that is, $K = F(S)$. This shows that K is uniquely determined by the polynomial $\psi(K)$, and so ψ is injective.

For the converse, if E is a finite field, the multiplicative group E^* of nonzero elements of E is cyclic. If α generates this group, then $E = F(\alpha)$ is simple. Now suppose that E is an infinite field and there are only finitely many intermediate fields between E and F. Let α, $\beta \in E$ and consider the intermediate fields $F(\alpha + a\beta)$, for $a \in F$. By hypothesis, $F(\alpha + a\beta) = F(\alpha + b\beta)$ for some $a \neq b \in F$. Hence, $\alpha + b\beta \in F(\alpha + a\beta)$, implying that

$$\beta = \frac{1}{a-b}[(\alpha + a\beta) - (\alpha + b\beta)] \in F(\alpha + a\beta)$$

and

$$\alpha = (\alpha + a\beta) - a\beta \in F(\alpha + a\beta)$$

Hence, $F(\alpha,\beta) \subseteq F(\alpha + a\beta)$. The reverse inclusion is evident and so $F(\alpha,\beta) = F(\alpha + a\beta)$, showing that any extension of F generated by two elements is a simple extension. Since $F < E$ is finite, it is finitely generated and an inductive argument can be used to show that $F < E$ is simple. ∎

2.6 Algebraic Extensions

Definition An extension E of F is **algebraic** over F (or $F < E$ is **algebraic**) if every element $\alpha \in E$ is algebraic over F. Otherwise, E is a **transcendental** extension of F. □

Theorem 2.6.1 A finite extension is algebraic.

Proof. If $F < E$ is finite and $\alpha \in E$ then the sequence of powers 1, α, α^2,... cannot be linearly independent over F and therefore some nontrivial polynomial in α must equal 0, implying that α is algebraic over F. ∎

Corollary 2.6.2 Any extension that is finitely generated by algebraic elements is algebraic. □

Theorem 2.6.3 Let $F < E$. The set K of all elements of E that are algebraic over F is a field, called the **algebraic closure of F in E.**

Proof. Let α, $\beta \in K$. The field $F(\alpha,\beta)$ is finitely generated over F by algebraic elements and so is algebraic over F, that is, $F(\alpha,\beta) \subseteq K$. This

implies that α^{-1}, $\alpha \pm \beta$ and $\alpha\beta$ all lie in K, and so K is a subfield of E. ∎

Theorem 2.6.4 The class of algebraic extensions is distinguished. It is also closed under the taking of arbitrary composites.

Proof. For D1, let $F < K < E$. It is clear that if $F < E$ is algebraic then so is $F < K$. Also, since any polynomial over F is a polynomial over K, $K < E$ is also algebraic. Conversely, suppose that $F < K$ and $K < E$ are algebraic and let $\alpha \in E$ have minimal polynomial $p(x) = \sum a_i x^i$ over K. Consider the tower of fields

$$F < F(a_1,\ldots,a_n) < F(a_1,\ldots,a_n,\alpha)$$

Since α is algebraic over $F(a_1,\ldots,a_n)$ and each a_i, being in K, is algebraic over F, we deduce that each step in the tower is finite and so $F < F(a_1,\ldots,a_n,\alpha)$ is finite. Hence, α is algebraic over F.

For D2, let $F < E$ be algebraic and let $F < K$, with E and K contained in a field L. We must show that $K < EK$ is algebraic. Let A be the algebraic closure of K in EK. Certainly $K < A < EK$. Since each element of E is algebraic over F it is *a fortiori* algebraic over K and so $E < A$. Hence, $EK < A < EK$, showing that $EK = A$ is algebraic over K.

Finally, if $\{E_i\}$ is a family of fields, each algebraic over F, then so is $\vee E_i$, since an element of $\vee E_i$ is also an element of a composite of only a finite number of members of the family. ∎

The algebraic closure of the rational numbers $\mathbb{Q}$ in the real numbers $\mathbb{R}$ is the field $\mathcal{A}$ of **algebraic numbers.** We saw in the previous chapter that there is an irreducible polynomial $p_n(x) \in \mathbb{Z}[x]$ of every positive degree n. Hence, $\mathcal{A}$ is an infinite algebraic extension of $\mathbb{Q}$, showing that the converse of Theorem 2.6.1 does not hold.

We note finally that if $F < E$ is algebraic and if $E = F(S)$ for some $S \subseteq E$ then each element of E is a polynomial in finitely many elements from S. This follows from the fact that each $\alpha \in F(S)$ is a rational function in finitely many elements of S and so there exists a finite subset $S_0 \subseteq S$ such that $\alpha \in F(S_0)$. Hence, our discussion in Section 2.5 related to finitely generated algebraic extensions applies here.

2.7 Algebraic Closures

Definition A field E is said to be **algebraically closed** if any nonconstant polynomial with coefficients in E splits in E. □

Theorem 2.7.1 Let F be a field. Then there is an extension E of F that is algebraically closed.

Proof. The following proof is due to Emil Artin. The first step is to construct an extension field F_1 of F, with the property that all nonconstant polynomials in F[x] have a root in F_1. To this end, for each nonconstant polynomial $p(x) \in F[x]$, we let X_p be an independent variable and consider the ring $\mathfrak{R}$ of all polynomials in the variables X_p over the field F. Let $\mathfrak{I}$ be the ideal generated by the polynomials $p(X_p)$. We contend that $\mathfrak{I}$ is not the entire ring $\mathfrak{R}$. For if it were, then there would exist polynomials $q_1,\ldots,q_n \in \mathfrak{R}$ and $p_1,\ldots,p_n \in \mathfrak{I}$ such that

$$q_1 p_1(X_{p_1}) + \cdots + q_n p_n(X_{p_n}) = 1$$

This is an algebraic expression over F in a finite number of independent variables. But there is an extension field E of F in which each of the polynomials $p_1(x),\ldots,p_n(x)$ has a root, say $\alpha_1,\ldots,\alpha_n$. Setting $X_{p_i} = \alpha_i$ and setting any other variables appearing in the equation above equal to 0 gives $0 = 1$. This contradiction implies that $\mathfrak{I} \neq \mathfrak{R}$.

Since $\mathfrak{I} \neq \mathfrak{R}$, there exists a maximal ideal $\mathfrak{J}$ such that $\mathfrak{I} \subseteq \mathfrak{J} \subset \mathfrak{R}$. Then $F_1 = \mathfrak{R}/\mathfrak{J}$ is a field in which each polynomial $p(x) \in F[x]$ has a root, namely $X_p + \mathfrak{J}$. (We may think of F_1 as an extension of F by identifying $\alpha \in F$ with $\alpha + \mathfrak{J}$.)

Using the same technique, we may define a tower of field extensions

$$F < F_1 < F_2 < \cdots$$

such that each nonconstant polynomial $p(x) \in F_i[x]$ has a root in F_{i+1}. The union $E = \bigcup F_i$ is an extension field of F. Moreover, any polynomial $p(x) \in E[x]$ has all of its coefficients in F_i for some i and so has a root in F_{i+1}, hence in E. It follows that every polynomial $p(x) \in E[x]$ splits over E. Hence E is algebraically closed. ∎

Definition Let $F < E$. Then E is an **algebraic closure** of F if $F < E$ is algebraic and E is algebraically closed. We will denote an algebraic closure of a field F by $\overline{F}$. □

Theorem 2.7.2 Let $F < E$. The following are equivalent.

1) E is an algebraic closure of F.
2) $F < E$ is algebraic and any nonconstant polynomial p(x) *over F* splits in E.
3) E is a maximal algebraic extension of F, that is, $F < E$ is algebraic and if $E < K$ is algebraic then $K = E$.

Proof. Clearly 1) implies 2). Suppose 2) holds and $E < K$ is algebraic. Let $\alpha \in K$. Then $F < E < E(\alpha)$ is an algebraic tower and so α is algebraic over F. But the minimal polynomial $min(\alpha,F)$ splits in E and so $\alpha \in E$. Thus $K = E$ and 3) holds. Finally, suppose 3) holds and let $p(x) \in E[x]$. Any splitting field K for $p(x)$ is algebraic over E and so must equal E, which implies that $p(x)$ splits in E. Hence, 1) holds. ∎

We can now easily establish the existence of algebraic closures.

Theorem 2.7.3 Let $F < A < E$ where A is the algebraic closure of F in E. If E is algebraically closed then A is also algebraically closed and hence is an algebraic closure of F. Thus, any field has an algebraic closure.

Proof. We have already seen that A is an algebraic extension of F. By hypothesis, any $p(x) \in A[x]$ splits in E and so all of its roots lie in E. Since these roots are algebraic over A, they are also algebraic over F and thus lie in A. Hence $p(x)$ splits in A and so A is algebraically closed. The final statement follows from Theorem 2.7.1. ∎

2.8 Embeddings

Homomorphisms between fields play a key role in the theory. Since a field F has no ideals other than $\{0\}$ and F, it follows that any nonzero (ring) homomorphism $\sigma:F \to L$ from F into L must be a monomorphism. If $f:A \to B$ is any function and if $C \subseteq A$, we denote the restriction of f to C by $f \mid_C$.

Definition Let F and L be fields. A monomorphism $\sigma:F \to L$ is called an **embedding** of F into L. We will denote the image of F under σ by σF or F^σ. If $F < E$, an embedding $\tau:E \to L$ for which $\tau \mid_F = \sigma$ is called an **extension** of σ to E. An embedding of E that extends the identity map $\iota:F \to F$ is called an embedding **over F**, or an **F-embedding**. We will denote the set of all embeddings of E into L over F by $Hom_F(E,L)$. If $p(x) = \sum a_i x^i \in F[x]$ and if $\sigma:F \to L$ is an embedding we denote the polynomial $\sum \sigma(a_i)x^i$ by $(\sigma p)(x)$ or $p^\sigma(x)$. □

Lemma 2.8.1

1) Let $\sigma:F \to L$ be an embedding of F into L and let $p(x) \in F[x]$. Then $\alpha \in F$ is a root of $p(x)$ if and only if $\sigma\alpha$ is a root of $p^\sigma(x)$.
2) If $\sigma:K \to L$ is an embedding of K into L and if $\{E_i \mid i \in I\}$ is a family of subfields of K then $\sigma(\vee E_i) = \vee \sigma F$.
3) If $\sigma:K \to L$ is an embedding of K into L and if $F < K$ and $\alpha_1, \ldots, \alpha_n \in K$ then

$$\sigma(F(\alpha_1,\ldots,\alpha_n)) = F^\sigma(\sigma\alpha_1,\ldots,\sigma\alpha_n)$$

Proof. Part 1) follows from the fact that $\sigma(p(\alpha)) = p^\sigma(\sigma\alpha)$. For part 2), since σ is injective, it preserves intersections. But

$$\vee E_i = \bigcap \{H \mid E_i < H < K \text{ for all } i \in I\}$$

and so

$$\sigma(\vee E_i) = \bigcap \{\sigma H \mid E_i < H < K \text{ for all } i \in I\}$$

Since σ:K$\rightarrow\sigma$K is an isomorphism, every H′ satisfying $\sigma E_i < H' < \sigma K$ is of the form σH for some H satisfying $E_i < H < K$ and so

$$\sigma(\vee E_i) = \bigcap \{H' \mid \sigma E_i < H' < \sigma K \text{ for all } i \in I\} = \vee \sigma E_i$$

We leave proof of part 3) to the reader. ∎

Even though the next result has a simple proof, the result is of major importance.

Theorem 2.8.2 Let $F < E$ be algebraic and let σ:E$\rightarrow$E be an embedding of E into itself over F. Then σ is an automorphism of E.

Proof. Let $\alpha \in E$ and let $p(x) = min(\alpha,F)$. Let S be the set of roots of p(x) that lie in E. Then $\alpha \in S$. If $\beta \in S$ then $\sigma\beta$ is also a root of p(x) in E, and so $\sigma\beta \in S$. Hence, $\sigma \mid_S$ is a permutation on S and so there is a $\beta \in S$ for which $\sigma\beta = \alpha$. This shows that σ is surjective, hence an automorphism of E. ∎

It is a cornerstone of the theory that an embedding σ:F$\rightarrow$L into an algebraically closed field can be extended to any algebraic extension of F. We begin with the case of a simple algebraic extension.

Suppose that σ:F$\rightarrow$L is an embedding of F into an algebraically closed field L. If $F < E$ and $\alpha \in E$ is algebraic over F then we may take advantage of the fact that α satisfies its minimal polynomial p(x) over F to extend σ to $F(\alpha)$ as follows. Since L is algebraically closed, $p^\sigma(x) \in F^\sigma[x]$ splits in L, and since σ is an embedding, $p^\sigma(x)$ is irreducible over σF. Hence $p^\sigma(x)$ is the minimal polynomial over σF of any of its roots in L. Let β be a root of $p^\sigma(x)$ in L. Then

$$F(\alpha) = \{f(\alpha) \mid f(x) \in F[x],\ \textit{deg}\ f(x) < \textit{deg}\ p(x)\}$$

and since $\textit{deg}\ p^\sigma(x) = \textit{deg}\ p(x)$,

$$F^\sigma(\beta) = \{g(\beta) \mid g(x) \in F^\sigma[x],\ \textit{deg}\ g(x) < \textit{deg}\ p(x)\}$$

Thus we may define a map $\overline{\sigma}$:F(α)→F$^{\sigma}$(β) by

$$\overline{\sigma}(f(\alpha)) = f^{\sigma}(\beta)$$

for any f(x) ∈ F[x]. It is straightforward to show that $\overline{\sigma}$ is an embedding of F(α) into F$^{\sigma}$(β) over σ and that $\overline{\sigma}\alpha = \beta$. This proves the first part of the following theorem. The rest of the theorem follows easily.

Theorem 2.8.3 Let F < E and let $\alpha \in E$ be algebraic over F, with minimal polynomial p(x) = *min*(α,F). Let σ:F→L be an embedding of F into an algebraically closed field L.

1) If β is a root of p$^{\sigma}$(x) in L then σ can be extended to an embedding $\overline{\sigma}$:F(α)→L for which $\overline{\sigma}\alpha = \beta$.
2) Any extension of σ to F(α) must map α to a root of p$^{\sigma}$(x) in L.
3) The number of extensions of σ to F(α) is equal to the number of distinct roots of *min*(α,F) in $\overline{F}$. ∎

Zorn's Lemma can now be used to extend the first part of this theorem to arbitrary algebraic extensions.

Theorem 2.8.4 Let F < E be algebraic. Any embedding σ:F→L into an algebraically closed field L can be extended to an embedding $\overline{\sigma}$:E→L. Moreover, if $\alpha \in E$, p(x) = *min*(α,F) and $\beta \in L$ is a root of p$^{\sigma}$(x), then we can arrange it so that $\overline{\sigma}\alpha = \beta$. (See Figure 2.8.1.)

Proof. Let $\mathcal{S}$ be the set of all embeddings τ:K→L over σ for which $\tau\alpha = \beta$ and F < K < E. Theorem 2.8.3 implies that $\mathcal{S}$ is not empty. Order the elements of $\mathcal{S}$ by saying that (τ':K'→L) ≥ (τ:K→L) if K < K' and τ' is an extension of τ. Then $\mathcal{S}$ is a partially ordered set. If $\mathcal{C}$ = {τ_i:K_i→L} is a chain in $\mathcal{S}$, the map τ: $\bigcup K_i$→L defined by the condition $\tau \mid_{K_i} = \tau_i$ is an upper bound for $\mathcal{C}$ in $\mathcal{S}$. Zorn's Lemma implies the existence of a maximal extension τ:K→L. We contend that K = E, for if not, there is an element $\gamma \in E - K$. But γ is algebraic over K and so we may extend τ to K(γ), contradicting the maximality of τ. ∎

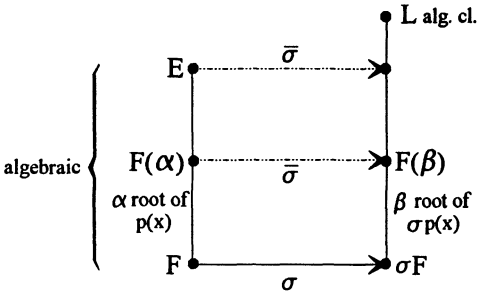

Figure 2.8.1

We can now establish the essential uniqueness of algebraic closures.

Corollary 2.8.5 Any two algebraic closures of a field F are isomorphic.

Proof. Let K and L be algebraic closures of F. The identity map ι:F→F can be extended to an embedding τ:K→L. Since K is algebraically closed so is τK. But L is an algebraic extension of τK and so L = τK. Hence, τ is an isomorphism. ∎

We close this section with a highly useful result on independence of embeddings. We choose a somewhat more general setting, however. A **monoid** is a nonempty set M with an associative binary operation and an identity element. If M and M′ are monoids, a **homomorphism** of M into M′ is a map ψ:M→M′ such that $\psi(\alpha\beta) = \psi(\alpha)\psi(\beta)$ and $\psi(1) = 1$.

Definition Let M be a monoid and let K be a field. A homomorphism χ:M→K*, where K* is the multiplicative group of all nonzero elements of K is called a **character** of M in K. □

Note that an embedding σ:E→L of fields defines a character σ:E*→L*.

Theorem 2.8.6 (E. Artin) Any set $\mathcal{T}$ of distinct characters of M in K is linearly independent over K.

Proof. Suppose to the contrary that

$$\alpha_1\chi_1 + \cdots + \alpha_n\chi_n = 0$$

for $\chi_i \in \mathcal{T}$ and $\alpha_i \in K$, not all 0. Look among all such nontrivial linear combinations of the χ_i's for one with the fewest number of nonzero coefficients and, by relabeling if necessary, assume that these coefficients are $\alpha_1, \ldots, \alpha_r$. Thus,

$$\alpha_1\chi_1(g) + \cdots + \alpha_r\chi_r(g) = 0 \tag{2.8.1}$$

for all $g \in M$ and this is the "shortest" such nontrivial equation (hence $\alpha_i \neq 0$ for all i). Note that since $\chi_i(g) \in K^*$, we have $\chi_i(g) \neq 0$ for all $g \in M$. Hence, $r > 1$.

Since $\chi_1 \neq \chi_r$, there is a $g \in M$ for which $\chi_1(g) \neq \chi_r(g)$. For any $h \in M$, we have

$$\alpha_1\chi_1(gh) + \cdots + \alpha_r\chi_r(gh) = 0$$

that is,

$$\alpha_1\chi_1(g)\chi_1(h) + \cdots + \alpha_r\chi_r(g)\chi_r(h) = 0$$

Multiplying (2.8.1) by $\chi_1(g)$ gives

$$\alpha_1\chi_1(g)\chi_1(h) + \cdots + \alpha_r\chi_1(g)\chi_r(h) = 0$$

Subtracting the previous two equations gives

$$\alpha_2[\chi_1(g) - \chi_2(g)]\chi_2(h) + \cdots + \alpha_r[\chi_1(g) - \chi_r(g)]\chi_r(h) = 0$$

and since the last coefficient is not zero, this contradicts the minimal nature of (2.8.1). Hence the characters are linearly independent. ∎

Corollary 2.8.7 (Dedekind Independence Theorem) Let E and L be fields. Any set of distinct embeddings of E into L is linearly independent over L. □

2.9 Splitting Fields and Normal Extensions

Let us repeat a definition from Chapter 1.

Definition Let $\mathfrak{F} = \{f_i(x) \mid i \in I\}$ be a family of polynomials in F[x]. A **splitting field** for $\mathfrak{F}$ over F is an extension field E of F with the property that each $f_i(x)$ splits in E and that E is generated by the set of all roots of every polynomial in $\mathfrak{F}$. □

It is clear that, given a particular algebraic closure $\overline{F}$ of F, there is a unique splitting field for $\mathfrak{F}$ in $\overline{F}$, since that splitting field must be the field generated by the roots in $\overline{F}$ of all polynomials in $\mathfrak{F}$. It is also true that any two splitting fields for $\mathfrak{F}$ are isomorphic by an isomorphism that fixes the elements of the base field F.

Theorem 2.9.1 Let $p(x) \in F[x]$. Any two splitting fields for p(x) over F are isomorphic over F. Specifically, if S_1 and S_2 are splitting fields for p(x) over F and if $\sigma: S_1 \to \overline{S}_2$ is an F-embedding of S_1 into an algebraic closure of S_2 then σ is an isomorphism of S_1 onto S_2.

Proof. By Theorem 2.4.8, we may extend the inclusion map $j: F \to \overline{S}_2$ to an embedding $\sigma: S_1 \to \overline{S}_2$ over F. For any such embedding, let R_i be the set of distinct roots of p(x) in S_i. Then $p^\sigma(x) = p(x)$ implies that $\sigma R_1 \subseteq R_2$. But σ is injective and each set R_i is finite, whence by symmetry, we have $\sigma R_1 = R_2$. It follows that

$$\sigma S_1 = \sigma[F(R_1)] = F(\sigma R_1) = F(R_2) = S_2$$

and so σ is an isomorphism. ∎

This result also holds for arbitrary families of polynomials.

Theorem 2.9.2 Let $\mathfrak{F}$ be a family of polynomials over F. Any two splitting fields for $\mathfrak{F}$ are isomorphic over F. Specifically, if S_1 and S_2 are splitting fields for $\mathfrak{F}$ over F and if $\sigma:S_1 \to \overline{S}_2$ is an F-embedding of S_1 into an algebraic closure of S_2 then σ is an isomorphism of S_1 onto S_2.

Proof. As in the proof of the previous theorem, we have an embedding $\sigma:S_1 \to \overline{S}_2$. Let $E_1 < S_1$ and $E_2 < S_2$ be splitting fields for a polynomial p(x) in $\mathfrak{F}$. Theorem 2.9.1 implies that the restriction of σ to E_1 is an isomorphism, whence $\sigma E_1 = E_2$. Taking the composite over the splitting fields E_1 in S_1 of all polynomials in $\mathfrak{F}$ gives

$$\sigma S_1 = \sigma(\vee E_1) = \vee \sigma E_1 = \vee E_2 = S_2 \qquad \blacksquare$$

Recall that if $F < E$ is algebraic then E is an algebraic closure of F if and only if any nonconstant polynomial p(x) over F splits in E. Perhaps the next best thing would be that every irreducible polynomial p(x) over F that has one root in E splits in E. This property happens to characterize splitting fields.

Theorem 2.9.3 Let $F < E$ be algebraic and let $F < E < \overline{F}$. The following are equivalent.

1) E is a splitting field for a family $\mathfrak{F}$ of polynomials over F.
2) Every embedding of E into $\overline{F}$ over F is an automorphism of E.
3) Every irreducible polynomial over F that has one root in E splits in E.

Proof. [1⇒2] Let σ be an embedding of E into $\overline{F}$ over F. Since E is a splitting field for a family $\mathfrak{F}$ of polynomials over F, we have $E = F(R)$, where R is the set of roots of the members of $\mathfrak{F}$. Since σ acts as a permutation on the roots of any member of $\mathfrak{F}$, we have $\sigma R = R$ and so

$$\sigma E = \sigma(F(R)) = F(\sigma R) = F(R) = E$$

[2⇒3] Let f(x) be an irreducible polynomial over F, with a root α in E. According to Theorem 2.8.4, if $\beta \in \overline{F}$ is a root of f(x), then the injection $j:F \to \overline{F}$ can be extended to an embedding $\sigma:E \to \overline{F}$ for which $\sigma\alpha = \beta$. By hypothesis, σ is an automorphism of E, whence β is also in E. Thus, f(x) splits in E.

[3⇒1] This follows immediately, since E is a splitting field for the family $\mathfrak{F} = \{min(\alpha,F) \mid \alpha \in E\}$. $\blacksquare$

Definition An algebraic extension $F < E$ that satisfies any (and hence all) of the conditions in the previous theorem is said to be a **normal extension.** We also say that E is **normal over** F. □

Corollary 2.9.4 If $F < E$ is a finite normal extension then E is the splitting field of a finite family of irreducible polynomials.

Proof. Let $E = F(\alpha_1,\ldots,\alpha_n)$. Since E is normal over F, each minimal polynomial $min(\alpha_i,F)$ splits in E. Clearly, E is generated by the roots of $min(\alpha_i,F)$ and so E is the splitting field of the finite family $\{min(\alpha_i,F)\}$. ∎

Note that any extension $F < E$, with E algebraically closed, is normal since *any* nonconstant $p(x) \in F[x]$ splits in E.

As it happens, the class of normal extensions is not distinguished.

Example 2.9.1 It is not hard to see that any extension of degree 2 is normal. The extension $\mathbb{Q} < \mathbb{Q}(\sqrt[4]{2})$ is not normal since $\mathbb{Q}(\sqrt[4]{2})$ contains exactly two of the four roots of $x^4 - 2$, which is irreducible over $\mathbb{Q}$. On the other hand,

$$\mathbb{Q} < \mathbb{Q}(\sqrt{2}) < \mathbb{Q}(\sqrt[4]{2})$$

with each step of degree 2 and therefore normal. As another example, since $\mathbb{C}$ is algebraically closed, $\mathbb{Q} < \mathbb{C}$ is normal but $\mathbb{Q} < \mathbb{Q}(\sqrt[4]{2})$ is not normal. □

The previous example notwithstanding, many of the properties that define distinguished classes do hold for normal extensions.

Theorem 2.9.5

1) If $F < E$ is normal and $F < K < E$ then $K < E$ is also normal.
2) The class of normal extensions is closed under lifting: If $F < E$ is normal and $F < K$ is any extension then $K < EK$ is normal.
3) The class of normal extensions is closed under the taking of arbitrary composites and intersections: If $\{E_i\}$ is a family of fields, each normal over F, and each contained in a single larger field, then $\bigvee E_i$ is normal over F and $\bigcap E_i$ is normal over F.

Proof. Part 1) follows from the fact that a splitting field for a family of polynomials over F is also a splitting field for the same family of polynomials over K. For part 2), let E be a splitting field for a family $\mathcal{F}$ of polynomials over F and let R be the set of roots in E of all polynomials in $\mathcal{F}$. Then $E = F(R)$. Hence, $EK = K(R)$, which shows that EK is a splitting field for the family $\mathcal{F}$, thought of as a family of

polynomials over K. Hence, $K < EK$ is normal. For part 3), let $\sigma: \vee E_i \to \overline{F}$ be an embedding over F. Then σ is an embedding when restricted to each E_i and so $\sigma E_i = E_i$, whence

$$\sigma(\vee E_i) = \vee \sigma E_i = \vee E_i$$

and

$$\sigma(\bigcap E_i) = \bigcap \sigma E_i = \bigcap E_i \quad \blacksquare$$

Normal Closures

Definition Let $F < E$ be algebraic and let $\overline{F}$ be an algebraic closure of F containing E. The **normal closure** of $F < E$ in $\overline{F}$ is the intersection of all fields L such that $E < L < \overline{F}$ and $F < L$ normal. We denote this field by E^{nc}. □

Note that since $F < \overline{F}$ is normal, the intersection described in the previous definition is a nontrivial one.

Theorem 2.9.6 Let $F < E < \overline{F}$ be algebraic, with normal closure E^{nc}.

1) E^{nc} is the smallest subfield of $\overline{F}$ with the property that $E < E^{nc}$ and $F < E^{nc}$ is normal.
2) $E^{nc} = \vee \sigma E$, over all $\sigma \in Hom_F(E,\overline{F})$.
3) E^{nc} is the splitting field in $\overline{F}$ of the family $\{min(\alpha,F) \mid \alpha \in E\}$.
4) E^{nc} is the splitting field in $\overline{F}$ of the family $\{min(\alpha,F) \mid \alpha \in B\}$ where B is a basis for E over F.
5) If $F < E$ is finite, then $F < E^{nc}$ is also finite.

Proof. We prove only part 2), leaving the rest for the reader. Let $E < L < \overline{F}$ with $F < L$ normal. Since $E < L$ is algebraic, any $\sigma \in Hom_F(E,\overline{F})$ may be extended to an embedding $\tau: L \to \overline{F}$ over F. Since $F < L$ is normal, τ is an automorphism of L. It follows that $\sigma E \subseteq L$ and so $\vee \sigma E < E^{nc}$. On the other hand, if we let $L = \vee \sigma E$, then $F < L$ is normal since if $\tau \in Hom_F(L,\overline{F})$ then $\tau\sigma$ runs over all elements of $Hom_F(L,\overline{F})$ as σ does and so

$$\tau L = \tau(\vee \sigma E) = \vee \tau\sigma(E) < \vee \sigma E = L$$

Since $F < L$ is algebraic, we deduce that $\tau L = L$, that is, τ is an automorphism of L over F. Hence, $F < L$ is normal and so $E^{nc} < L = \vee \sigma E$. This shows that $\vee \sigma E = E^{nc}$. ∎

Exercises

1. Let R be an integral domain containing a field F. Show that if $[R:F] < \infty$ then R must be a field.
2. If $F < E$ is algebraic and R is a ring such that $F \subseteq R \subseteq E$, show that R is a field. Is this true if $F < E$ is not algebraic?
3. Let $F < E$ and $F < K$ be finite extensions and assume that EK is defined. Show that $[EK:F] \leq [E:F][K:F]$, with equality if [E:F] and [K:F] are relatively prime.
4. Let $\sigma: K \to E$ be a homomorphism of fields and let $F < K \cap E$. Show that σ is F–linear if and only if $\sigma(a) = a$ for all $a \in F$.
5. Let $F < E$ be a *quadratic extension*, that is, an extension of degree 2. Show that E has a basis over F of the form $\{1,a\}$ where $a^2 \in F$.
6. Prove that any extension of degree 2 is normal.
7. Let F be an infinite field and let $F < E$ be an algebraic extension. Show that $|E| = |F|$.
8. Let $F < \overline{F}$ where $\overline{F}$ is an algebraic closure of F and let $G = Aut_F(\overline{F})$ be the group of all automorphism of $\overline{F}$ fixing F pointwise. Let
$$\overline{F}^G = \{a \in \overline{F} \mid \sigma a = a \text{ for all } \sigma \in G\}$$
be the *fixed field* of F under G. Evidently $F < \overline{F}^G < \overline{F}$. Show that the minimal polynomial of any $\alpha \in \overline{F}^G$ over F has only one distinct root in $\overline{F}$. Show also that the minimal polynomial of any $\alpha \in \overline{F}$ over $\overline{F}^G$ has no multiple roots. *Hint*: for the latter statement, consider the polynomial $p(x) = \prod (x - a_i)$ where a_i are the *distinct* roots of $min(\alpha, \overline{F}^G)$.
9. Let p be a prime and let $\alpha \neq 1$ be a complex p-th root of unity. Show that $min(\alpha,\mathbb{Q}) = 1 + x + x^2 + \cdots + x^{p-1}$. What is the splitting field for $x^p - 1$ over $\mathbb{Q}$?
10. Suppose that $F < E$ is a finite extension and that $E = F(S)$ for some set $S \subseteq E$. Must there exist a finite subset $S_0 \subseteq S$ for which $E = F(S_0)$?
11. Let F be a field of characteristic $p \neq 0$ and let $\alpha \in F$. Show that the following are equivalent: (i) $\alpha^{p^k} \in F$ (ii) $F(\alpha^{p^k}) = F$ (iii) $[F(\alpha)]^{p^k} \subseteq F$ where $[F(\alpha)]^{p^k} = \{s^{p^k} \mid s \in F(\alpha)\}$.
12. Let $F < E$ be a finite normal extension and let $p(x) \in F[x]$ be irreducible. Suppose that the polynomials f(x) and g(x) are monic irreducible factors of p(x) over E. Show that there exists a $\sigma \in Aut_F(E)$ for which $f^\sigma(x) = g(x)$.
13. Let $F < E$ be algebraic. Show that a normal closure for $F < E$ exists and that any two normal closures are isomorphic over F. Show also that if $F < E$ is finite, so is $F < E^{nc}$. If $F < E$ is algebraic and $\sigma \in Hom_F(E,\overline{E})$ then $Im\,\sigma$ is contained in the normal closure of $F < E$ that lies in $\overline{E}$.

14. Let F be a field and let $\alpha_1,\ldots,\alpha_n$ be distinct elements of F. Prove that if $a_1\alpha_1^k+\cdots+a_n\alpha_n^k=0$ for all integers $k\geq 0$ then $a_i=0$ for all i.
15. Show that an extension $F<E$ is algebraic if and only if any subalgebra S of E over F is actually a subfield of E.
16. Let $F<E$ be normal. Can any automorphism of F be extended to an automorphism of E?
17. Suppose that F and E are fields and $\sigma:F\to E$ is an embedding. Construct an extension of F that is isomorphic to E.

Constructions

The goal of the following series of exercises is to prove that certain constructions are not possible using straight edge and compass alone. In particular, not all angles can be trisected, a circle cannot be "squared" and a cube cannot be "doubled." The first step is to define the term *constructible.* We assume the existence of two distinct points P_1 and P_2 and take the distance between these points to be one unit.

Definition A point, line or circle in the plane is said to be **constructible** if and only if it can be obtained by a finite number of applications of the following rules.

1) P_1 and P_2 are constructible.
2) The line through any two constructible points is constructible.
3) The circle with center at one constructible point and passing through another constructible point is constructible.
4) The points of intersection of any two constructible lines or circles are constructible. □

C1. Show that if a line L and point P are constructible, then the line through P perpendicular to L is also constructible.
C2. Show that if a line L and point P are constructible, then the line through P parallel to L is also constructible.
C3. Taking the constructible line through P_1 and P_2 as the x-axis and the point P_1 as the origin, the y-axis is also constructible. Show that any point (a,b) with integer coordinates is constructible.
C4. Show that the perpendicular bisector of any line segment connecting two constructible points is constructible.
C5. If P, Q and R are constructible points and L is a constructible line through R then a point S can be constructed on L such that the distance from S to R is the same as the distance from P to Q. (Thus, given distances can be marked off on constructible lines.)

Definition A real number r is **constructible** if its absolute value is the distance between two constructible points. □

C6. Show that any integer is constructible.

C7. Prove that a point (a,b) is constructible if and only if its coordinates a and b are constructible real numbers.

C8. Prove that the set of numbers that are constructible forms a subfield of the real numbers containing $\mathbf{Q}$. *Hint*: to show that the product of two constructible numbers is constructible or that the inverse of a nonzero constructible number is constructible, use similar triangles.

C9. Prove that if $\alpha > 0$ is constructible, then so is $\sqrt{\alpha}$. *Hint*: first show that a circle of diameter $1 + \alpha$ is constructible and that a line L through the center of the circle is constructible. Let P and Q be the intersection points of the circle with the line L. Mark off α units along the diameter PQ from P and denote that point by R. Is R constructible? Construct a line M through R perpendicular to L. Let S be one point of intersection of M and the circle. What is the length of the line segment RS?

The two previous exercises prove the following theorem.

Theorem C1 If the elements of a field $F < \mathbb{R}$ are constructible, and if $\alpha \in F$, then $F(\sqrt{\alpha}) = \{a + b\sqrt{\alpha} \mid a, b \in F\}$ is constructible. □

Theorem C2 Let F be a subfield of $\mathbb{R}$ and let $E > F$ be a quadratic extension. Then $E = F(\sqrt{\alpha})$ for some $\alpha \in F$.

Proof. Exercise. ∎

It follows from the two previous theorems that if F is constructible and if $F < E$ is a quadratic extension then E is constructible. More generally, we have

Theorem C3 If $\mathbf{Q} < E_1 < E_2 < \cdots < E_n$ is a tower of fields, each one a quadratic extension of the previous one then every element of E_n is constructible. □

We now turn to a converse of Theorem C3.

Theorem C4 Let four constructible points, whose coordinates lie in a field $F < \mathbb{R}$, be given. Let L and M be lines or circles constructed from these points. Then the points of intersection of L and M have coordinates in a quadratic extension of F.

Proof. Exercise. ∎

The import of the previous theorem is that each time we construct a constructible number α, the number lies in a quadratic extension of the

field of previously constructed numbers. Thus, we have

Theorem C5 A real number is constructible if and only if it lies in a field E_n that is at the top of a tower of fields

$$\mathbb{Q} < E_1 < E_2 < \cdots < E_n$$

each one a quadratic extension of the previous one. Hence, if α is constructible, then $[\mathbb{Q}(\alpha):\mathbb{Q}]$ must be a power of 2. □

Now consider what it means to say that an angle of θ° is constructible. Informally, we will take this to mean that we may construct a line L through the origin that makes an angle of θ° with the x-axis.

C10. Show that such a line L is constructible if and only if the real number $\cos \theta^\circ$ is constructible. (This is an informal demonstration, since we have not formally defined angles.)

The previous exercise prompts us to make the following definition.

Definition An angle of θ° is **constructible** if the real number $\cos \theta$ is constructible. □

C11. Show that a 60° angle is constructible.

C12. Show that a 20° angle is not constructible. *Hint*: verify the formula

$$\cos 3\theta = 4 \cos^3 \theta - 3 \cos \theta$$

Let $\tau = \cos 20^\circ$ and show that τ is a root of

$$p(x) = 8x^3 - 6x - 1$$

Show that p(x) is irreducible over $\mathbb{Q}$ and so $[\mathbb{Q}(\tau):\mathbb{Q}] = 3$.

C13. Prove that every constructible real number is algebraic over $\mathbb{Q}$. Assuming that π is transcendental over $\mathbb{Q}$, show that any circle with a constructible radius cannot be "squared," that is, a square cannot be constructed whose area is that of a unit circle.

C14. Verify that it is impossible to "double" any cube whose side length r is constructible, that is, it is impossible to construct an edge of a cube whose volume is twice that of a cube with side length r.

Chapter 3
Algebraic Independence

In this chapter, we discuss the structure of an arbitrary field extension $F < E$. Specifically, we will see that, for any extension $F < E$, there exists an intermediate field $F < F(S) < E$ whose second step $F(S) < E$ is algebraic and whose first step $F < F(S)$ is *purely transcendental.* The latter means that there is no nontrivial polynomial dependency (over F) among the elements of S, and so these elements act as "independent variables" over F. Thus, F(S) is the field of all rational functions in these variables.

3.1 Dependence Relations

We begin with a general notion of dependence, intended to model linear independence.

Definition Let X be a nonempty set and let $\Delta \subseteq X \times \mathcal{P}(X)$ be a binary relation from X to the power set of X. We write $x \prec S$ (read: x is **dependent on** S) for $(x,S) \in \Delta$ and $S \prec T$ when $s \prec T$ for all $s \in S$. Then Δ is a **dependence relation** if it satisfies the following properties, for all S, T and $U \in \mathcal{P}(X)$,

1) (**reflexivity**)

$$S \prec S$$

2) (**compactness**)

$$x \prec S \Rightarrow x \prec S_0 \text{ for some finite subset } S_0 \text{ of } S$$

3) **(transitivity)**

$$S \prec T,\ T \prec U \Rightarrow S \prec U$$

4) **(Steinitz exchange axiom)**

$$x \prec S,\ x \not\prec S - \{s\} \Rightarrow s \prec (S - \{s\}) \cup \{x\}$$

If $x \not\prec S$ we say that x is **independent of** S. □

Definition A subset $S \subseteq X$ is **dependent** if $s \prec S - \{s\}$ for some $s \in S$ (equivalently, if $S \prec S - \{s\}$). A subset $S \subseteq X$ is **independent** if $s \not\prec S - \{s\}$ for all $s \in S$. (Hence the empty set is independent.) □

The reader should have no trouble supplying a proof for the following lemma.

Lemma 3.1.1

1) If $S \prec T$ then $S \prec T'$ for any superset T' of T.
2) Any superset of a dependent set is dependent.
3) Any subset of an independent set is independent.
4) If S is a dependent set, then some finite subset S_0 of S is dependent. Equivalently, if every finite subset of T is independent, then T is independent. □

Theorem 3.1.2 If S is independent and $x \not\prec S$ then $S \cup \{x\}$ is independent.

Proof. Let $s \in S$. If $s \prec (S \cup \{x\}) - \{s\}$ then since $s \not\prec S - \{s\}$, the exchange axiom would imply that $x \prec S$, a contradiction. Hence $s \not\prec (S \cup \{x\}) - \{s\}$. Furthermore, by hypothesis $x \not\prec S = (S \cup \{x\}) - \{x\}$. Thus, $S \cup \{x\}$ is independent. ∎

Definition A set $B \subseteq X$ is called a **base** if B is independent and $X \prec B$. □

Theorem 3.1.3 Let X be a nonempty set with a dependence relation $\prec$.

1) $B \subseteq X$ is a base for X if and only if it is a maximal independent set in X.
2) $B \subseteq X$ is a base for X if and only if B is minimal with respect to the property $X \prec B$.
3) Let $A \subseteq S \subseteq X$, where A is an independent set (possibly empty) and $X \prec S$. Then there is a base B for X such that $A \subseteq B \subseteq S$.

Proof. For part 1), assume B is a base. Then B is independent. If B is not maximal independent, there exists an $x \in X - B$ for which $B \cup \{x\}$

is independent. Hence, $x \not\prec (B \cup \{x\}) - \{x\} = B$, a contradiction to $X \prec B$. For the converse, if B is a maximal independent set and $x \not\prec B$ then $B \cup \{x\}$ is independent, which is not the case. Hence, $X \prec B$ and B is a base.

For part 2), if B is a base, then $X \prec B$. Suppose that some proper subset $B_0 \subset B$ satisfies $X \prec B_0$. If $b \in B - B_0$ then $b \prec B_0 \prec B - \{b\}$, contracting the independence of B. Hence B is minimal. Conversely, suppose that B is minimal with respect to the property $X \prec B$. If B is dependent then $X \prec B \prec B - \{b\}$ for some $b \in B$, a contradiction to the minimality of B. Hence B is independent and a base for X.

For part 3), we apply Zorn's lemma. The set $\mathcal{I}$ of all independent sets B in X satisfying $A \subseteq B \subseteq S$ is nonempty, since $A \in \mathcal{I}$. Order $\mathcal{I}$ by set inclusion. If $\mathcal{C} = \{C_i\}$ is a chain in $\mathcal{I}$, then the compactness property implies that the union $\bigcup C_i$ is an independent set, which also lies in $\mathcal{I}$. Hence, Zorn's lemma implies the existence of a maximal element $C \in \mathcal{I}$, that is, C is independent, $A \subseteq C \subseteq S$ and C is maximal with respect to these two properties. This maximality implies that $S \prec C$ and so $X \prec S \prec C$, which implies that C is a base. ∎

To prove that any two bases for X have the same cardinality, we require a lemma.

Lemma 3.1.4 Let S be a finite dependent set and let $A \subseteq S$ be an independent subset of S. Then there exists $\alpha \in S - A$ for which $S \prec S - \{\alpha\}$.

Proof. Among all subsets of $S - A$, choose a maximal one B for which $A \cup B$ is independent. Then B is a proper (perhaps empty) subset of $S - A$. If $\alpha \in S - (A \cup B)$ then $\alpha \prec A \cup B \prec S - \{\alpha\}$ and so $S \prec S - \{\alpha\}$.∎

Theorem 3.1.5 Any two bases for a set X have the same cardinality.

Proof. Let B and C be bases for X. We first assume that at least one of B or C is finite; say $B = \{b_1, \ldots, b_m\}$ is finite. Choose $c_1 \in C$. The set $C_1 = \{c_1, b_1, \ldots, b_m\}$ satisfies the conditions of the previous lemma (with $A = \{c_1\}$) and so, after renumbering the b_i's if necessary, we deduce that

$$X \prec C_1 \prec \{c_1, b_1, \ldots, b_{m-1}\}$$

For any $c_2 \in C - \{c_1\}$, the set $C_2 = \{c_1, c_2, b_1, \ldots, b_{m-1}\}$ satisfies the conditions of the lemma (with $A = \{c_1, c_2\}$) and so, again after possible renumbering, we get

$$X \prec C_2 \prec \{c_1, c_2, b_1, \ldots, b_{m-2}\}$$

Continuing this process, we must exhaust all of the elements of C before running out of elements of B, for if not, then a proper subset C' of C would have the property that $X \prec C'$, in contradiction to the independence of C. Hence, $|C| \leq |B|$. Since this shows that C is finite, we may repeat the argument with the roles of B and C reversed to get $|B| = |C|$.

Let us now assume that B and C are both infinite sets, and let $C = \{c_i \mid a \in I\}$. Thus, $|C| = |I|$. For each $b \in B$, we have $b \prec C$ and so there is a finite subset $I_b \subset I$ such that $b \prec \{c_i \mid i \in I_b\}$. This gives a map $b \rightarrow I_b$ from B to the set of finite subsets of the index set I. Moreover,

$$I = \bigcup_{b \in B} I_b$$

for if $j \in I - \bigcup I_b$ then, for any $b \in B$, we have

$$b \prec \{c_i \mid i \in I_b\} \prec C - \{c_j\}$$

and so $c_j \prec B \prec C - \{c_j\}$, which contradicts the independence of C. Hence,

$$|C| = |I| = \left|\bigcup_{b \in B} I_b\right| \leq \aleph_0 |B| = |B|$$

Again reversing the roles of B and C shows that $|B| = |C|$. ∎

3.2 Algebraic Dependence

We recall a definition.

Definition Let $F < E$. An element $t \in E$ is **transcendental** over F if t is not algebraic over F, that is, if there is no nonzero polynomial $p(x) \in F[x]$ such that $p(t) = 0$. □

Recall that if t is transcendental over F then F(t) is the field of all rational functions in the variable t, over the field F.

Definition Let $F < E$ and let $S \subseteq E$. An element $\alpha \in E$ is **algebraically dependent on S over F**, written $\alpha \prec S$, if α is algebraic over F(S). If α is not algebraically dependent on S over F, that is, if α is transcendental over F(S) then α is said to be **algebraically independent of S over F** and we write $\alpha \not\prec S$. □

The first order of business is to show that algebraic dependence is a dependence relation.

Theorem 3.2.1 Algebraic dependence is a dependence relation.

Proof. Since any $s \in S$ is algebraic over $F(S)$ we have $S \prec S$. To show compactness, let $\alpha \prec S$ and let C be the set of coefficients of $min(\alpha,F(S))$. Since $C \subseteq F(S)$, each $c \in C$ is a rational function over F in a finite number of elements of S and so there is a finite subset S_0 of S for which $C \subseteq F(S_0)$. Hence α is algebraic over $F(S_0)$, that is, $\alpha \prec S_0$.

For transitivity, suppose that $\alpha \prec S$ and $S \prec T$ and consider the tower

$$F(T) < F(T \cup S) < F(T \cup S,\alpha)$$

Since every element of S is algebraic over $F(T)$, and since α is algebraic over $F(T \cup S)$ we deduce that α is algebraic over $F(T)$, whence $\alpha \prec T$.

Finally, we verify the exchange axiom. Suppose that $\alpha \prec S$ and $\alpha \not\prec S - \{s\}$. Let $p(x) = min(\alpha,F(S))$. Since $F(S) = F(S - \{s\})(s)$, the coefficients of $p(x)$ are polynomials in s over $F(S - \{s\})$, that is,

$$p(x) = \sum_{i=0}^{d} f_i(s)x^i$$

where we may assume that $f_d(x) \neq 0$. Hence, the polynomial

$$p(x,y) = \sum_{i=0}^{d} f_i(y)x^i$$

in two independent variables is not the zero polynomial. This polynomial can also be written

$$p(x,y) = \sum_{i=0}^{e} g_i(x)y^i$$

where $g_i(x) \in F(S - \{s\})[x]$ and $g_e(x) \neq 0$. Then

$$0 = p(\alpha,s) = \sum_{i=0}^{e} g_i(\alpha)s^i$$

Since $g_e(x) \in F(S - \{s\})[x]$ is nonzero and α is transcendental over $F(S - \{s\})$, we infer that $g_e(\alpha) \neq 0$ and $e > 0$. Hence, the equation above shows that $s \prec F(S - \{s\} \cup \{\alpha\})$. ∎

We may now take advantage of the results derived for dependence relations.

Definition Let $F < E$.

1) A subset $S \subseteq E$ is **algebraically dependent over F** if $s \prec S - \{s\}$ for some $s \in S$, that is, if s is algebraic over $F(S - \{s\})$ for some $s \in S$.

2) A subset $S \subseteq E$ is **algebraically independent over F** if $s \notin S - \{s\}$ for all $s \in S$, that is, if s is transcendental over $F(S - \{s\})$ for all $s \in S$. (Hence the empty set is algebraically independent over F.) □

Lemma 3.2.2

1) Any superset of an algebraically dependent set is algebraically dependent.
2) Any subset of an algebraically independent set is algebraically independent. □

Theorem 3.2.3 If S is algebraically independent over F and α is transcendental over F(S) then $S \cup \{\alpha\}$ is algebraically independent over F. □

Let us provide another characterization of algebraically dependent sets.

Theorem 3.2.4 Let $F < E$. A subset S of E is algebraically dependent over F if and only if there is some nonzero polynomial $p(x_1,\ldots,x_n)$ in $n \geq 1$ variables over F for which $p(s_1,\ldots,s_n) = 0$, for distinct $s_i \in S$.

Proof. Suppose first that S is algebraically dependent over F. Then some $s \in S$ is algebraic over $F(S - \{s\})$ and so there exists a polynomial p(x) of degree $d > 0$ over $F(S - \{s\})$ for which $p(s) = 0$. Such a polynomial has the form

$$p(x) = \sum_{i=0}^{d} \frac{p_i(s_1,\ldots,s_m)}{q_i(s_1,\ldots,s_m)} x^i$$

where $p_i(x_1,\ldots,x_m)$ and $q_i(x_1,\ldots,x_m)$ are polynomials in m variables and the $s_i \in S - \{s\}$ are distinct. Note that $p_d(s_1,\ldots,s_m) \neq 0$ and $q_i(s_1,\ldots,s_m) \neq 0$ for all i. Letting $x = s$ and clearing this of denominators gives

$$0 = \sum_{i=0}^{d} r_i(s_1,\ldots,s_m)s^i$$

for polynomials $r_i(x_1,\ldots,x_m)$, with $r_d(s_1,\ldots,s_m) \neq 0$. Thus $r_d(x_1,\ldots,x_m)$ is not the zero polynomial and $p(x) = \sum r_i(x_1,\ldots,x_m)x^i$ is a nonzero polynomial satisfied by the $m+1$ distinct elements $s_1,\ldots,s_m,s$ in S.

For the converse, suppose that $p(s_1,\ldots,s_n) = 0$ for distinct $s_i \in S$, where $p(x_1,\ldots,x_n)$ is a nonzero polynomial over F. We may assume without loss of generality that $s_2,\ldots,s_n$ do not enjoy a similar polynomial dependency and hence that

$$p(x_1,\ldots,x_n) = \sum_{i=0}^{d} p_i(x_2,\ldots,x_n)x_1^i$$

where $p_d(x_2,\ldots,x_n) \neq 0$ and $p_d(s_2,\ldots,s_n) \neq 0$. Hence the nonzero polynomial

$$p(x) = \sum_{i=0}^{d} p_i(s_2,\ldots,s_n)x^i$$

satisfies $p(s_1) = 0$, showing that s_1 is algebraic over $F(S - \{s_1\})$ and hence that S is algebraically dependent over F. ∎

Corollary 3.2.5 Let $F < E$ and let $S = \{s_1,\ldots,s_n\}$ be a subset of E. Then S is algebraically independent over F if and only if s_m is transcendental over $F(s_1,\ldots,s_{m-1})$ for all $m = 1,\ldots,n$.

Proof. If S is algebraically independent then s_m is transcendental over $F(S - \{s_m\})$ and therefore also over the smaller field $F(s_1,\ldots,s_{m-1})$. For the converse, if S is algebraically dependent then there is a nonzero polynomial dependency of the form

$$0 = \sum_{i=0}^{d} p_i(s_1,\ldots,s_{m-1})s_m^i$$

for some $m \leq n$ where $p_d(s_1,\ldots,s_{m-1}) \neq 0$, whence s_m is algebraic over $F(s_1,\ldots,s_{m-1})$. This contradiction implies that S is algebraically independent. ∎

3.3 Transcendence Bases

Definition Let $F < E$. A **transcendence basis** for E over F is a subset $B \subseteq E$ that is algebraically independent over F and for which $E \prec B$, that is, for which $F(B) < E$ is algebraic. □

Since algebraic dependence is a dependence relation, we immediately get the following two results.

Theorem 3.3.1 Let $F < E$. A subset $B \subseteq E$ is a transcendence basis for E over F if and only if it satisfies either one of the following.

1) B is a maximal algebraically independent subset of E over F.
2) B is minimal with respect to the property that $F(B) < E$ is algebraic. □

Theorem 3.3.2 Let $F < E$.

1) Any two transcendence bases for E over F have the same cardinality. This cardinality is called the **transcendence degree** of E over F, and is denoted by $[E:F]_t$.
2) Suppose $F \subseteq A \subseteq S \subseteq E$ where A is algebraically independent over F and $F(S) < E$ is algebraic. Then there exists a transcendence basis B for E over F satisfying $A \subseteq B \subseteq S$. In particular, $[E:F]_t \leq |S|$. □

Definition An extension $F < E$ is said to be **purely transcendental** if $E = F(B)$ for some transcendence basis B for E over F. □

We remark that if E is purely transcendental over F then $E = F(B)$ for *some* transcendence basis B, but not all transcendence bases for E over F need generate E. The reader is asked to supply an example in the exercises.

The following few simple results concerning transcendental extensions will prepare the way to finishing the proof (promised in Chapter 2) that the class of finitely generated extensions is distinguished.

Corollary 3.3.3 If E is finitely generated over F and B is a transcendence basis for E over F then B is a finite set and $F(B) < E$ is a finite extension.

Proof. Theorem 3.3.2 implies that B is finite. The second part follows from the fact that E is finitely generated over F(B) as well, and a finitely generated algebraic extension is finite. ∎

Theorem 3.3.4 Let $F < K < E$ and suppose that $F < K$ is algebraic. If $T \subseteq E$ is algebraically independent over F, then T is also algebraically independent over K. In other words, T remains algebraically independent over any algebraic extension of the base field.

Proof. If T is not algebraically independent over K, there exists $t \in T$ algebraic over $K(T - \{t\})$. Since $F < K$ is algebraic, we deduce that $F(T - \{t\}) < K(T - \{t\})$ is algebraic, and so each step in the tower

$$F(T - \{t\}) < K(T - \{t\}) < K(T - \{t\})(t) = K(T)$$

is algebraic, whence $t \in K(T)$ is algebraic over $F(T - \{t\})$, in contradiction to the algebraic independence of T over F. ∎

We are now in a position to finish the proof that the class of finitely generated extensions is distinguished. Note how much more involved

this task is than showing that finite or algebraic extensions are distinguished.

Theorem 3.3.5 Let $F < K < E$. If E is finitely generated over F then K is also finitely generated over F. Thus, the set of finitely generated extensions is distinguished.

Proof. Let $S = \{s_1,\ldots,s_k\}$ be a transcendence basis for K over F. Then the second step in the tower $F < F(S) < K < E$ is algebraic and E is finitely generated over F(S). Hence, if we can prove the theorem for algebraic intermediate fields, we will know that K is finitely generated over F(S) and therefore also over F, since S is a finite set.

Thus, we may assume that $F < K < E$ with $F < K$ algebraic and show that [K:F] is finite. Let $T = \{t_1,\ldots,t_n\}$ be a transcendence basis for E over F. Our plan is to show that

$$[K:F] \leq [E:F(T)]$$

(see Figure 3.3.1) by showing that any finite subset of K that is linearly independent over F is also linearly independent over F(T) [as a subset of E]. Since [E:F(T)] is finite by Corollary 3.3.3, the proof will be complete.

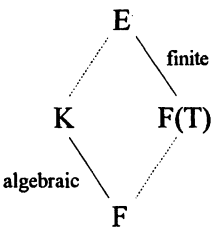

Figure 3.3.1

First, we observe that, by Theorem 3.3.4, since T is algebraically independent over F, it is also algebraically independent over the algebraic extension K of F.

Let $Y = \{y_1,\ldots,y_m\} \subseteq K$ be linearly independent over F. Suppose that

$$\sum r_i(t_1,\ldots,t_n)y_i = 0$$

where $r_i(t_1,\ldots,t_n) \in F(T)$. By clearing denominators if necessary, we may assume that each $r_i(t_1,\ldots,t_n)$ is a polynomial over F. Collecting terms involving like powers of the t_i's gives

$$\sum_{e_1,\ldots,e_n}\Big(\sum_i a_{e_1,\ldots,e_n,i}\,y_i\Big)\,t_1^{e_1}\cdots t_n^{e_n}=0$$

where $a_{e_1,\ldots,e_n,i}\in F$ is the coefficient of $t_1^{e_1}\cdots t_n^{e_n}$ in $r_i(t_1,\ldots,t_n)$. Since T is algebraically independent over K, the products $t_1^{e_1}\cdots t_n^{e_n}$ are linearly independent over K, and hence also over $F(y_1,\ldots,y_m)\subseteq K$. Thus

$$\sum_i a_{e_1,\ldots,e_n,i}\,y_i=0$$

and the linear independence of Y over F then implies that

$$a_{e_1,\ldots,e_n,i}=0$$

Hence $r_i(t_1,\ldots,t_n)=0$ for all i. This shows that Y is linearly independent over F(T), as desired. ∎

The next theorem gives some verisimilar facts about simple transcendental extensions; in particular, if $E=F(t)$, where t is transcendental over F, then any nonconstant rational function in t is also transcendental over F and E is algebraic over any intermediate field other than the base field F.

Theorem 3.3.6

1) Suppose that $E=F(t)$, where t is transcendental over F. If $s=f(t)/g(t)\in F(t)$ where f(t) and g(t) are relatively prime and at least one is nonconstant, then s is transcendental over F, t is algebraic over F(s) and $[F(t):F(s)]=max(deg\ f(t),\ deg\ g(t))$.
2) If t is transcendental over F then F(t) is algebraic over any field K satisfying $F<K<F(t)$, $K\neq F$.
3) If $F<E$ is purely transcendental then any $\alpha\in E-F$ is transcendental over F.

Proof. For 1), if we show that t is algebraic over F(s), it will follow that s is transcendental over F, for otherwise $F<F(s)<F(t)$ would be an algebraic tower. The polynomial

$$p(x)=g(x)s-f(x)\in F(s)[x]$$

has the property that $p(t)=g(t)s-f(t)=0$. Moreover, p(x) is irreducible over F(s). For if we think of p(x) as a polynomial in the two (independent) variables x and s, it is clear that if p(x) has a nontrivial factorization, one of the factors must be a nontrivial common factor of f(x) and g(x), which is impossible. Since

$$deg\ p(x) = max(deg\ f(x),\ deg\ g(x))$$

part 1) is proved. Part 2) follows easily from part 1).

For part 3), if $\alpha \in E - F$ then $\alpha \in F(t_1,\ldots,t_n)$ for some finite set $\{t_1,\ldots,t_n\}$ of algebraically independent elements. By part 1), every element of $F(t_1)$ not in F is transcendental over F. Similarly, every element of $F(t_1,t_2)$ not in $F(t_1)$ is transcendental over $F(t_1)$ and hence also over F. Continuing this argument gives the desired result. ∎

We leave it as an exercise to show that the converse of part 3) is false, that is, there exist extensions $F < E$ that are not purely transcendental but for which every $\alpha \in E - F$ is transcendental over F.

The following is an example of an extension that is neither algebraic nor purely transcendental.

Example 3.3.1 Let $n \geq 3$ and let F be a field with $char(F) \nmid n$. Let u be transcendental over F, let v be a root of $p(x) = x^n + u^n - 1$ in some splitting field and let $E = F(u,v)$. Clearly, E is not algebraic over F. We contend that E is also not purely transcendental over F. Since v is algebraic over F(u), we deduce that $\{u\}$ is a transcendence basis for E over F and so $[E:F]_t = 1$. If E were purely transcendental over F there would exist a transcendental element t over F for which $F(t) = F(u,v)$. Let us show that this is not possible.

If $F(t) = F(u,v)$ then

$$u = \frac{a(t)}{b(t)} \quad \text{and} \quad v = \frac{c(t)}{d(t)}$$

where a(t), b(t), c(t) and d(t) are polynomials over F. Hence

$$\frac{a^n(t)}{b^n(t)} + \frac{c^n(t)}{d^n(t)} = 1$$

or

$$[a(t)d(t)]^n + [b(t)c(t)]^n = [b(t)d(t)]^n$$

This can be written

$$f^n(t) + g^n(t) = h^n(t)$$

for nonconstant polynomials f(t), g(t) and h(t), which we may assume to be pairwise relatively prime. Let us assume that $deg\ f(t) \leq deg\ g(t)$, in which case $deg\ h(t) \leq deg\ g(t)$. We now divide by $h^n(t)$ and take the derivative with respect to t to get (after some simplification)

$$f^{n-1}[f'h - fh'] + g^{n-1}[g'h - gh'] = 0$$

Since f and g are relatively prime, we deduce that $g^{n-1} \mid f'h - fh'$. But this implies

$$(n-1)deg\, g \leq deg\, fh - 1 = deg\, f + deg\, h - 1 \leq 2deg\, g - 1$$

which is not possible for $n \geq 3$. Hence, $F < F(u,v)$ is not purely transcendental. □

While the vector space dimension is multiplicative over a tower of fields, the transcendence degree is additive, as we see in the next theorem.

Theorem 3.3.7 Let $F < K < E$.

1) If $S \subseteq K$ is algebraically independent over F and $T \subseteq E$ is algebraically independent over K then $S \cup T$ is algebraically independent over F.
2) If S is a transcendence basis for K over F and T is a transcendence basis for E over K then $S \cup T$ is a transcendence basis for E over F.
3) $[E:F]_t = [E:K]_t + [K:F]_t$

Proof. For part 1), suppose for the purposes of contradiction that $S \cup T$ is algebraically dependent over F. Then there exists an $\alpha \in S \cup T$ that is algebraic over $F(S_0 \cup T_0)$ for some finite sets $S_0 \subseteq S$ and $T_0 \subseteq T$ not containing α, and we may assume that no proper subset T_1 of T_0 has the property that α is algebraic over $F(S_0 \cup T_1)$. If $\alpha \in T$ then since α is algebraic over $F(S_0 \cup T_0)$, it is also algebraic over the larger field $K(T - \{\alpha\})$, in contradiction to the algebraic independence of T over K. Hence $\alpha \notin T$ and so $\alpha \in S$. But then T_0 cannot be empty, since S is algebraically independent over F. If $t \in T_0$ then the minimality of T_0 implies that α is not algebraic over $S_0 \cup T_0 - \{t\}$, that is, $\alpha \not\prec S_0 \cup T_0 - \{t\}$. But $\alpha \prec S_0 \cup T_0$ and so the exchange axiom gives $t \prec S_0 \cup T_0 \cup \{\alpha\} - \{t\}$. In other words, t is algebraic over $F(S_0 \cup T_0 \cup \{\alpha\} - \{t\})$, and hence also over the larger field $K(T - \{t\})$, again contradicting the algebraic independence of T over K. This proves part 1).

For part 2), we know by part 1) that $S \cup T$ is algebraically independent over F. Also, since $F(S) < K$ and $K(T) < E$ are algebraic, each step in the tower $F(S \cup T) < K(T) < E$ is algebraic and so $F(S \cup T) < E$ is algebraic. Hence, $S \cup T$ is a transcendence basis for F over E. Part 3) follows directly from part 2). ∎

*3.4 Simple Transcendental Extensions

The class of purely transcendental extensions is much less well behaved than the class of algebraic extensions. For example, let t be transcendental over F. Then in the tower $F < F(t^2) < F(t)$, the extension $F < F(t)$ is purely transcendental (and simple) but the second step $F(t^2) < F(t)$ is not transcendental at all.

In addition, if $F < E$ is purely transcendental and $F < K < E$, it does not necessarily follow that the first step $F < K$ is purely transcendental. However, this is true for simple transcendental extensions. The proof of this simple statement illustrates some of the apparent complexities in dealing with transcendental extensions.

Theorem 3.4.1 (Luroth's Theorem) Let t be transcendental over F. If $F < K < F(t)$ and $K \neq F$ then $K = F(s)$ for some $s \in F(t)$.

Proof. The idea behind the proof is straightforward. Since $K \neq F$, we know by Theorem 3.3.6 that $K < F(t)$ is algebraic. Indeed, for any $s \in K - F$, the tower $F(s) < K < F(t)$ is algebraic. We want to find an $s \in K - F$ for which $[F(t):F(s)] = [F(t):K]$, showing that $K = F(s)$. Recall from Theorem 3.3.6 that if $s = f(t)/g(t) \in K - F$ where f and g are relatively prime polynomials over F, then

$$d_s = [F(t):F(s)] = max(deg\ f(x), deg\ g(x))$$

Let

$$p(x) = min(t,K) = x^n + \frac{a_1(t)}{b_1(t)}x^{n-1} + \cdots + \frac{a_n(t)}{b_n(t)}$$

where $a_i(t)$, $b_i(t) \in F(t)$. Then $[F(t):K] = n$ and we wish to show that $d_s = n$ for some $s \in K - F$. Evidently $d_s \geq n$ for all $s \in K - F$.

Note that since t is not algebraic over F, not all of the coefficients of p(x) can lie in F. Therefore, we may let

$$s = \frac{a_k(t)}{b_k(t)} \in K - F$$

for some k and assume that $a_k(t)$ and $b_k(t)$ are relatively prime. Consider the polynomial

$$h(x) = a_k(x) - \frac{a_k(t)}{b_k(t)}b_k(x)$$

Since $s \notin F$, we have $h(x) \neq 0$. But $h(t) = 0$ and so $p(x) \mid h(x)$ over K. In other words, there exists $q(x) \in K[x]$ such that

$$a_k(x) - \frac{a_k(t)}{b_k(t)}b_k(x) = q(x)p(x)$$

or

$$a_k(x)b_k(t) - a_k(t)b_k(x) = b_k(t)q(x)p(x)$$

Multiplying both sides of this by

$$r(t) = b_1(t)\cdots b_n(t)$$

gives

$$r(t)[a_k(x)b_k(t) - a_k(t)b_k(x)] = b_k(t)q(x)r(t)p(x) \tag{3.4.1}$$

where

$$r(t)p(x) = b_1(t)\cdots b_n(t)x^n + \sum_{i=1}^{n}[b_1(t)\cdots b_{i-1}(t)a_i(t)b_{i+1}(t)\cdots b_n(t)]x^{n-i}$$

Now, we wish to factor out the greatest common divisor g(t) of the coefficients of x^j (for $j = 0,\ldots,n$) from the right side of this expression. Note that g(t) divides the gcd of any two of these coefficients, in particular, g(t) divides the gcd of

$$b_1(t)\cdots b_n(t) \quad \text{and} \quad b_1(t)\cdots b_{k-1}(t)a_k(t)b_{k+1}(t)\cdots b_n(t)$$

which is $b_1(t)\cdots b_{k-1}(t)b_{k+1}(t)\cdots b_n(t)$, since $a_k(t)$ and $b_k(t)$ are relatively prime. Hence, once g(t) is factored out of r(t)p(x):

$$r(t)p(x) = g(t)p'(t,x)$$

where $p'(t,x) \in F[t,x]$ is *primitive*, in the sense that it is not divisible by any nonconstant polynomial in t, we still have as factors among the coefficients of p'(t,x) the polynomials $b_k(t)$ and $a_k(t)$. Thus, the degree of p'(t,x) with respect to t satisfies

$$t\text{-}deg(p'(t,x)) \geq max(deg\ a_k(t), deg\ b_k(t)) = d_s \tag{3.4.2}$$

Thus, (3.4.1) becomes

$$r(t)[a_k(x)b_k(t) - a_k(t)b_k(x)] = b_k(t)q(x)g(t)p'(t,x) \tag{3.4.3}$$

Next we multiply both sides of (3.4.3) by a polynomial u(t) that will clear all of the denominators of q(x), giving

$$u(t)r(t)[a_k(x)b_k(t) - a_k(t)b_k(x)] = b_k(t)q'(t,x)p'(t,x)$$

where $p'(t,x)$, $q'(t,x) \in F[t,x]$. Since p'(t,x) is not divisible by any nonconstant polynomial in t, we must have $u(t)r(t) \mid b_k(t)q'(t,x)$. Hence, there exists a polynomial $q''(t,x) \in F[t,x]$ for which

$$a_k(x)b_k(t) - a_k(t)b_k(x) = q''(t,x)p'(t,x) \tag{3.4.4}$$

Now, the t–degree of the left hand side of this equation is at most

$$max(deg\ a_k(t), deg\ b_k(t)) = d_s$$

and by (3.4.2) the t–degree of the right hand side is at least d_s. Hence, the t–degree of either side of (3.4.4) is d_s and (3.4.2) implies that $t\text{–}deg(q''(t,x)) = 0$, that is

$$a_k(x)b_k(t) - a_k(t)b_k(x) = q''(x)p'(t,x) \tag{3.4.5}$$

where $q''(x) \in F[x]$. Since the right side of (3.4.5) is not divisible by any nonconstant polynomial in t, neither is the left side. But the left side is symmetric in x and t, so it cannot be divisible by any nonconstant polynomial in x either. Hence, $q''(x)p'(t,x)$ is not divisible by any nonconstant polynomial in x, implying that $q''(x) \in F$, that is,

$$a_k(x)b_k(t) - a_k(t)b_k(x) = q''p'(t,x) \tag{3.4.6}$$

where $q'' \in F$. Finally, since the x–degree and t–degree of the left side of (3.4.6) agree, this is also true of the right side. Hence by (3.4.2),

$$n = x\text{–}deg(p'(t,x)) = t\text{–}deg(p'(t,x)) \geq d_s \geq n$$

Thus, $d_s = n$, and the proof is complete. ∎

It can be shown that Luroth's theorem does not extend beyond simple transcendental extensions, but a further discussion of this topic would go beyond the intended scope of this book.

We conclude with a determination of all F-automorphisms of a simple transcendental extension F(t). Let $GL_n(F)$ denote the group of all nonsingular $n \times n$ matrices over F. The proof provides a nice application of Theorem 3.3.6.

Theorem 3.4.2 Let $F < F(t)$ be a simple transcendental extension and let $Aut_F(F(t))$ denote the group of all automorphism of F(t) over F

1) For each $A = \begin{bmatrix} a & b \\ c & d \end{bmatrix} \in GL_2(F)$ there is a unique $\sigma_A \in Aut_F(F(t))$ for which

$$\sigma_A : t \to \frac{at + b}{ct + d}$$

Moreover, all automorphisms of F(t) over F have the form σ_A for some $A \in GL_2(F)$.

2) If $A,B \in GL_2(F)$, then

$$\sigma_{AB} = \sigma_A \sigma_B \quad \text{and} \quad \sigma_{A^{-1}} = \sigma_A^{-1}$$

and $\sigma_A = \sigma_B$ if and only if AB^{-1} is a nonzero scalar matrix. In other words, the map $\tau: GL_2(F) \to Aut_F(F(t))$ defined by $\tau A = \sigma_A$ is an epimorphism with kernel equal to the group of all nonzero scalar matrices in $GL_2(F)$.

Proof. Clearly, the map σ_A can be extended to a homomorphism of F(t) over F by setting

$$\sigma_A\left(\frac{f(t)}{g(t)}\right) = \frac{f(\sigma_A(t))}{g(\sigma_A(t))}$$

Since $max(deg(at+b), deg(ct+d)) = 1$, Theorem 3.3.6 implies that $[F(t):F(\sigma_A t)] = 1$ and so $\sigma_A(F(t)) = F(\sigma_A t) = F(t)$, showing that σ_A is surjective. Since σ_A is injective as well (fields have no nontrivial ideals), it is an automorphism of F(t) over F.

We leave it to the reader to show that $\sigma_A \sigma_B = \sigma_{AB}$ and that $\sigma_C = \iota$ if and only if C is a scalar multiple of the identity matrix. It follows that

$$\sigma_A \sigma_{A^{-1}} = \sigma_\iota = \iota \quad \text{and} \quad \sigma_{A^{-1}} \sigma_A = \sigma_\iota = \iota$$

and so

$$\sigma_{A^{-1}} = \sigma_A^{-1}$$

Also, $\sigma_A = \sigma_B$ if and only if $\sigma_{AB^{-1}} = \iota$, that is, if and only if AB^{-1} is a scalar multiple of the identity.

If $\sigma \in Aut_F(F(t))$ then $F(t) = \sigma(F(t)) = F(\sigma t)$ and so $[F(t):F(\sigma t)] = 1$, which by Theorem 3.3.6 implies that $\sigma t = \sigma_A t$ for some 2×2 matrix over F. Hence, $\sigma = \sigma_A$. Since σ^{-1} also has the form σ_B for some matrix B, we have

$$\iota = \sigma_A \sigma_B = \sigma_{AB}$$

which implies that $AB = aI$, for some $a \in F$, whence A is nonsingular. ∎

Exercises

1. Find an example of a purely transcendental extension $F < E$ with two transcendence bases B and C such that $E = F(B)$ but $F(C)$ is a proper subfield of E.
2. Let $F < E$ and $F < K$. Show that $[EK:K]_t \leq [E:F]_t$.

3. Let $F < E < K$ and let $T \in K - E$. Show that $[E(T):F(T)]_t \leq [E:F]_t$ with equality if T is algebraically independent over F or algebraic over F.
4. Use the results of the previous exercise to show that if $F < K < E$ and $F < L < E$ then $[KL:F]_t \leq [K:F]_t + [L:F]_t$.
5. Let F be a field of characteristic $\neq 2$ and let u be transcendental over F. Suppose that $u^2 + v^2 = 1$. Show that F(u,v) is a purely transcendental extension by showing that $F(u,v) = F(w)$ where $w = (1 + v)/u$.
6. Let $F < K < E$ and suppose that $S \subseteq E$ is algebraically independent over K. Prove that $F(S) < K(S)$ is algebraic if and only if $F < K$ is algebraic.
7. Show that the converse of part 3) of Theorem 3.3.5 is false by describing an extension E of F that is not purely transcendental, but for which every $\alpha \in E - F$ is transcendental over F.
8. Prove that the transcendence degree of $\mathbb{R}$ over $\mathbb{Q}$ is $|\mathbb{R}|$.
9. Show that $[\mathbb{C}:\mathbb{Q}]_t = |\mathbb{C}|$.
10. (An extension of Luroth's Theorem) Suppose that $F < E$ is purely transcendental. Show that any simple extension of F contained in E is transcendental over F.
11. With regard to Theorem 3.4.2, show that $\sigma_A \sigma_B = \sigma_{AB}$ and $\sigma_C = \iota$ if and only if C is a scalar multiple of the identity matrix I.
12. Prove Lemma 3.1.1.

Chapter 4
Separability

4.1 Separable Polynomials

Let us recall a few facts about separable polynomials from Chapter 1.

Definition An irreducible polynomial $p(x) \in F[x]$ is **separable** if it has no multiple roots in any extension of F. An irreducible polynomial that is not separable is **inseparable.** □

Theorem 4.1.1

1) An irreducible polynomial $p(x)$ is separable if and only if $p'(x) \neq 0$.
2) If F is a field of characteristic 0, or a finite field, then all irreducible polynomials over F are separable.
3) Let $\text{char}(F) = p \neq 0$ and let $p(x)$ be irreducible.
   a) If $p(x)$ is inseparable, then there exists a positive integer d such that $p(x) = q(x^{p^d})$, where $q(x)$ is separable. In this case, all roots of $p(x)$ have multiplicity p^d.
   b) If $p(x) = h(x^{p^d})$ where $h(x)$ is any nonconstant polynomial and d is a positive integer, then $p(x)$ is inseparable.
4) Inseparable polynomials exist. □

The exponent d in part 3a) of the previous theorem is quite important and deserves a special name. Note that it can be characterized as the largest integer for which $p(x) = q(x^{p^d})$.

Definition Let $p(x) \in F[x]$ be an irreducible polynomial. If $\text{char}(F) = p \neq 0$, the integer d for which $p(x) = q(x^{p^d})$, with $q(x)$ separable, is called the **radical exponent** of $p(x)$. If $\text{char}(F) = 0$, the **radical exponent** of $p(x)$ is defined to be 0. If α is algebraic over F, the **radical exponent** of α over F is the radical exponent of $min(\alpha,F)$. □

The following definition allows us to handle the cases $\text{char}(F) = 0$ and $\text{char}(F) = p \neq 0$ simultaneously.

Definition The **exponent characteristic** expchar(F) of a field F is defined to be 1 if $\text{char}(F) = 0$ and $\text{char}(F)$ otherwise. □

Thus, any irreducible polynomial $p(x)$ has the form $p(x) = q(x^{p^d})$ where $q(x)$ is separable, p is the exponent characteristic of F and d is the radical exponent of $p(x)$. Moreover, $p(x)$ is separable if and only if its radical exponent is 0.

Definition Let $F < E$. Then $\alpha \in E$ is **separable over F** if α is algebraic over F and its minimal polynomial $min(\alpha,F)$ is separable. The extension $F < E$ is **separable** (or E is **separable over** F) if every element of E is separable over F. □

Before proceeding, we record a useful lemma. If F is a field and $S \subseteq F$ then S^n denotes the set $\{s^n \mid s \in S\}$.

Lemma 4.1.2 Let $F < E$ be algebraic with $\text{expchar}(F) = p$ and let $S \subseteq E$.

1) $F(S^{p^k}) = F([F(S)]^{p^k})$ for any $k \geq 0$.

2) $F(S) = F(S^{p^k})$ holds for some $k \geq 1$ if and only if it holds for all $k \geq 1$.

3) $F = F^{p^k}$ holds for some $k \geq 1$ if and only if it holds for all $k \geq 1$.

Proof. Part 1) follows from the fact that $[F(S)]^{p^k} = F^{p^k}(S^{p^k})$ and so

$$F([F(S)]^{p^k}) = F(F^{p^k}(S^{p^k})) = F(S^{p^k})$$

To prove part 2), suppose that $F(S) = F(S^{p^k})$ for some $k \geq 1$. Using part 1), we have

$$F(S) = F(S^{p^k}) = F([F(S)]^{p^k}) < F([F(S)]^{p^{k-1}}) = F(S^{p^{k-1}})$$

from which we conclude that $F(S) = F(S^{p^r})$ for all $r \leq k$. In particular $F(S) = F(S^p)$ and so again using part 1), we obtain

$$F(S) = F(S^{p^k}) = F([F(S)]^{p^k}) = F([F(S^p)]^{p^k}) = F(S^{p^{k+1}})$$

and so $F(S) = F(S^{p^r})$ for all $r \geq k$ as well. For part 3), we observe that

$$F^{p^k} < F^p < F$$

and so $F = F^{p^k}$ holds for some $k \geq 1$ if and only if $F = F^p$, which holds if and only if $F = F^{p^k}$ for all $k \geq 1$. ∎

4.2 Separable Degree

If $F < E$ is algebraic and if $\sigma: F \to L$ is an embedding of F into an algebraically closed field L, we let $\mathcal{E}_\sigma(E,F)$ denote the set of all extensions of σ to an embedding of E into L. Remarkably, the cardinality of $\mathcal{E}_\sigma(E,F)$ does not depend on σ or L.

Theorem 4.2.1 If $F < E$ is algebraic and $\sigma: F \to L$ is an embedding of F into an algebraically closed field L then the cardinality of $\mathcal{E}_\sigma(E,F)$ depends only on the extension $F < E$ and not on σ or L. In other words, if $\tau: F \to L'$ is an embedding with L' algebraically closed, then $|\mathcal{E}_\sigma(E,F)| = |\mathcal{E}_\tau(E,F)|$.

Proof. Observe first that if $\overline{\sigma}$ is an extension of σ to E then $\overline{\sigma}E$ is algebraic over σF and therefore contained in the algebraic closure of σF in L. Hence we may as well assume that L is an algebraic closure of σF. Similarly, we may assume that L' is an algebraic closure of τF.

Referring to Figure 4.2.1, the map $\tau\sigma^{-1}: \sigma(F) \to \tau(F)$ is an isomorphism that can be extended, by Theorem 2.8.4, to an embedding $\lambda: L \to L'$. Since $\sigma F < L$ is algebraic, so is $\tau F < \lambda L$, and since λL is algebraically closed, we have $\lambda L = L'$, implying that $\lambda: L \to L'$ is an isomorphism.

If $\overline{\sigma} \in \mathcal{E}_\sigma(E,F)$ then the map $\lambda\overline{\sigma}: E \to L'$ is an embedding of E into L' extending τ on F. This defines a map from $\mathcal{E}_\sigma(E,F)$ to $\mathcal{E}_\tau(E,F)$ given by $\overline{\sigma} \mapsto \lambda\overline{\sigma}$. It is clear that this map has an inverse given by $\overline{\tau} \mapsto \lambda^{-1}\tau$ and so both maps are bijections. ∎

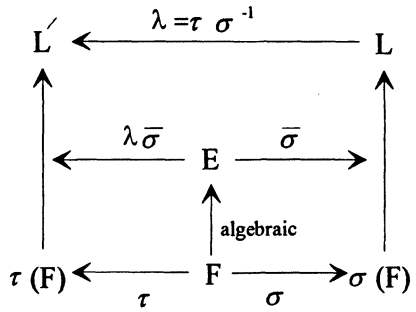

Figure 4.2.1

In view of Theorem 4.2.1, we may make the following definition.

Definition Let $F < E$ be an algebraic extension and let $\sigma: F \to L$ be an embedding of F into an algebraically closed field L. The cardinality of the set $\mathcal{E}_\sigma(E,F)$ is called the **separable degree** of E over F and is denoted by $[E:F]_s$. □

It will be convenient for our present discussion to adopt the following definitions, at least temporarily.

Definition An algebraic extension $F < E$ is **degreewise separable** if $[E:F]_s = [E:F]$. An algebraic extension $F < E$ is **separably generated** if $E = F(S)$ where each $\alpha \in S$ is separable over F. □

We next prove that the separable degree is multiplicative.

Theorem 4.2.2 If $F < K < E$ then $[E:F]_s = [E:K]_s[K:F]_s$.

Proof. The set $\mathcal{E}_j(K,F)$ of extensions of the inclusion map $j: F \to \overline{E}$ to an embedding $\bar{j}: K \to \overline{E}$ has cardinality $[K:F]_s$. Each such extension $\bar{j} \in \mathcal{E}_j(K,F)$ can be further extended to an embedding $j': E \to \overline{E}$. Clearly, the resulting extensions are all distinct and so

$$| \mathcal{E}_j(E,F) | \geq | \mathcal{E}_j(K,F) | \cdot | \mathcal{E}_{\bar{j}}(E,K) |$$

On the other hand, if $\sigma \in \mathcal{E}_j(E,F)$ and $\sigma_0: K \to \overline{E}$ is the restriction of σ to K then σ_0 is the extension of $j: F \to \overline{E}$ to K, hence an element of $\mathcal{E}_j(K,F)$. Since σ is the extension of σ_0 to E, σ is obtained by a double extension of $j: F \to \overline{E}$ and so equality holds in the inequality above. ∎

4.3 The Simple Case

Now let us consider simple extensions in the present context. Let $F < F(\alpha)$ be algebraic. If $p(x) = min(\alpha, F)$ and if $j: F \to \overline{F}$ is the inclusion map then Theorem 2.8.3 implies that $[F(\alpha):F]_s = | \mathcal{E}_j(F(\alpha),F) |$ is equal to the number of distinct roots of p(x). If p(x) is separable, it has $deg\ p(x) = [F(\alpha):F]$ distinct roots and so

$$[F(\alpha):F]_s = [F(\alpha):F]$$

If $p(x) = q(x^{p^d})$ has radical exponent $d \geq 1$, then each root of p(x) has multiplicity p^d and so

$$p^d[F(\alpha):F]_s = deg\ p(x) = [F(\alpha):F]$$

We thus have the following theorem.

Theorem 4.3.1 Let $F < F(\alpha)$ be algebraic with expchar(F) = p. If $min(\alpha,F)$ has radical exponent d, then

$$p^d[F(\alpha):F]_s = [F(\alpha):F] \tag{4.3.1}$$

In particular, $[F(\alpha):F]_s \mid [F(\alpha):F]$. Moreover, the following are equivalent.

1) α is separable over F.
2) $F < F(\alpha)$ is degreewise separable; that is, $[F(\alpha):F]_s = [F(\alpha):F]$.
3) $F < F(\alpha)$ is separable.

Proof. We have seen that (4.3.1) holds and since α is separable if and only if its radical exponent is 0, it follows that 1) and 2) are equivalent. Clearly 3) implies 1). To see that 2) implies 3), let $\beta \in F(\alpha)$ and consider the tower $F < F(\beta) < F(\alpha)$. Then

$$[F(\alpha):F(\beta)]_s[F(\beta):F]_s = [F(\alpha):F]_s = [F(\alpha):F] = [F(\alpha):F(\beta)][F(\beta):F]$$

Since $F(\alpha) = F(\beta)(\alpha)$, the extension $F(\beta) < F(\alpha)$ is simple and so each factor on the far left divides the corresponding factor on the far right, implying that the corresponding factors are equal. In particular, $[F(\beta):F]_s = [F(\beta):F]$, showing (by the equivalence of parts 1 and 2) that β is separable over F. Hence $F < F(\alpha)$ is separable. ∎

Note that, according to the previous theorem, if α is separable so is any polynomial in α. The following is another characterization of separable elements.

Theorem 4.3.2 Let α be algebraic over F, with expchar(F) = p. Then α is separable over F if and only if

$$F(\alpha) = F(\alpha^{p^k})$$

for some $k \geq 1$, and hence for all $k \geq 1$.

Proof. Lemma 4.1.2 allows us to confine our attention to k = 1. Suppose α is separable over F. First suppose that α is separable over F. The polynomial $(x - \alpha)^p = x^p - \alpha^p \in F(\alpha^p)[x]$ has α as a root and so there exists an $r \leq p$ such that

$$min(\alpha,F(\alpha^p)) = (x - \alpha)^r$$

Since $p(x) = min(\alpha,F)$ also has coefficients in $F(\alpha^p)$, we have $(x-\alpha)^r \mid p(x)$. But $p(x)$ is separable, and so $r = 1$. Thus $r(x) = x - \alpha$, implying that $\alpha \in F(\alpha^p)$ and consequently $F(\alpha) = F(\alpha^p)$.

Conversely, suppose that $F(\alpha) = F(\alpha^p)$ and let $p(x) = min(\alpha,F)$. If α is not separable over F then $p(x) = q(x^p)$. Since $q(\alpha^p) = p(\alpha) = 0$, we get

$$[F(\alpha^p):F] \leq deg\ q(x) = \frac{1}{p}[F(\alpha):F]$$

which is contrary to $F(\alpha) = F(\alpha^p)$. Thus α is separable over F. ∎

4.4 The Finite Case

Now we consider an arbitrary finite extension $F < E$. By Theorem 2.5.2, we may let $E = F(\alpha_1,\ldots,\alpha_n)$ where α_i is algebraic over F. Taking separable degrees in the tower

$$F < F(\alpha_1) < F(\alpha_1,\alpha_2) < \cdots < F(\alpha_1,\ldots,\alpha_n) \tag{4.4.1}$$

gives

$$[F(\alpha_1,\ldots,\alpha_n):F]_s = \prod_{i=1}^{n} [F(\alpha_1,\ldots,\alpha_i):F(\alpha_1,\ldots,\alpha_{i-1})]_s$$

Since each step on the right is simple, Theorem 4.3.1 implies that each separable degree on the right divides the corresponding vector space degree, and so

$$[F(\alpha_1,\ldots,\alpha_n):F]_s \mid [F(\alpha_1,\ldots,\alpha_n):F]$$

Theorem 4.4.1 Let $F < E$ be finite. Then $[E:F]_s \mid [E:F]$. Also, the following are equivalent.

1) E is separably generated.
2) $F < E$ is degreewise separable; that is, $[E:F]_s = [E:F]$.
3) $F < E$ is separable.

Proof. [1⇒2] Suppose that $E = F(S)$ where the elements of S are separable over F. The finiteness of $F < E$ implies that $E = F(\alpha_1 \ldots \alpha_n)$, for some $n > 0$, where $\alpha_i \in S$. Since α_i is separable over $F(\alpha_1,\ldots,\alpha_{i-1})$, each step in the tower (4.4.1) is generated by a single separable element. Hence, each step is degreewise separable and the multiplicativity of degrees implies that $F < E$ is degreewise separable. [2⇒3] Let $\beta \in E$ and consider the tower $F < F(\beta) < E$. Since $F < E$ is degreewise separable, so is $F < F(\beta)$ and so β is separable over F. Hence, $F < E$ is separable. [3⇒1] This is clear from the definition. ∎

Thus, for finite extensions, the notions of separability, degreewise separability and separably generated are equivalent. Note that if $F < K < E$ is finite then $F < E$ is separable if and only if $K < E$ and $F < K$ are separable. We will show later that the class of separable extensions (finite or otherwise) is distinguished. Let us have another characterization of finite separable extensions.

Theorem 4.4.2 If $F < E$ is separable then $E = F(E^{p^k})$ for all $k \geq 1$. By way of converse, if $F < E$ is finite and $E = F(E^{p^k})$ for some $k \geq 1$, then $F < E$ is separable.

Proof. Suppose $F < E$ is separable. Lemma 4.1.2 allows to to confine our attention to $k = 1$. For any $\alpha \in E$, we have $F(\alpha) = F(\alpha^p) \subseteq F(E^p)$ and so $E \subseteq F(E^p)$. The reverse inclusion is obvious and so $E = F(E^p)$.

Now suppose that $E = F(E^p)$. Since $F < E$ is finite, we have $E = F(S^p)$ for some finite subset $S \subseteq E$. Since $E = F(S^p) < F(S) < E$, we have $E = F(S) = F(S^p)$ and so Lemma 4.1.2 implies that $E = F(S^{p^k})$ for all $k \geq 1$. If d is the maximum of the radical exponents of the elements of S then every element of S^{p^d} is separable over F and so $E = F(S^{p^d})$ is separably generated over F and therefore separable over F. ∎

Corollary 4.4.3 Let $F < E$ be a separable extension and let $S \subseteq E$.

1) If S spans E over F, then S^{p^k} spans E over F, for any $k \geq 1$.
2) If $F < E$ is finite and S is linearly independent over F, then S^{p^k} is linearly independent over F, for any $k \geq 1$.
3) If $F < E$ is finite and S is a basis for E over F, then S^{p^k} is a basis for E over F, for any $k \geq 1$.

Proof. If S spans E over F, then S^p spans E^p over F^p, and hence also over F. Hence S^p spans $F(E^p) = E$ over F. Repeating this argument proves part 1). For part 2), since $F < F(S)$ is separable and S spans F(S) over F, we conclude from part 1) that S^{p^k} spans F(S) over F. Since

$$|S^{p^k}| = |S| < \infty$$

it follows that S^{p^k} is a basis for F(S) over F and is therefore linearly independent over F. Part 3) follows from parts 1) and 2). ∎

We now prove that all finite separable extensions are actually simple extensions.

Theorem 4.4.4 If $F < E$ is a finite separable extension then there exists a $\gamma \in E$ such that $E = F(\gamma)$. If F is an infinite field, there exist infinitely many such primitive elements γ.

Proof. If F is a finite field, then so is E, and we appeal to the fact that

the multiplicative group E^* of nonzero elements of E is cyclic. If $E^* = \langle\gamma\rangle$ then $E = F(\gamma)$ and E is simple over F. Let us now assume that F is an infinite field.

Since $F < E$ is finitely generated, it is sufficient to consider the case $E = F(\alpha,\beta)$, and then appeal to an inductive argument. Let $\sigma_1,\ldots,\sigma_n$ be the distinct embeddings of E into $\overline{F}$ over F. Consider the polynomial

$$p(x) = \prod_{i \neq j} [(\sigma_i - \sigma_j)(\alpha) + (\sigma_i - \sigma_j)(\beta)x] \in \overline{F}[x]$$

Since none of the linear factors on the right is 0, we conclude that $p(x) \neq 0$. Since F is infinite, there must infinitely many elements $s \in F$ such that $p(s) \neq 0$. Hence $(\sigma_i - \sigma_j)(\alpha) + s(\sigma_i - \sigma_j)(\beta) \neq 0$ for all $i \neq j$, that is, the n elements $\gamma_i = \sigma_i\alpha + s\sigma_i\beta = \sigma_i(\alpha + s\beta)$ are distinct. But each γ_i is a root of $min(\alpha + s\beta,F)$ and so

$$[E:F] \geq [F(\alpha + s\beta):F] \geq n = [E:F]_s = [E:F]$$

from which it follows that $E = F(\alpha + s\beta)$. ∎

Corollary 4.4.5 If F has characteristic 0 or if F is a finite field then any finite extension of F is simple. □

We can improve upon Theorem 4.4.4 without too much additional work. This result will prove useful to us later.

Theorem 4.4.6 If $E = F(\alpha_1,\ldots,\alpha_n,\beta)$ where α_i is separable over F and β is algebraic over F then $F < E$ is a simple extension.

Proof. If F is finite, then E is finite, and therefore $F < E$ is simple. Let us assume that F is infinite. Theorem 4.4.4 implies that $E = F(\alpha,\beta)$ for some α separable over F. We may proceed as in the proof of that theorem to obtain an element $\beta + s\alpha$ for which the elements $\sigma_i(\beta + s\alpha)$ are distinct, where $\sigma_1,\ldots,\sigma_n$ are the distinct embeddings of E into $\overline{F}$ over F and $\sigma_1 = \iota$. Note that the set $\{\sigma_1\alpha,\ldots,\sigma_n\alpha\}$ contains a complete set of roots of $p_\alpha(x) = min(\alpha,F)$ and $\{\sigma_1\beta,\ldots,\sigma_n\beta\}$ contains a complete set of roots of $p_\beta(x) = min(\beta,F)$.

Let $q(x) = p_\beta(\beta + s\alpha - sx)$. Since $\sigma_1\alpha = \alpha$, we have

$$q(\sigma_1\alpha) = p_\beta(\beta) = 0$$

and since $\sigma_1\beta + s\sigma_1\alpha - s\sigma_i\alpha \neq \sigma_i\beta$ for $i \neq 1$, we have

$$q(\sigma_i\alpha) = p_\beta(\sigma_1\beta + s\sigma_1\alpha - s\sigma_i\alpha) \neq 0$$

for $i \neq 1$. Hence, the polynomials $p_\alpha(x)$ and $q(x)$, both of which have

coefficients in $F(\beta + \sigma\alpha)$, have precisely one root in common, namely $\sigma_1\alpha = \alpha$. Thus, since $p_\alpha(x)$ has no multiple roots, the greatest common divisor of $p_\alpha(x)$ and $q(x)$ is $x - \alpha$, which must have its coefficients in $F(\beta + s\alpha)$ as well. In other words $\alpha \in F(\beta + s\alpha)$, from which it follows that $\beta \in F(\beta + s\alpha)$, whence $F(\alpha,\beta) = F(\beta + s\alpha)$. ∎

4.5 The Algebraic Case

For arbitrary algebraic extensions $F < E$, we have the following.

Theorem 4.5.1 Let $\text{expchar}(F) = p$. An algebraic extension $F < E$ is separable if and only if it is separably generated. If $F < E$ is separable then $E = F(E^{p^k})$ for all $k \geq 1$.

Proof. If $F < E$ is separable then E is separably generated (by itself) over F. For the converse, assume that $E = F(S)$ where each $\alpha \in S$ is separable over F and let $\beta \in E$. Then $\beta \in F(S_0)$ for some finite subset $S_0 \subseteq S$. Since $F < F(S_0)$ is finitely generated and algebraic, it is finite. Thus, Theorem 4.4.1 implies that $F < F(S_0)$ is separable. Hence β is separable over F and so $F < E$ is separable. The last statement was proved in Theorem 4.4.2. ∎

We may now establish that the class of separable extensions is distinguished.

Theorem 4.5.2 The class of separable extensions is distinguished. It is also closed under the taking of arbitrary composites. If $F < E$ is separable and E^{nc} is the normal closure of E over F then $F < E^{nc}$ is separable.

Proof. Let $F < K < E$. If all extensions are finite, we have already shown (by a degree argument) that $F < E$ is separable if and only if $F < K$ and $K < E$ are separable. In general, we leave it as an exercise to show that if $F < E$ is separable then $F < K$ and $K < E$ are separable. Suppose that $F < K$ and $K < E$ are separable and let $\alpha \in E$. Let $C \subseteq K$ be the set of coefficients of $p(x) = min(\alpha,K)$. Then $p(x) = min(\alpha,F(C))$ and so α is separable over $F(C)$. It follows that each step in the tower $F < F(C) < F(C,\alpha)$ is finite and separable, implying that α is separable over F. This shows that $F < E$ is separable and completes verification of property D1) in the definition of distinguished class.

For property D2), let $F < E$ be separable and let $F < K$. Since every element of E is separable over F it is also separable over the larger field K. Hence $EK = K(E)$ is separably generated and is therefore separable.

The fact that separable extensions are closed under the taking of

arbitrary composites follows from the finitary property of arbitrary composites. That is, each element of an arbitrary composite involves elements from only a finite number of the fields in the composite and so is an element of a finite composite, which is separable.

Finally, the normal closure E^{nc} is the composite $\vee(\sigma E)$ for $\sigma \in Hom_F(E,\overline{E})$. Since $F < E$ is separable and $\sigma: E \to \sigma E$ is an isomorphism over F, the elements $\alpha \in E$ and $\sigma\alpha \in \sigma E$ have the same minimal polynomial and so the separability of α over F implies that of $\sigma\alpha$, whence $F < \sigma E$ is separable. Since separability is preserved under composites, $F < E^{nc}$ is separable. ∎

4.6 Pure Inseparability

The antithesis of a separable element is a *purely inseparable* element.

Definition An element α algebraic over F is **purely inseparable** over F if its minimal polynomial $min(\alpha,F)$ has the form $(x-\alpha)^n$ for some $n \geq 1$. An algebraic extension $F < E$ is **purely inseparable** if every element of E is purely inseparable over F. □

Note that any $\alpha \in F$ is purely inseparable over F. In fact, an element α is both separable and purely inseparable over F if and only if $\alpha \in F$. It follows that, for extensions of fields of characteristic 0 or finite fields, there are no "interesting" purely inseparable elements.

Example 4.6.1 Let $char(F) = 2$. If t is transcendental over F, then t is purely inseparable over $F(t^2)$, since its minimal polynomial over $F(t^2)$ is $x^2 - t^2 = (x-t)^2$. □

Example 4.6.2 Here we present an example of an element that is neither separable nor purely inseparable over a field F. Let $char(F) = p$ and let $\alpha \in F$ be nonzero. Let t be transcendental over F and let

$$s = \frac{t^{p^2}}{t^p + \alpha}$$

According to Theorem 3.3.6, $F(s) < F(t)$ is algebraic and has degree equal to p^2. Since t is a root of the monic polynomial

$$p(x) = x^{p^2} - sx^p - s\alpha$$

of degree x^{p^2} over F(s), this must be the minimal polynomial for t over F(s). Since $p(x) = q(x^p)$, we deduce that t is not separable over F(s). On the other hand, if t were purely inseparable over F(s), there would

exist $\beta \in F(s)$ for which

$$x^{p^2} - sx^p - s\alpha = (x - \beta)^{p^2} = x^{p^2} - \beta^{p^2}$$

which would imply that $s = 0$, which is not the case. Hence, t is neither separable nor purely inseparable over F(s). □

Definition Let $F < E$ be finite. Since $[E:F]_s \mid [E:F]$, we may write

$$[E:F] = [E:F]_s[E:F]_i$$

where $[E:F]_i$ is the **inseparable degree** or **degree of inseparability** of E over F. □

Note that, while the separable degree is defined for infinite extensions, the inseparable degree is defined only for finite extensions.

Definition If $F < E$ is algebraic and $[E:F]_s = 1$, we say that $F < E$ is **degreewise purely inseparable**. When $F < E$ is finite, this is equivalent to $[E:F]_i = [E:F]$. □

Theorem 4.6.1 Let $F < E$ be a finite extension with expchar(F) = p.

1) If $F < K < E$ then $[E:F]_i = [E:K]_i[K:F]_i$.
2) $F < E$ is separable if and only if $[E:F]_i = 1$.
3) If $\alpha \in E$ then $[F(\alpha):F]_i = p^d$ where d is the radical exponent of α.
4) $[E:F]_i$ is a power of p.

Proof. The first three statements are clear. The last statement follows from the fact that $F < E$ is finitely generated and the inseparable degree is multiplicative. We leave the details to the reader. ∎

We next characterize purely inseparable elements.

Theorem 4.6.2 Let α be algebraic over F, with radical exponent d and let $p(x) = min(\alpha,F)$. The following are equivalent.

1) α is purely inseparable over F.
2) The polynomial $(x - \alpha)^n$ has coefficients in F, for some $n \geq 1$.
3) $p(x) = (x - \alpha)^{p^d} = x^{p^d} - \alpha^{p^d}$.
4) α is a root of $x^{p^k} - \beta$, for some $\beta \in F$ and $k \geq 0$.
5) $\alpha^{p^k} \in F$ for some $k \geq 0$.
6) d is the smallest nonnegative integer for which $\alpha^{p^d} \in F$.

Proof. We establish only those implications that are not immediate. Recall that $p(x) = q(x^{p^d})$ where $q(x)$ is separable over F.

[2⇒3] If 2) holds then $q(x^{p^d}) \mid (x-\alpha)^n$ and so $q(x^{p^d}) = (x-\alpha)^r$ for some $1 \leq r \leq n$. It follows that $r = mp^d$, where $m = deg\ q(x)$. Hence,

$$q(x^{p^d}) = (x-\alpha)^{mp^d} = (x^{p^d} - \alpha^{p^d})^m$$

Thus $q(x) = (x-\alpha^{p^d})^m$ and the separability of $q(x)$ implies that $m = 1$, whence

$$r = p^d \text{ and } p(x) = (x-\alpha)^{p^d}$$

[5⇒6] If 5) holds then

$$r(x) = x^{p^k} - \alpha^{p^k} = (x-\alpha)^{p^k}$$

is a polynomial over F with $r(\alpha) = 0$. Hence $q(x^{p^d}) \mid (x-\alpha)^{p^k}$, showing that $k \geq d$. Since $r(x) \in F[x]$, the fact that 2) implies 3) shows that

$$p(x) = x^{p^d} - \alpha^{p^d}$$

and so $\alpha^{p^d} \in F$. Hence d is the smallest integer for which $\alpha^{p^d} \in F$.

[6⇒1] If 6) holds, then

$$r(x) = (x-\alpha)^{p^d} = x^{p^d} - \alpha^{p^d}$$

is a polynomial over F with α as a root, and so $p(x) \mid r(x)$. Hence, $p(x)$ has the form $(x-\alpha)^n$ for some $n \geq 1$ and α is purely inseparable over F. ∎

Theorem 4.6.3 Let $F < E$ be algebraic. The following are equivalent.

1) E is purely inseparably generated; that is, generated by purely inseparable elements.
2) $F < E$ is degreewise purely inseparable; that is, $[E:F]_s = 1$.
3) $F < E$ is a purely inseparable extension.

Proof. [1⇒2] Suppose first that $E = F(I)$ where all elements of I are purely inseparable over F. Any embedding $\sigma: E \to L$ over F is uniquely determined by its values on the elements of I. But if $\alpha \in I$ then $\sigma\alpha$ is a root of the minimal polynomial $min(\alpha,F)$ and so $\sigma\alpha = \alpha$. Hence σ must be the identity and $[E:F]_s = 1$.

[2⇒3] Let $\alpha \in E$. Then $[F(\alpha):F]_s = 1$ and since $F < F(\alpha)$ is a finite extension, Theorem 4.3.1 implies that

$$p^d = [F(\alpha):F] = deg\ min(\alpha,F)$$

Since $min(\alpha,F) = q(x^{p^d})$, it follows that $q(x)$ is linear and so

$$min(\alpha,F) = x^{p^d} - \beta$$

for some $\beta \in F$, which implies by Theorem 4.6.2 that α is purely inseparable over F. [3⇒1] This is clear. ∎

We can now show that the class of purely inseparable extensions is distinguished.

Theorem 4.6.4 The class of purely inseparable extensions is distinguished. It is also closed under the taking of arbitrary composites.

Proof. Let $F < K < E$. Since pure inseparability is equivalent to degreewise pure inseparability and $[E:F]_s = 1$ if and only if $[E:K]_s = 1$ and $[K:F]_s = 1$, it is clear that D1) holds. For D2), suppose that $F < E$ is purely inseparable and $F < K$. Since every element of E is purely inseparable over F, it is also purely inseparable over the larger field K. Hence $EK = K(E)$ is purely inseparably generated and therefore purely inseparable. We leave proof of the last statement to the reader. ∎

4.7 Separable and Purely Inseparable Closures

Let $F < E$. According to Theorem 4.4.1, if α, $\beta \in E$ are separable over F then $F(\alpha,\beta)$ is separable over F. It follows that $\alpha \pm \beta$, $\alpha\beta$, and α^{-1} (for $\alpha \neq 0$) are separable over F. Hence, the set of all elements of E that are separable over F is a subfield of E. A similar statement holds for purely inseparable elements.

Definition Let $F < E$. The field

$$F^{sc} = \{\alpha \in E \mid \alpha \text{ separable over } F\}$$

is called the **separable closure** of F in E. The field

$$F^{ic} = \{\alpha \in E \mid \alpha \text{ is purely inseparably over } F\}$$

is called the **purely inseparable closure** of F in E. □

The separable closure allows us to decompose an arbitrary algebraic extension into separable and purely inseparable parts.

Theorem 4.7.1 Let $F < E$ be algebraic.

1) In the tower $F < F^{sc} < E$ the first step is separable and the second step is purely inseparable.
2) $E^{[E:F]_i} \subseteq F^{sc}$.
3) Any embedding $\sigma: E \to \overline{E}$ is uniquely determined by its restriction to F^{sc}.

Proof. For part 1), if $\alpha \in E$ has radical exponent d, then $min(\alpha,F) = q(x^{p^d})$ where $q(x) = min(\alpha^{p^d},F)$ is separable and so $\alpha^{p^d} \in F^{sc}$. Thus, Theorem 4.6.2 implies that α is purely inseparable over F^{sc}. This shows that $F^{sc} < E$ is pusrely inseparable. For part 2), since $p^d = [F(\alpha):F]_i \mid [E:F]_i$ we see that

$$\alpha^{[E:F]_i} \in F^{sc}$$

for all $\alpha \in E$ and so $E^{[E:F]_i} \subseteq F^{sc}$. We leave proof of the last statement to the reader. ∎

Corollary 4.7.2 Let $F < E$ be finite. Then $[E:F]_s = [F^{sc}:F]$ and $[E:F]_i = [E:F^{sc}]$. □

Part 1 of Theorem 4.7.1 shows that any algebraic extension can be decomposed into a separable extension followed by a purely inseparable extension. In general, the reverse is not possible. Although $F < F^{ic}$ is purely inseparable, the elements of $E - F^{ic}$ need not be separable over F; they are simply not purely inseparable over F. However, it is not hard to see when $F^{ic} < E$ is separable.

Theorem 4.7.3 Let $F < E$ be algebraic. Then $F^{ic} < E$ is separable if and only if $E = F^{sc}F^{ic}$.

Proof. If $F^{ic} < E$ is separable then so is $F^{sc}F^{ic} < E$. But since $F^{sc} < E$ is purely inseparable, so is $F^{sc}F^{ic} < E$. Thus, we have $E = F^{sc}F^{ic}$. Conversely, if $E = F^{sc}F^{ic}$ then $F^{ic} < F^{sc}F^{ic}$, being a lifting of a separable extension $F < F^{sc}$, is also separable. ∎

We can do better than the previous theorem when $F < E$ is a normal extension, which includes the case $E = \overline{F}$. Let $G = Aut_F(E)$ be the set of all automorphisms of E over F. Since $F < E$ is normal, G is also the set of all embeddings of E into $\overline{F}$ over F. We define the **fixed field** of G in E by

$$F(G) = \{\alpha \in E \mid \sigma\alpha = \alpha \text{ for all } \sigma \in G\}$$

Theorem 4.7.4 Let $F < E$ be a normal extension. Let $G = Aut_F(E)$ and let $F(G)$ be the fixed field of G in E. Then $F(G) = F^{ic}$. Furthermore, in the tower $F < F^{ic} < E$, the first step is purely inseparable and the second step is separable.

Proof. Let $\alpha \in F(G)$. If $\beta \in \overline{F}$ is a root of $p(x) = min(\alpha,F)$ then there exists an embedding $\sigma:E \to \overline{F}$ over F for which $\sigma\alpha = \beta$. But $\sigma\alpha = \alpha$ and so $\beta = \alpha$. Hence $min(\alpha,F)$ has only one root and so $\alpha \in F^{ic}$. On the other hand, if $\alpha \in F^{ic}$ then any $\sigma \in G$ must map α to itself, since it must map α to a root of $min(\alpha,F)$. Hence $\alpha \in F(G)$. This proves that $F(G) = F^{ic}$.

Now let $\alpha \in E$ and $p(x) = min(\alpha,F(G))$. Let $q(x) = \prod(x - r_i)$ where $R = \{r_1,\ldots,r_n\}$ is the set of *distinct* roots of $p(x)$ in E. Since any $\sigma \in G$ is a permutation of R, we deduce that $q^\sigma(x) = q(x)$ and so the coefficients of $q(x)$ lie in $F(G)$. Hence $q(x) = p(x)$ and α is separable over $F(G)$. ∎

Corollary 4.7.5 If $F < E$ is normal then $F^{ic} < E$ is separable and $E = F^{sc}F^{ic}$. □

Let us conclude this section with a characterization of simple algebraic extensions. If $E = F(\alpha)$ is a simple algebraic extension of F and if d is the radical exponent of α, we have seen that $p^d = [E:F]_i$ is the *smallest* nonnegative power of p such that α^{p^d} is separable over F, or equivalently, such that $E^{p^d} \subseteq F^{sc}$. It turns out that this property actually characterizes simple algebraic extensions. Before proving this, we give an example where this property fails to hold.

Example 4.7.1 Let u and v be transcendental over K with $\text{char}(K) = p \neq 0$. Let $E = K(u,v)$ and $F = K(u^p,v^p)$. It is easily seen that $F < E$ is purely inseparable with $[E:F]_i = p^2$. However, $\alpha \in E$ implies $\alpha^p \in F$ and so $E^p \subseteq F$. □

We next require the following useful lemma.

Lemma 4.7.6 If $\text{char}(F) = p \neq 0$ and $\alpha \in F$, $\alpha \notin F^p$ then $f(x) = x^{p^k} - \alpha$ is irreducible for every $k \geq 1$.

Proof. Let $\beta \in \overline{F}$ be a root of $f(x) = x^{p^k} - \alpha$. Then

$$f(x) = (x - \beta)^{p^k}$$

If $p(x) = min(\beta,F)$ then $p(x) \mid f(x)$ and so $p(x) = (x - \beta)^{p^d}$ for some $d \leq k$. But if $d < k$ then

$$\beta^{p^d} \in F$$

and so

$$\alpha = \beta^{p^k} = (\beta^{p^{k-1}})^p \in F^p$$

contrary to assumption. Hence $d = k$ and $f(x)$ is irreducible. ∎

Theorem 4.7.7 Let $F < E$ be a finite extension with $[E:F]_i = p^d$. Then $F < E$ is simple if and only if d is the smallest nonnegative integer for which $E^{p^d} \subseteq F^{sc}$.

Proof. We have seen that if $F < E$ is simple then d is the smallest such nonnegative integer. For the converse, note first that if F is a finite field then so is E, implying that E^* is cyclic and so $F < E$ is simple. Let us assume that F is an infinite field and look at the second step in the tower $F < F^{sc} < E$. This step is purely inseparable. Since $F^{sc} < E$ is finite, we have

$$E = F^{sc}(\beta_1, \ldots, \beta_n)$$

If for some $k < d$, we have $\beta_i^{p^k} \in F^{sc}$ for all i, then $E^{p^k} \subseteq F^{sc}$, contrary to hypothesis. Hence one of the β_i's, say β, satisfies

$$\beta^{p^d} \in F^{sc}, \quad \beta^{p^k} \notin F^{sc} \text{ for } k < d$$

It follows that

$$[F^{sc}(\beta):F^{sc}]_i = p^d = [E:F]_i \geq [E:F^{sc}]_i$$

Since $F^{sc}(\beta) < E$, we have $[F^{sc}(\beta):F^{sc}]_i = [E:F^{sc}]_i$ and since the extensions involved are purely inseparable, we get $[F^{sc}(\beta):F^{sc}] = [E:F^{sc}]$. Hence, $E = F^{sc}(\beta)$.

Our tower now has the form $F < F^{sc} < F^{sc}(\beta)$ where β is purely inseparable over F^{sc}. In addition, $F < F^{sc}$ is finite and separable and therefore simple. Thus there exists $\alpha \in F^{sc}$ such that $F^{sc} = F(\alpha)$ and the tower takes the form $F < F(\alpha) < F(\alpha,\beta)$ where α is separable over F and β is purely inseparable over $F(\alpha)$. By Theorem 4.4.6, the extension $F < F(\alpha,\beta)$ is simple. ∎

Note that Theorem 4.7.7 implies that the extension $F < E$ of Example 4.7.1 is not simple.

4.8 Perfect Fields

Definition A field F is **perfect** if every irreducible polynomial over F is separable. □

It is clear from the definitions that if F is perfect then any algebraic extension of F is separable. Conversely, suppose that every algebraic extension of F is separable. If $p(x) \in F[x]$ is irreducible and α is a root of $p(x)$ in some extension of F then $F < F(\alpha)$ is algebraic and so α is separable over F, that is, $p(x)$ is separable. Thus, F is perfect.

Theorem 4.8.1 A field F is perfect if and only if every algebraic extension of F is separable over F. □

Theorem 4.8.2 Every field of characteristic 0 and every finite field is perfect. □

Note that if $\text{expchar}(F) = p$ then $F^p = \{\alpha^p \mid \alpha \in F\}$ is a subfield of F. The map $\phi: F \to F$ defined by $\sigma_p \alpha = \alpha^p$ is called a **Frobenius map**. It is a monomorphism since $\alpha^p \pm \beta^p = (\alpha \pm \beta)^p$.

Theorem 4.8.3 Let F be a field with $\text{expchar}(F) = p$. The following are equivalent.

1) F is perfect.
2) $F = F^{p^k}$ for some (and hence all) $k \geq 1$.
3) The Frobenius map σ_{p^k} is an automorphism, for some (and hence all) $k \geq 1$.

Proof. [1⇒2] Suppose F is perfect. Let $\alpha \in F$ and consider the polynomial $p(x) = x^p - \alpha \in F[x]$. If β is a root of $p(x)$ in a splitting field then $\beta^p = \alpha$ and so

$$p(x) = x^p - \beta^p = (x - \beta)^p$$

Hence β is purely inseparable over F. But β is also separable over F and therefore $\beta \in F$. Hence, $\alpha \in F^p$ for all $\alpha \in F$, that is, $F \subseteq F^p$. Since the reverse inclusion is manifest, we have $F = F^p$. Lemma 4.1.2 implies the desired result.

[2⇒1] We may assume that $p > 1$. If 2) holds then Lemma 4.1.2 implies that $F^p = F$. It follows that if $p(x) \in F[x]$ is irreducible but not separable, then

$$p(x) = \sum a_i (x^p)^i = \sum b_i^p (x^i)^p = (\sum b_i x^i)^p$$

contradicting the fact that $p(x)$ is irreducible. Hence, $p(x)$ is separable and so F is perfect. Since the Frobenius map is a monomorphism, statements 2) and 3) are easily seen to be equivalent. ∎

While it is true that any algebraic extension of a perfect field is perfect, not all subfields of a perfect field need be perfect.

Theorem 4.8.4
1) If $F < E$ is algebraic and F is perfect then E is perfect.
2) If $F < E$ is finite and E is perfect then F is perfect.

Proof. Part 1) follows from Theorem 4.8.1 and the fact that every algebraic extension of E is an algebraic extension of F. For part 2), let $\text{expchar}(F) = p$ and suppose first that $F < E$ is simple. Thus, $E = F(\alpha)$ is perfect and α is algebraic over F, with minimal polynomial $p(x) = \sum a_i x^i$. Then

$$0 = [\sum a_i \alpha^i]^p = \sum a_i^p \alpha^{pi}$$

Hence, the degree of α^p over F^p is no greater than the degree of α over F, in symbols, $[F^p(\alpha^p):F^p] \leq [F(\alpha):F]$. But $F^p(\alpha^p) = [F(\alpha)]^p = F(\alpha)$ since $F(\alpha)$ is perfect and so $[F(\alpha):F^p] \leq [F(\alpha):F]$. Since $F^p < F$, equality holds and $F^p = F$, whence F is perfect. Since $F < E$ is finitely generated by algebraic elements, the result follows by repetition of the previous argument. ∎

Note that we cannot drop the finiteness condition in part 2) of the previous theorem since, for example, $F < \overline{F}$ is algebraic and $\overline{F}$ is perfect even if F is not.

Perfect Closures

Let $\text{char}(F) = p \neq 0$ and let $\overline{F}$ be an algebraic closure of F. For each $k \geq 1$, the set

$$F^{1/p^k} = \{\alpha \in \overline{F} \mid \alpha^{p^k} \in F\}$$

is a subfield of $\overline{F}$. Moreover, we have

$$F \subseteq F^{1/p} \subseteq F^{1/p^2} \subseteq \cdots$$

The union

$$pcl(F) = \bigcup_{k=1}^{\infty} F^{1/p^k}$$

which is also a subfield of $\overline{F}$, is known as the **perfect closure** of F in $\overline{F}$, which name is justified by the following theorem.

Theorem 4.8.5 Let F be a field of characteristic $p \neq 0$. Then $pcl(F)$ is the smallest perfect subfield of $\overline{F}$ containing F.

Proof. To see that $pcl(F)$ is perfect, observe that if $\alpha \in pcl(F)$ then $\alpha^{p^k} \in F$ for some $k \geq 1$. Hence, letting β be a root of $x^p - \alpha$ in $\overline{F}$, we have $\alpha = \beta^p$, where

$$\beta^{p^{k+1}} = \alpha^{p^k} \in F$$

and so $\beta \in pcl(F)$. This shows that $pcl(F) \subseteq [pcl(F)]^p$. Since the reverse inclusion is obvious, it follows that $pcl(F)$ is perfect.

In addition, if $F < K < pcl(F)$ and $\alpha \in pcl(F) - K$, the fact that $\alpha^{p^k} \in F$ for some $k \geq 1$ implies that α is purely inseparable over F and hence also over K. But since α is not in K, it cannot be separable over K as well. Thus K is not perfect. ∎

Exercises

1. Let $F < K < E$. If $F < E$ is separable, show that $F < K$ and $K < E$ are separable.
2. Prove that if $F < E$ is finite and separable then there are only finitely many intermediate fields between E and F.
3. Show that all algebraically closed fields are perfect. If t is transcendental over F then F(t) is not perfect.
4. Let α be algebraic over F, where expchar(F) = p and let d be the radical exponent of α. Show that α^{p^k} is separable over F if and only if $k \geq d$.
5. Let p and q be distinct primes. Then $\mathbb{Q} < \mathbb{Q}(\sqrt{p}, \sqrt{q})$ is finite and separable and therefore simple. Describe an infinite class of primitive elements for this extension. Find the minimal polynomial for each primitive element.
6. Let $E = F(\alpha_1, \ldots, \alpha_n)$ be separable over an infinite field F. Prove that there are an infinite number of n-tuples $(a_1, \ldots, a_n) \in F^n$ for which $E = F(a_1\alpha_1 + \cdots + a_n\alpha_n)$.
7. Show that the class of purely inseparable extensions is closed under the taking of arbitrary composites.
8. Let $F < E$. Define the *purely inseparable closure* of F in E and show that it is a field.
9. If $F < E$ is algebraic prove that any embedding $\sigma: E \to \overline{E}$ is uniquely determined by its restriction to $F^{sc}(E)$.
10. Prove that if $F < E$ is finite and expchar(F) = p then $[E:F]_i$ is a power of p.
11. Show that lifting an extension by a purely inseparable extension does not affect the separable degree. That is, show that if $F < E$ is algebraic and $F < P$ is purely inseparable then $[EP:P]_s = [E:F]_s$.
12. Let $F < S$ be finite separable and $F < P$ be finite purely inseparable. Prove that $P < SP$ is separable and $[SP:P] = [S:F]$. In fact, if B is a basis for S over F, prove that it is also a basis for SP over P.
13. Show that if $F < E$ is finite and $F < S$ is finite separable then $[ES:S]_i = [E:F]_i$.

14. Let $F < E$ be a finite extension and let $\alpha \in E$ be algebraic over F. Let H be the set of embeddings of E into $\overline{E}$ over F. The elements of H permute the roots of $p(x) = min(\alpha,F)$. Let β be a root of p(x). Show that $|\{\sigma \in H \mid \sigma\alpha = \beta\}| = [E:F(\alpha)]_s$. Hence, the multiset $\{\sigma\alpha \mid \sigma \in H\}$ contains $[E:F(\alpha)]_s$ copies of each root of p(x).
15. Let $F < E$ be a finite extension that is not separable. Show that for each $n \geq 1$ there exists a subfield E_n of E for which $E_n < E$ is purely inseparable and $[E:E_n]_i = p^n$.
16. Prove that if $F \neq pcl(F)$ then the extension $F < pcl(F)$ is infinite.

Part 2
Galois Theory

Chapter 5

Galois Theory I

5.1 Galois Connections

The traditional Galois correspondence between intermediate fields and subgroups of the Galois group is one of the main themes of this book. We choose to approach this theme through a more general concept, however.

Definition Let P and Q be partially ordered sets. A **Galois connection** on the pair (P,Q) is a pair (Π,Ω) of maps $\Pi:P\to Q$ and $\Omega:Q\to P$, where we write $\Pi(p) = p^*$ and $\Omega(q) = q'$, with the following properties:

1) (**order reversing**) For all $p \in P$, $q \in Q$,

$$p \leq q \Rightarrow p^* \geq q^* \quad \text{and} \quad r \leq s \Rightarrow r' \geq s'$$

2) For all $p \in P$, $q \in Q$,

$$p \leq p^{*\prime} \quad \text{and} \quad q \leq q'^{*}$$ □

Theorem 5.1.1 For any $p \in P$ and $q \in Q$, we have

1) $p^{*\prime *} = p^*$,
2) $q'^{*\prime} = q'$.

Proof. Since $p \leq p^{*\prime}$, the order reversing property of $*$ gives

$$p^{*\prime *} \leq p^* \leq (p^*)'^*$$

from which part 1) follows. Part 2) is similar. ∎

Corollary 5.1.2 The map $p \to p^{*\prime}$ is a **closure operation** on P, that is, if we denote $p^{*\prime}$ by $cl(p)$, then for all $p \in P$, $q \in Q$,

1) **(Extensive)**
$$p \leq cl(p)$$

2) **(Idempotent)**
$$cl(cl(p)) = cl(p)$$

3) **(Isotone)**
$$p \leq q \Rightarrow cl(p) \leq cl(q)$$

Similarly, the map $q \to q'^{*}$ is a closure operation on Q. □

Definition An element $p \in P$ is said to be **closed** if $cl(p) = p$, and similarly for Q. We denote the set of all closed elements in P by $Cl(P)$, and similarly for Q. □

Theorem 5.1.3 The image of any element under Π or Ω is closed. In addition, the maps Π and Ω are order-reversing bijective inverse maps between the sets $Cl(P)$ and $Cl(Q)$.

Proof. Theorem 5.1.1 shows that the image of an element under Π or Ω is closed. Moreover, if $q \in Cl(Q)$ is closed, then $q' \in Cl(P)$ and $\Pi q' = q'^{*} = cl(q) = q$ is in the image of Π, and so Π maps $Cl(P)$ onto $Cl(Q)$. If $p, r \in Cl(P)$ and $p^{*} = r^{*}$, then $p^{*\prime} = r^{*\prime}$, that is, $p = r$. Hence Π is injective. A similar argument applies to Ω. Finally, since $p^{*\prime} = p$ for $p \in Cl(P)$, it follows that $\Omega \circ \Pi = \iota$ on $Cl(P)$ and similarly, $\Pi \circ \Omega = \iota$ on $Cl(Q)$. ∎

Theorem 5.1.4 Let $\Pi: P \to Q$ and $\Omega: Q \to P$ be a Galois connection, where P and Q are lattices.

1) If $p_i \in Cl(P)$ and $\wedge p_i$ exists in P, then $\wedge p_i \in Cl(P)$. If P is a complete lattice then so is $Cl(P)$, with meet given by meet in P. Similar statements hold for Q.
2) *De Morgan's Laws* hold in $Cl(P)$ and $Cl(Q)$. That is, for p, $q \in Cl(P)$ and r, $s \in Cl(Q)$, we have

$$(p \wedge q)^{*} = p^{*} \vee q^{*},\ (p \vee q)^{*} = p^{*} \wedge q^{*}$$
$$(r \wedge s)' = r' \vee s',\ (r \vee s)' = r' \wedge s'$$

Proof. For part 1), suppose that $p_i \in Cl(P)$ and $\wedge p_i$ exists as a meet in P. Since $\wedge p_i \leq p_j$ for all j, we have $cl(\wedge p_i) \leq cl(p_j) = p_j$, whence $cl(\wedge p_i) \leq \wedge p_j$. Since the reverse inequality holds as well, we have equality, whence $\wedge p_i \in Cl(P)$. It follows from Theorem 0.1.1 that if P

is a complete lattice, so is $Cl(P)$, under meet in P.

For part 2), observe first that $p \wedge q \leq p$ and $p \wedge q \leq q$ imply that $(p \wedge q)^* \geq p^*$ and $(p \wedge q)^* \geq q^*$, whence $(p \wedge q)^* \geq p^* \vee q^*$. If $r \geq p^*$ and $r \geq q^*$ for $r \in Cl(P)$ then $r' \leq p$ and $r' \leq q$, whence $r' \leq p \wedge q$. Thus, $r \geq (p \wedge q)^*$. It follows by definition of join that $(p \wedge q)^* = p^* \vee q^*$. The other parts of De Morgan's Laws are proved similarly. ∎

Let $\mathbb{Z}^+$ denote the set of positive integers.

Definition We will say that a Galois connection (Π,Ω) on (P,Q) is **indexed** if the following hold. For each $p, q \in P$ with $p \leq q$, there exists a number $(q:p) \in \mathbb{Z}^+ \cup \{\infty\}$, called the **degree** of q over p. Similarly, for each $r, s \in Q$ with $r \leq s$, there exists a number $(s:r) \in \mathbb{Z}^+ \cup \{\infty\}$, called the **degree** of s over r. Moreover, the following properties hold.

1) (**Degree is multiplicative**) If $s_1, s_2, s_3 \in P$ or $s_1, s_2, s_3 \in Q$ then

$$s_1 \leq s_2 \leq s_3 \Rightarrow (s_3:s_1) = (s_3:s_2)(s_2:s_1)$$

2) (**Π and Ω are degree-nonincreasing**) If $p, q \in P$ then

$$p \leq q \Rightarrow (p^*:q^*) \leq (q:p)$$

If $r, s \in Q$ then

$$r \leq s \Rightarrow (r':s') \leq (s:r)$$

3) If $s, t \in P$ or $s, t \in Q$ then

$$(s:t) = 1 \Rightarrow s = t$$

If $(s:t) < \infty$, then s is said to be a **finite extension** of t. (We observe some obvious understandings about ∞; for instance, $n \leq \infty$ for all $n \in \mathbb{Z}^+$, $\infty \leq \infty$, $n \cdot \infty = \infty$ for $n \in \mathbb{Z}^+$ and $\infty \leq k \leq \infty$ implies $k = \infty$.) □

From now on, when writing (p:q), it is with the tacit assumption that $p \leq q$. While Π and Ω are degree-nonincreasing in general, these maps are degree *preserving* when restricted to $Cl(P)$ and $Cl(Q)$, as we now show.

Theorem 5.1.5 Let (Π,Ω) be an indexed Galois connection on (P,Q).

1) If $p, q \in Cl(P)$ and $p \leq q$ then $(q:p) = (p^*:q^*)$.
2) If $p \in Cl(P)$ and $(q:p) < \infty$ then $q \in Cl(P)$. In particular, if 0 is closed and $(1:0)$ is finite then all elements are closed.

Similar statements hold for Q.

Proof. If $p \in Cl(P)$ then $p = p^{*\prime}$ and so

$$(q{:}p) \geq (p^*{:}q^*) \geq (q^{*\prime}{:}p^{*\prime}) = (q^{*\prime}{:}p) = (q^{*\prime}{:}q)(q{:}p)$$

If $q \in Cl(P)$ then $q^{*\prime} = q$, equality holds throughout and part 1) is proved. If $(q{:}p)$ is finite then we may cancel to get $(q^{*\prime}{:}q) = 1$, which implies that $q = q^{*\prime}$ is closed. This proves part 2). ∎

Thus, an indexed Galois connection induces a degree-preserving, order-reversing bijection between $Cl(P)$ and $Cl(Q)$.

5.2 The Galois Correspondence

Now we describe one of the most important Galois connections.

Definition The **Galois group** of an extension $F < E$, denoted by $G_F(E)$, is the group of all automorphisms of E over F. □

Note that when $F < E$ is algebraic, Theorem 2.8.2 implies that $G_F(E) = Hom_F(E,E)$.

Let $F < E$ and let $\mathfrak{F}$ be the complete lattice of all intermediate fields, that is, fields K such that $F < K < E$, ordered by set inclusion. Let $\mathfrak{G}$ be the complete lattice of all subgroups of the Galois group $G_F(E)$, ordered by set inclusion. We define two maps $\Pi{:}\mathfrak{F} \to \mathfrak{G}$ and $\Omega{:}\mathfrak{G} \to \mathfrak{F}$ by

$$\Pi(K) = G_K(E)$$

and

$$\Omega(H) = F(H) = \{\alpha \in E \mid \sigma\alpha = \alpha \text{ for all } \sigma \in H\}$$

where $F(H)$ is the fixed field of H.

Theorem 5.2.1 Let $F < E$. The pair of maps (Π,Ω) defined by $\Pi{:}K \mapsto G_K(E)$ and $\Omega{:}H \mapsto F(H)$ is a Galois connection. We refer to it as the **Galois correspondence** of $F < E$.

Proof. It is clear from the definitions that

$$K \subseteq J \Rightarrow G_J(E) \subseteq G_K(E)$$

and

$$H \subseteq I \Rightarrow F(I) \subseteq F(H)$$

Also, any element of K is fixed by every element of $G_K(E)$, that is,

$$K \subseteq F(G_K(E))$$

Finally, any $\sigma \in J$ fixes every element in $F(J)$, that is,

$$J \subseteq G_{F(J)}(E) \qquad \blacksquare$$

Since $\mathfrak{F}$ and $\mathfrak{G}$ are complete lattices, Theorem 5.1.4 gives

Corollary 5.2.2 The set $Cl(\mathfrak{F})$ of closed intermediate fields and the set $Cl(\mathfrak{G})$ of closed subgroups of $G_F(E)$ are complete lattices, where meet is intersection. In particular, the intersection of closed intermediate fields is closed and the intersection of closed subgroups is closed. □

We would like to show that the Galois correspondence of an algebraic extension $F < E$ is indexed, where $(K:L) = [K:L]$ is the degree of the extension $F < E$ and $(H:J)$ is the index of the subgroup J in the group H. It is not hard to see that these degrees satisfy the first and third properties in the definition of an indexed correspondence. The next theorem shows that the map $\Pi: K \mapsto G_K(E)$ is degree-nonincreasing.

Theorem 5.2.3 Let $F < E$ be algebraic and let $F < L < K < E$. Then

$$(G_L(E):G_K(E)) \leq [K:L]_s \leq [K:L] \tag{5.2.1}$$

1) If $F < E$ is normal, then equality holds in the first inequality in (5.2.1) and the map $\psi: G_L(E) \to Hom_L(K,E)$ defined by $\psi\sigma = \sigma \mid_K$ induces a bijection

$$\frac{G_L(E)}{G_K(E)} \leftrightarrow Hom_L(K,E)$$

2) If $F < E$ is both normal and separable, then equality holds throughout (5.2.1).

Proof. If $\sigma, \tau \in G_L(E)$, the following are equivalent

$$\sigma \mid_K = \tau \mid_K$$
$$\tau^{-1}\sigma\alpha = \alpha, \text{ for all } \alpha \in K$$
$$\tau^{-1}\sigma \in G_K(E)$$
$$\sigma \in \tau G_K(E)$$

Thus, $\psi\sigma = \psi\tau$ if and only if σ and τ lie in the same coset of $G_K(E)$. Hence ψ induces a bijection from the set of cosets of $G_K(E)$ in $G_L(E)$

onto $Im(\psi)$. Since

$$Im(\psi) \subseteq Hom_L(K,E) \subseteq Hom_L(K,\overline{E})$$

we get

$$\begin{aligned}(G_L(E):G_K(E)) = |\, Im(\psi)\,| &\leq |\, Hom_L(K,E)\,| \\ &\leq |\, Hom_L(K,\overline{E})\,| = [K:L]_s\end{aligned}$$

which proves the first part of the theorem.

To prove part 1), suppose that $F < E$ is normal. Then $L < E$ is also normal. If $\sigma \in Hom_L(K,\overline{E})$ then σ can be extended to $\overline{\sigma} \in Hom_L(E,\overline{E}) = G_L(E)$. It follows that σ maps K into E, whence $\sigma \in Hom_L(K,E)$ and so $Hom_L(K,\overline{E}) = Hom_L(K,E)$. Moreover, since any $\sigma \in Hom_L(K,E)$ can be extended to $\overline{\sigma} \in G_L(E)$ and since $\sigma = \psi\overline{\sigma} \in Im(\psi)$, it follows that $Im(\psi) = Hom_L(K,E)$ and so equality holds in both inequalities in the previous display. This proves part 1). Part 2) is clear. ∎

To show that the map $H \mapsto F(H)$ is degree-nonincreasing, we require a preliminary result.

Theorem 5.2.4 Let $F < E$. Let $H \subseteq G_F(E)$. For $\alpha \in E$, define $\hat{\alpha}:H \to E$ by $\hat{\alpha}\sigma = \sigma\alpha$ (thus, $\hat{\alpha}$ is evaluation at α). Then $\alpha_1,\ldots,\alpha_n$ are linearly independent over $F(H)$ if and only if $\hat{\alpha}_1,\ldots,\hat{\alpha}_n$ are linearly independent over E.

Proof. Suppose that the $\hat{\alpha}_i$'s are independent over E, and let $\sum a_i\alpha_i = 0$ where $a_i \in F(H)$. Then for any $\sigma \in H$,

$$0 = \sigma\Big(\sum a_i\alpha_i\Big) = \sum a_i(\sigma\alpha_i) = \sum a_i(\hat{\alpha}_i\sigma)$$

Hence $\sum a_i\hat{\alpha}_i = 0$, implying that $a_i = 0$ for all i.

For the converse, suppose that $\alpha_1,\ldots,\alpha_n$ are independent over $F(H)$ and let $\sum x_i\hat{\alpha}_i = 0$ on H. If this equation has a nonzero solution $x_1,\ldots,x_n$ in E, consider a solution with the fewest number of nonzero entries and, by renumbering if necessary, assume the nonzero entries to be $x_1,\ldots,x_s$. Dividing by x_s if necessary, we may also assume that $x_s = 1$. Thus

$$x_1\hat{\alpha}_1 + \cdots + x_{s-1}\hat{\alpha}_{s-1} + \hat{\alpha}_s = 0 \tag{5.2.2}$$

Equation (5.2.2) is equivalent to

$$x_1(\sigma\alpha_1) + \cdots + x_{s-1}(\sigma\alpha_{s-1}) + \sigma\alpha_s = 0 \tag{5.2.3}$$

for all $\sigma \in H$. In particular, for σ equal to the identity map, we get

$$x_1\alpha_1 + \cdots + x_{s-1}\alpha_{s-1} + \alpha_s = 0$$

which implies, owing to the independence of the α_i's, that not all of the x_i's can lie in $F(H)$. Let us assume that $x_1 \notin F(H)$.

Applying $\tau \in H$ to (5.2.3) gives

$$\tau(x_1)(\tau\sigma\alpha_1) + \cdots + \tau(x_{s-1})(\tau\sigma\alpha_{s-1}) + \tau\sigma\alpha_s = 0$$

for all $\sigma \in H$. But as σ varies over the subgroup H so does $\tau\sigma$ and so

$$\tau(x_1)(\sigma\alpha_1) + \cdots + \tau(x_{s-1})(\sigma\alpha_{s-1}) + \sigma\alpha_s = 0$$

for all $\sigma,\tau \in H$, or equivalently,

$$(\tau x_1)\hat{\alpha}_1 + \cdots + (\tau x_{s-1})\hat{\alpha}_{s-1} + \hat{\alpha}_s = 0 \tag{5.2.4}$$

Since $x_1 \notin F(H)$, we may choose $\tau \in H$ such that $\tau(x_1) \neq x_1$. Finally, subtracting (5.2.2) from (5.2.4) gives

$$[(\tau x_1) - x_1]\hat{\alpha}_1 + \cdots + [(\tau\hat{\alpha}_{s-1}) - x_{s-1}]\hat{\alpha}_{s-1} = 0$$

which is shorter than (5.2.2). This contradiction completes the proof. ∎

Now we can show that the map $H \mapsto F(H)$ is degree-nonincreasing.

Theorem 5.2.5 Let $F < E$ be algebraic and let H and J be subgroups of $G_F(E)$ with $J \subseteq H \subseteq G_F(E)$. Then

$$[F(J):F(H)] \leq (H:J)$$

Proof. If $(H:J) = \infty$ there is nothing to prove, so let $(H:J) = r < \infty$. Choose one σ_i from each coset of J in H, for $i = 1,\ldots,r$. Let $\alpha_1,\ldots,\alpha_n \in F(J)$ be linearly independent over $F(H)$ and assume for the purposes of contradiction that $n > r$. The system

$$\begin{aligned} x_1(\hat{\alpha}_1\sigma_1) + x_2(\hat{\alpha}_2\sigma_1) + \cdots + x_n(\hat{\alpha}_n\sigma_1) &= 0 \\ &\vdots \\ x_1(\hat{\alpha}_1\sigma_r) + x_2(\hat{\alpha}_2\sigma_r) + \cdots + x_n(\hat{\alpha}_n\sigma_r) &= 0 \end{aligned}$$

has more unknowns than equations and so it has a nonzero solution $x_1,\ldots,x_n$ in E. Hence, there exist $\beta_1,\ldots,\beta_n \in E$, not all 0, such that

$$\beta_1(\widehat{\alpha}_1\sigma_i) + \cdots + \beta_n(\widehat{\alpha}_n\sigma_i) = 0 \tag{5.2.5}$$

for all $i = 1,\ldots,r$.

Now, any $\tau \in H$ has the form $\tau = \sigma_i\rho$ where $\rho \in J$. Since $\alpha_j \in F(J)$, we have $\rho\alpha_j = \alpha_j$ and so

$$\widehat{\alpha}_j\tau = \widehat{\alpha}_j(\sigma_i\rho) = (\sigma_i\rho)(\alpha_j) = \sigma_i\alpha_j = \widehat{\alpha}_j\sigma_i$$

Hence, it follows from (5.2.5) that

$$\beta_1\widehat{\alpha}_1 + \cdots + \beta_n\widehat{\alpha}_n = 0$$

as a map on H. This contradicts the previous theorem, which says that the $\widehat{\alpha}_i$'s are independent over E. Hence $n \leq r$. ∎

Thus, the Galois correspondence of an algebraic extension $F < E$ is indexed. As a consequence, we have the following theorem.

Theorem 5.2.6 Let $F < E$ be algebraic and let (Π,Ω) be the Galois correspondence of $F < E$. Then (Π,Ω) is indexed. Hence

1) Π and Ω are degree-nonincreasing, order-reversing maps.
2) Π and Ω are degree-preserving, order-reversing bijections (inverses of each other) between the lattice $Cl(\mathfrak{F})$ of closed intermediate fields of $F < E$ and the lattice $Cl(\mathfrak{G})$ of closed subgroups of the Galois group $G_F(E)$. More specifically,
   a) If $F < L < K < E$ with K, L closed then

$$[K:L] = (G_L(E):G_K(E))$$

   b) If $J \subseteq H \subseteq G_F(E)$ with H, J closed then

$$(H:J) = [F(J):F(H)]$$

   c) For $K, L \in Cl(\mathfrak{F})$ and $H, J \in Cl(\mathfrak{G})$, we have

$$G_{K\cap L}(E) = G_K(E) \vee G_L(E), \quad G_{K\vee L}(E) = G_K(E) \cap G_L(E)$$
$$F(H \cap J) = F(H) \vee F(J), \quad F(H \wedge J) = F(H) \cap F(J)$$

In addition, any finite extension of a closed intermediate field or closed subgroup is closed. □

We should note that the joins in part 2c) of the previous theorem are joins in the corresponding lattices. Thus, for instance, $G_K(E) \vee G_L(E)$ is

the smallest *closed* subgroup of $G_F(E)$ containing $G_K(E)$ and $G_L(E)$, which need not be the smallest subgroup of $G_F(E)$ containing these groups. (In other words, $Cl(\mathfrak{F})$ need not be a sublattice of $\mathfrak{F}$ and $Cl(\mathfrak{G})$ need not be a sublattice of $\mathfrak{G}$.)

Corollary 5.2.7 If $F < E$ is finite then $| G_F(E) | < \infty$. □

5.3 Who's Closed?

We turn our attention to the question of which intermediate fields of an extension and which subgroups of the Galois group are closed.

Definition A normal separable extension is called a **Galois extension.** □

The next theorem follows from the relevant properties of normal and separable extensions.

Theorem 5.3.1

1) Let $F < K < E$. If $F < E$ is Galois then $K < E$ is Galois.
2) The class of Galois extensions is closed under lifting: If $F < E$ is Galois and $F < K$ then $K < EK$ is Galois.
3) The class of Galois extensions is closed under arbitrary composites and intersections: If $F < E_i$ are Galois and $\vee E_i$ is defined then $F < \vee E_i$ is Galois and $F < \bigcap E_i$ is Galois. □

It is not hard to describe the closed intermediate fields of an algebraic extension $F < E$.

Theorem 5.3.2 Let $F < E$ be algebraic and consider the Galois correspondence on $F < E$.

1) An intermediate field K is closed if and only if $K < E$ is a Galois extension.
2) If K is closed and $K < L < E$ then L is also closed.
3) The following are equivalent.
   a) F is closed.
   b) $F < E$ is a Galois extension.
   c) All intermediate fields are closed.

Proof. According to Theorem 4.7.4, if $K < E$ is normal then $cl(K) = F(G_K(E)) = K^{ic}$, the purely inseparable closure of K in E. Hence, if $K < E$ is Galois then $cl(K) = K$. For the converse, suppose that K is closed. Let $\alpha \in E$ with $p(x) = min(\alpha, K)$ of degree n. Since $[K(\alpha):K]$ is finite, we know that $K(\alpha)$ is closed and

$$n = [K(\alpha):K] = (G_K(E):G_{K(\alpha)}(E))$$

Let $\sigma_1,\ldots,\sigma_n$ be a complete set of coset representatives of $G_{K(\alpha)}(E)$ in $G_K(E)$. It is easy to see that $\tau \in \sigma_i G_{K(\alpha)}(E)$ if and only if $\tau\alpha = \sigma_i\alpha$. Hence there are precisely n distinct images of α under the Galois group $G_K(E)$. But each of these images is a root of the minimal polynomial p(x) and so p(x) is separable with all of its roots in E. Hence $K < E$ is both separable and normal. This proves statement 1) and shows that 3a) and 3b) are equivalent. All of the statements in 3) are equivalent since $F < E$ is Galois if and only if $K < E$ is Galois for all intermediate fields K. Similarly, 2) follows from 1). ∎

Note that if $F < E$ is algebraic then E is closed since $E = F(\langle\iota\rangle)$ where $\iota \in G_F(E)$ is the identity.

If K is a closed intermediate field, then

$$[E:K] = (G_K(E):G_E(E)) = |\, G_K(E)\,|$$

In the finite case, the converse also holds.

Theorem 5.3.3 Let $F < E$ be a finite extension.

1) An intermediate field K is closed if and only if $[E:K] = |\, G_K(E)\,|$.
2) The following are equivalent.
   a) $F < E$ is Galois.
   c) F is closed.
   d) All intermediate fields are closed.
   e) $[E:K] = |\, G_K(E)\,|$ for all intermediate fields K.
   f) $[E:F] = |\, G_F(E)\,|$.

Proof. We have seen that K closed implies $[E:K] = |\, G_K(E)\,|$. Conversely, if $[E:K] = |\, G_K(E)\,|$ then

$$[E:K] = (G_K(E):G_E(E)) = [F(G_E(E)):F(G_K(E))] = [E:F(G_K(E))]$$

and so the finiteness of $F < E$ implies that $K = F(G_K(E))$, that is, K is closed. Part 2) follows from the previous theorem. ∎

As for the matter of which subgroups are closed, let $F < E$ be algebraic. Since the trivial subgroup $G_E(E) = \langle\iota\rangle$ is closed, any finite subgroup of $G_F(E)$ is closed. Thus, if $F < E$ is finite then $G_F(E)$ is finite and all subgroups are closed. We may now give a complete answer to the question of who's closed in the finite case.

Theorem 5.3.4 If $F < E$ is finite then all subgroups of the Galois group $G_F(E)$ are closed and an intermediate field K is closed if and only if $K < E$ is a Galois extension. In particular, if $F < E$ is Galois then all intermediate fields are closed. □

As the next example shows, in the general algebraic case, not all subgroups need be closed.

Example 5.3.1 For this example, we borrow from a later chapter the fact that for any prime power p^d, there exists a finite field $GF(p^d)$ of size p^d and $GF(p^d) < GF(p^r)$ if and only if $d \mid r$.

Let $F = \mathbb{Z}_p$ and let $E = \overline{F}$ be an algebraic closure of F. Since F is a finite field, it is perfect and so $F < E$ is separable. Since E is algebraically closed, $F < E$ is normal. Hence $F < E$ is a Galois extension and therefore F is closed. Let $H = \langle \sigma_p \rangle$ be the subgroup of $G_F(E)$ generated by the Frobenius map $\sigma_p : \alpha \to \alpha^p$. The fixed field $F(H)$ is the set of all $\alpha \in E$ for which $\alpha^p = \alpha$, in other words, the roots in E of the polynomial $p(x) = x^p - x$. But $p(x)$ has p roots in F and so $F(H) = F$. It follows that

$$cl(H) = G_{F(H)}(E) = G_F(E)$$

Hence, all we need do is show that $H \neq G_F(E)$ to conclude that H is not closed.

Let q be a prime and consider the field

$$P = GF(p^q) \cup GF(p^{q^2}) \cup GF(p^{q^3}) \cup \cdots$$

Then P is a proper subfield of E, since it does not contain, for instance, the subfield $GF(p^{q+1})$. Hence $[E:P] > 1$ and since $P < E$ is Galois, the group $G_P(E)$ is not trivial. Let $\sigma \in G_P(E)$. If $\sigma \in H$ then $\sigma = \sigma_p^k$ for some k and so

$$F(\langle \sigma \rangle) = \{\alpha \in E \mid \sigma_p^k \alpha = \alpha\} = \{\alpha \in E \mid \alpha^{p^k} = \alpha\}$$

is the set of roots in E of the polynomial $x^{p^k} - x$. Hence $F(\langle \sigma \rangle)$ is finite. But $F(\langle \sigma \rangle)$ contains the infinite set P. This contradiction implies that $\sigma \notin H$ and so $H \neq G_F(E)$. □

The Galois correspondence begins with a field extension $F < E$ and the corresponding Galois group $G_F(E)$. We may also begin with a field E and a group G of automorphisms of E. Then we can form the fixed field

$$F(G) = \{\alpha \in E \mid \sigma\alpha = \alpha \text{ for all } \sigma \in G\}$$

and consider the Galois correspondence (Π,Ω) on $F(G) < E$. Since G is a subgroup of $G_{F(G)}(E)$, it is in the domain of the map Ω and so $F(G) = \Omega(G)$. Hence, $F(G)$ is closed under the Galois correspondence and so $F(G) < E$ is a Galois extension. If G is closed, which happens, for instance, when G is finite, then $G_{F(G)}(E) = G$.

Theorem 5.3.5 Let E be a field and let G be a group of automorphisms of E. Then the extension $F(G) < E$ is Galois. If G is closed (for example, if G is finite) then $G = G_{F(G)}(E)$. □

5.4 Normal Subgroups and Normal Extensions

If $F < E$ is normal and K is an intermediate field, we know that $K < E$ is also normal, but $F < K$ need not be. However, we can neatly describe when $F < K$ is normal in terms of Galois groups. (This is an example of the power and purpose of Galois theory.)

Suppose first that $F < K$ is normal ($F < E$ need not be normal). Since any $\tau \in G_F(E)$ sends K onto itself, it follows that $\tau^{-1}\sigma\tau \in G_K(E)$ for any $\sigma \in G_K(E)$, that is, $G_K(E)$ is a normal subgroup of $G_F(E)$, in symbols, $G_K(E) \triangleleft G_F(E)$.

Conversely, suppose that $G_K(E) \triangleleft G_F(E)$. We want to show that $F < K$ is normal. Let $\alpha \in K$ have minimal polynomial p(x) over F. If β is any other root of p(x), then Theorem 2.8.4 implies the existence of a $\tau \in \mathrm{Hom}_F(E,\overline{E})$ such that $\tau\alpha = \beta$. If $F < E$ is normal, then $\tau \in G_F(E)$. If $\sigma \in G_K(E)$, the normality of $G_K(E)$ implies that $\sigma\tau = \tau\sigma'$ for some $\sigma' \in G_K(E)$ and so

$$\sigma\beta = \sigma\tau\alpha = \tau\sigma'\alpha = \tau\alpha = \beta$$

Thus, σ fixes all of the roots of p(x) and so all of the roots of p(x) lie in $F(G_K(E))$. If K is closed, then all of the roots of p(x) lie in K and so K is normal over F. We have proven most of the following.

Theorem 5.4.1 Let $F < K < E$.

1) If $F < K$ is normal then $G_K(E) \triangleleft G_F(E)$.
2) If $F < E$ is normal, $K < E$ is Galois and $G_K(E) \triangleleft G_F(E)$ then $F < K$ is normal.
3) If $F < E$ is Galois then $F < K$ is normal if and only if $G_K(E) \triangleleft G_F(E)$.

Moreover, if $F < K$ and $F < E$ are normal, the map $\psi: G_F(E) \to G_F(K)$ defined by

$$\psi\sigma \to \sigma \mid_K$$

is an epimorphism whose kernel is $G_K(E)$. Thus,

$$G_F(K) \simeq \frac{G_F(E)}{G_K(E)}$$

Proof. We need only prove the last statement. Let $\sigma \in G_F(E)$. Since $F < K$ is normal, the restriction $\sigma \mid_K$, being an embedding of K into $\overline{E}$ over F, is an automorphism of K and thus lies in $G_F(K)$. Hence ψ maps $G_F(E)$ to $G_F(K)$. Moreover, for $\sigma, \tau \in G_F(E)$, we have

$$(\sigma\tau) \mid_K = \sigma(\tau \mid_K) = (\sigma \mid_K)(\tau \mid_K)$$

which shows that ψ is a group homomorphism. The kernel of ψ is $G_K(E)$ since if $\sigma \in G_F(E)$ then $\sigma \mid_K = \iota$ if and only if $\sigma \in G_K(E)$. Finally, the map ψ is surjective since the normality of $F < E$ implies that any $\sigma \in G_F(K)$ can be extended to an element of $G_F(E)$, whose restriction to K is σ. ∎

5.5 More on Galois Groups

We now examine the behavior of Galois groups under lifting and under the taking of composites. We assume that all composites mentioned are defined.

Theorem 5.5.1 (The Galois group of a lifting) Let $F < E$ be Galois and let $F < K$. Then $K < EK$ is Galois. Moreover, the restriction map $\psi: G_K(EK) \to G_{K \cap E}(E)$ defined by $\psi\sigma = \sigma \mid_E$ is an isomorphism. Thus

$$G_K(EK) \simeq G_{K \cap E}(E)$$

In addition,

1) $K \cap E = F$ implies $G_K(EK) \simeq G_F(E)$.
2) If $F < E$ is finite, then $G_K(EK) \simeq G_F(E)$ implies $K \cap E = F$.

Proof. We have already seen that $K < EK$ is Galois. The normality of $F < E$ implies that ψ is a homomorphism from $G_K(EK)$ into $G_{K \cap E}(E)$. If $\sigma \in G_K(EK)$ and $\sigma \mid_E = \iota$ then σ fixes E as well as K and so it fixes all elements of EK, whence $\sigma = \iota$. Thus ψ is injective. It remains to show that $Im\,\psi = G_{K \cap E}(E)$.

To avoid confusion, let us use the notation $F_E(\cdot)$ for the fixed field with respect to the Galois correspondence on $F < E$, and $F_{EK}(\cdot)$ for the fixed field with respect to the Galois correspondence on $K < EK$. Since $K < EK$ is Galois, we deduce that K is closed with respect to the Galois

correspondence on $K < EK$ and so

$$\begin{aligned} F_E(Im\ \psi) &= \{\alpha \in E \mid \tau\alpha = \alpha \text{ for all } \tau \in Im(\psi)\} \\ &= \{\alpha \in E \mid (\sigma \mid_E)\alpha = \alpha \text{ for all } \sigma \in G_K(EK)\} \\ &= \{\alpha \in E \mid \sigma\alpha = \alpha \text{ for all } \sigma \in G_K(EK)\} \\ &= E \cap F_{EK}(G_K(EK)) \\ &= E \cap K \end{aligned}$$

Now, if we show that $Im\ \psi$ is closed with respect to the Galois correspondence on $F < E$, it follows by taking Galois groups that

$$Im\ \psi = G_{K \cap E}(E)$$

and thus ψ is surjective, completing the proof. If $F < E$ is finite, then all subgroups of the Galois group $G_F(E)$ are closed, and we are finished. We will postpone the proof in the infinite case until we have discussed the Krull topology, later in this chapter.

Finally, statement 1) is clear. As to statement 2), we have $G_F(E) \simeq G_{K \cap E}(E)$ and since $G_{K \cap E}(E) < G_F(E)$ with both finite, we deduce that $G_{K \cap E}(E) = G_F(E)$, whence $K \cap E = F$ follows by taking fixed fields. ∎

Theorem 5.5.1 yields a plethora of useful statements about degrees, all of which can be read from Figure 5.5.1. We leave details of the proof to the reader. [Part 3) of the next result is particularly useful.]

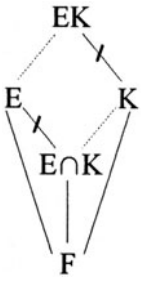

Figure 5.5.1

Corollary 5.5.2 Suppose that $F < E$ is finite Galois and $F < K$, with EK defined. Then

1) $[EK:K] = [E:E \cap K]$ and $[EK:K] \mid [E:F]$.

If $F < K$ is also finite then

2) $[EK:F] = [E:E \cap K][K:F]$ and $[EK:F] \mid [E:F][K:F]$.

3) $[EK:F] = [E:F][K:F]$ if and only if $E \cap K = F$.

More generally, if $F < E_i$ is finite Galois for $i = 1,\ldots,n-1$ and $F < E_n$ is finite then

4) $$[E_1 \cdots E_n:F] = \prod_{i=1}^{n} [E_i:E_i \cap (E_{i+1} \cdots E_n)]$$
where $E_{i+1} \cdots E_n = F$ when $i = n$.

5) $[E_1 \cdots E_n:F] = \prod_{i=1}^{n} [E_i:F]$ if and only if $E_i \cap (E_{i+1} \cdots E_n) = F$ for all i,
where $E_{i+1} \cdots E_n = F$ when $i = n$. □

We now turn to the Galois group of a composite.

Theorem 5.5.3 (The Galois group of a composite) Let $\mathfrak{F} = \{E_i \mid i \in I\}$ be a family of fields, all contained in a larger field. If $F < E_i$ is Galois over F for all $i \in I$, then the composite $\vee E_i$ is Galois over F. If $G = \prod G_F(E_i)$ is the direct product of the Galois groups $G_F(E_i)$ and if $\pi_i: G \to G_F(E_i)$ is projection onto the i-th coordinate, then the map

$$\psi: G_F(\vee E_i) \to \prod G_F(E_i)$$

defined by

$$\pi_i(\psi\sigma) = \sigma \mid_{E_i}$$

is a monomorphism of groups. Hence, $G_F(\vee E_i)$ is isomorphic to a subgroup of the direct product $\prod G_F(E_i)$.

Moreover, if $\mathfrak{F} = \{E_1,\ldots,E_n\}$ is a finite family of finite extensions, then the following are equivalent

1) ψ is an isomorphism and

$$G_F(E_1 \vee \cdots \vee E_n) \simeq G_F(E_1) \times \cdots \times G_F(E_n)$$

2) $E_i \cap (E_{i+1} \cdots E_n) = F$ for all $i = 1,\ldots,n$.

Proof. Let $K = \vee E_i$. We have already seen that $F < K$ is Galois. Let $\sigma \in G_F(K)$. Since each $F < E_i$ is normal, we have $\sigma \mid_{E_i} \in G_F(E_i)$. If $\tau \in G_F(K)$ then

$$\pi_i(\psi(\sigma\tau)) = (\sigma\tau) \mid_{E_i} = (\sigma \mid_{E_i})(\tau \mid_{E_i}) = \pi_i(\psi\sigma)\pi_i(\psi\tau) = \pi_i[(\psi\sigma)(\psi\tau)]$$

and so $\psi(\sigma\tau) = (\psi\sigma)(\psi\tau)$. Thus, ψ is a homomorphism of groups. If

$\sigma \mid_{E_i} = \iota$ for all $i \in I$, then since each element of K is a rational function (over F) in finitely many elements of $\bigcup E_i$, we must have $\sigma = \iota$, whence ψ is injective.

When $\mathfrak{F}$ is a finite family of finite extensions, all Galois groups are finite. It follows that

$$| Im\, \psi | = | G_F(\vee E_i) | = [\vee E_i : F]$$

and

$$| \prod G_F(E_i) | = \prod | G_F(E_i) | = \prod [E_i : F]$$

Hence ψ is surjective if and only if $[\vee E_i : F] = \prod [E_i : F]$ and Corollary 5.5.2 gives the desired result. ∎

The following corollary will prove useful.

Corollary 5.5.4 Suppose that $F < E$ is a finite Galois extension with Galois group of the form

$$G = G_F(E) = G_1 \times \cdots \times G_n$$

If

$$H_i = G_1 \times \cdots \times \{\iota\} \times \cdots \times G_n$$

where $\{\iota\}$ is in the i-th coordinate and if $E_i = F(H_i)$ then

1) $F < E_i$ is Galois with Galois group $G_F(E_i) \simeq G_i$,
2) $E = E_1 \vee \cdots \vee E_n$,
3) $E_i \cap (E_{i+1} \cdots E_n) = F$ for all $i = 1, \ldots, n$.

Proof. Since $F < E$ is finite and Galois, all intermediate fields and all subgroups of G are closed. Since $H_i \lhd G$, it follows from Theorem 5.4.1 that $F < E_i$ is a Galois extension and

$$G_F(E_i) \simeq \frac{G_F(E)}{G_{E_i}(E)} = \frac{G}{H_i} \simeq G_i$$

In addition, $F < \vee E_i$ is Galois. Since

$$G_{\vee E_i}(E) = \bigcap G_{E_i}(E) = \bigcap H_i = \{\iota\} = G_E(E)$$

taking fixed fields gives $\vee E_i = E$. Hence, $G_F(\vee E_i) \simeq \prod G_F(E_i)$ and Theorem 5.5.3 implies that $E_i \cap (E_{i+1} \cdots E_n) = F$ for all $i = 1, \ldots, n$. ∎

Abelian and Cyclic Extensions

Extensions are often named after their Galois groups. Here is a very important example.

Definition An extension $F < E$ is **abelian** if it is Galois and if the Galois group $G_F(E)$ is abelian. An extension $F < E$ is **cyclic** if it is Galois and if the Galois group $G_F(E)$ is cyclic. □

The basic properties of abelian and cyclic extensions are given in the next theorem, whose proof is left as an exercise.

Theorem 5.5.5

1) If $F < E$ and $F < K$ are abelian, then $F < EK$ is abelian.
2) If $F < E$ is abelian (cyclic) and $F < K$, then $K < EK$ is abelian (cyclic).
3) If $F < K < E$ with $F < E$ abelian (cyclic), then $F < K$ and $K < E$ are abelian (cyclic). □

*5.6 Linear Disjointness

If $F < K$ and $F < L$ are finite extensions, the degree $[KL:F]$ provides a certain measure of the "independence" of the extensions. Assuming that $[K:F] \leq [L:F]$, we have

$$[L:F] \leq [KL:F] \leq [L:F][K:F]$$

The "least" amount of independence occurs when $[KL:F] = [L:F]$, or equivalently, when $K < L$ and the "greatest" amount of independence occurs when

$$[KL:F] = [K:F][L:F] \tag{5.6.1}$$

We have seen (Corollary 5.5.2) that, if one of the extensions is Galois, then (5.6.1) holds if and only if $K \cap L = F$. For finite extensions in general, we cannot make such a simple statement. However, we can express (5.6.1) in a variety of useful ways. For instance, (5.6.1) holds for arbitrary finite extensions if and only if whenever $\{\alpha_i\} \subseteq K$ is linearly independent over F and $\{\beta_j\} \subseteq L$ is independent over F then $\{\alpha_i\beta_j\}$ is also independent over F.

To explore the situation more fully (and for not necessarily finite extensions), it is convenient to employ tensor products. (All that is needed about tensor products is contained in Chapter 0.)

Let $F < K$ and $F < L$. The multiplication map $\sigma: K \times L \to KL$ defined by $\sigma(\alpha,\beta) = \alpha\beta$ is bilinear and so there exists a unique linear map $\psi: K \otimes L \to KL$ for which $\psi(\alpha \otimes \beta) = \alpha\beta$. (The tensor product is over F.) This map is a morphism of F-algebras, since

$$\psi[(\alpha \otimes \beta)(\gamma \otimes \delta)] = \psi(\alpha\gamma \otimes \beta\delta) = \alpha\gamma\beta\delta = (\alpha\beta)(\gamma\delta) = \psi(\alpha \otimes \beta)\psi(\gamma \otimes \delta)$$

Note that the image of ψ is the F-algebra $K[L] = L[K]$ of all elements of the form

$$k_1\ell_1 + \cdots + k_n\ell_n$$

for $k_i \in K$ and $\ell_i \in L$. Hence, if $F < K$ or $F < L$ is algebraic, then $KL = K[L]$ and so the map ψ is surjective.

If F is a field, we use the term **F-independent** to mean linearly independent over F.

Theorem 5.6.1 Let $F < E$ and suppose that K and L are intermediate fields. The following are equivalent.

1) The linear map ψ defined above is injective.
2) If $\{\alpha_i\} \subseteq K$ is F-independent then it is also L-independent.
3) If $\{\alpha_i\} \subseteq K$ and $\{\beta_j\} \subseteq L$ are both F-independent then $\{\alpha_i\beta_j\}$ is also F-independent.
4) If $\{\alpha_i\}$ is a basis for K over F and $\{\beta_j\}$ is a basis for L over F then $\{\alpha_i\beta_j\}$ is a basis for K[L] over F.
5) There is a basis for K over F that is L-independent.

If $F < K$ and $F < L$ are finite, then each of 1) to 5) is equivalent to

6) $[KL:F] = [K:F][L:F]$.

If $F < K$ and $F < L$ are finite and one is Galois, then each of 1) to 6) is equivalent to

7) $K \cap L = F$.

Proof. [1⇒2] Let $\{\alpha_i\} \subseteq K$ be F-independent and suppose that $\sum \ell_i\alpha_i = 0$ for $\ell_i \in L$. Since ψ is a monomorphism and

$$\psi(\sum \ell_i \otimes \alpha_i) = \sum \ell_i\alpha_i = 0$$

we have

$$\sum \ell_i \otimes \alpha_i = 0$$

Theorem 0.8.2 now implies that $\ell_i = 0$ for all i.

[2⇒3] Let $\{\alpha_i\}$ and $\{\beta_j\}$ be F-independent. If

$$\sum_{i,j} a_{ij}\alpha_i\beta_j = 0$$

with $a_{ij} \in F$ then since $\{\alpha_i\}$ is also L-independent, the coefficients of α_i must equal 0, that is,

$$\sum_j a_{ij}\beta_j = 0$$

for all i. Since the β_i's are also F-independent, we get $a_{ij} = 0$ for all i, j.

[3⇒4] This follows from the fact that if $\{\alpha_i\}$ spans K over F and $\{\beta_j\}$ spans L over F then $\{\alpha_i\beta_j\}$ spans K[L] over F.

[4⇒1] The map ψ sends a basis $\{\alpha_i \otimes \beta_j\}$ for $K \otimes L$ to a basis $\{\alpha_i\beta_j\}$ for K[L] and is therefore injective.

Thus, each of 1) to 4) is equivalent, and by symmetry we may add the equivalent statement that any F-independent subset of L is also K-independent. It is clear that 2) implies 5).

[5⇒2] Let $\{\alpha_i\}$ be a basis for K over F that is L-independent. Let $\{\beta_j\}$ be an F-independent subset of L. We show that $\{\beta_j\}$ is also K-independent. Let $\sum_i \kappa_i\beta_i = 0$ where $\kappa_i \in K$. Then $\kappa_i = \sum_j a_{ij}\alpha_j$, where $a_{ij} \in F$, and so

$$\sum_i \sum_j a_{ij}\beta_j\alpha_i = 0$$

But the α_i's are L-independent and so

$$\sum_j a_{ij}\beta_j = 0$$

for all i. Hence $a_{ij} = 0$ for all i, j. It follows that $\kappa_i = 0$ for all i, whence $\{\beta_j\}$ is K-independent.

[1⇔6] In the finite (hence algebraic) case, we have remarked that the map $\psi: K \otimes L \to KL$ is surjective and so it is also injective if and only if $dim\ K \otimes L = dim\ KL$, which by Corollary 0.8.5 is equivalent to

$$(dim\ K)(dim\ L) = dim\ KL$$

all dimensions being over F.

[6⇔7] This follows from Corollary 5.5.2. ∎

Definition If any of the equivalent conditions hold in Theorem 5.6.1, we say that K and L are **linearly disjoint** over F. □

*5.7 The Krull Topology

We have seen that if $F < E$ is a finite Galois extension, then all subgroups of the Galois group $G_F(E)$ are closed but if $F < E$ is infinite and Galois, this need not be true (see Example 5.3.1). The use of the term *closed* suggests the presence of a topology, which we now define.

Definition Let E^E be the set of all functions from E into E. We define a topology $\mathcal{T}$ on E^E, called the **finite topology**, by specifying as subbasis all sets of the form

$$S_{u,v} = \{f:E\to E \mid fu = v\}$$

where $u, v \in E$. A basis for $\mathcal{T}$ thus consists of all sets of the form

$$\{f:E\to E \mid fu_1 = v_1,\ldots,fu_k = v_k\}$$

where $u_i, v_i \in E$. □

Of course, if $F < E$, then the Galois group $G_F(E)$ is a subset of E^E.

Theorem 5.7.1 If $F < E$ is algebraic then $G_F(E)$ is closed in the finite topology.

Proof. We show that any $f \in E^E$ that lies in the closure $cl(G_F(E))$ of the Galois group is actually in $G_F(E)$. A basic open neighborhood of f has the form

$$\{g \in E^E \mid gu_1 = fu_1,\ldots,gu_k = fu_k\}$$

and so $f \in cl(G_F(E))$ implies that for any $u_1,\ldots,u_k \in E$ there is a $\sigma \in G_F(E)$ for which $\sigma u_i = fu_i$ for $i = 1,\ldots,k$. It follows that f is a homomorphism. For if $u, v \in E$ and $\alpha, \beta \in F$ then there is a $\sigma \in G_F(E)$ for which

$$\sigma u = fu, \quad \sigma v = fv,$$

$$\sigma(\alpha u + \beta v) = f(\alpha u + \beta v), \quad \sigma(uv) = f(uv)$$

Hence,

$$f(\alpha u + \beta v) = \sigma(\alpha u + \beta v) = \alpha\sigma u + \beta\sigma v = \alpha fu + \beta fv$$

and

$$f(uv) = \sigma(uv) = (\sigma u)(\sigma v) = (fu)(fv)$$

which shows that f is a homomorphism. Also, $fu = 0$ implies $\sigma u = 0$ for some $\sigma \in G_F(E)$ and so $u = 0$, showing that f is injective. Similarly, f

fixes F pointwise. Thus, f is an embedding of E into itself over F. Since $F < E$ is algebraic, we deduce that $f \in G_F(E)$. ∎

Thus, if $F < E$ is a Galois extension, the Galois group $G_F(E)$ is closed in the finite topology on E^E. The subspace topology inherited by $G_F(E)$ is called the **Krull topology** on $G_F(E)$. It follows that a subset of $G_F(E)$ is closed in the Krull topology if and only if it is closed in the finite topology on E^E.

To avoid any temporary confusion, we refer to a subset of $G_F(E)$ that is closed in the Krull topology as **k-closed** and a subgroup of $G_F(E)$ that is closed in the sense of the Galois correspondence as **g-closed.** Similarly, we use the term **k-open** for open sets in the Krull topology.

Let us determine the closure $\overline{H}$ in the Krull topology of a subgroup H of $G_F(E)$. If $\tau \in \overline{H}$ then given $u_1,\ldots,u_n \in E$, there is a $\sigma \in H$ for which $\tau u_i = \sigma u_i$, for $i = 1,\ldots,n$. This implies that τ fixes any element of the fixed field $F(H)$. Hence, $\tau \in \overline{H}$ if and only if, given $u_1,\ldots,u_n \in E$, there is a $\sigma \in H$ for which

$$\tau \mid_{F(H)(u_1,\ldots,u_n)} = \sigma \mid_{F(H)(u_1,\ldots,u_n)}$$

Since any finite extension of $F(H)$ contained in E has the form $F(H)(u_1,\ldots,u_n)$, we can say that $\tau \in \overline{H}$ if and only if for any finite extension K of $F(H)$ contained in E, there exists a $\sigma \in H$ for which $\tau \mid_K = \sigma \mid_K$.

If $F(H) < K$ is a finite extension and K^{nc} is the normal closure then $F(H) < K^{nc}$ is a finite Galois extension. Thus $\tau \in \overline{H}$ if and only if for any finite Galois extension K of $F(H)$ contained in E, there exists a $\sigma \in H$ for which $\tau \mid_K = \sigma \mid_K$. Finally, letting

$$H \mid_K = \{\sigma \mid_K : \sigma \in H\}$$

we can say that $\tau \in \overline{H}$ if and only if for any finite Galois extension K of $F(H)$ contained in E, we have $\tau \mid_K \in H \mid_K$.

If $\tau \in \overline{H}$ and $K = F(H)$, we have

$$\tau \mid_{F(H)} \in H \mid_{F(H)} = \{\iota\}$$

and so $\tau \in G_{F(H)}(E)$, the g-closure of H, whence

$$\overline{H} \subseteq G_{F(H)}(E)$$

To see that the reverse inclusion holds, suppose that $\tau \in G_{F(H)}(E)$ and let $F(H) < K$ be a finite Galois extension contained in E. Since $F(H)$ is

contained in K, we have

$$\begin{aligned} F(\mathrm{H}) &= \{\alpha \in \mathrm{E} \mid \sigma\alpha = \alpha \text{ for all } \sigma \in \mathrm{H}\} \\ &= \{\alpha \in \mathrm{K} \mid \sigma\alpha = \alpha \text{ for all } \sigma \in \mathrm{H}\} \\ &= \{\alpha \in \mathrm{K} \mid \sigma\alpha = \alpha \text{ for all } \sigma \in \mathrm{H} \mid_{\mathrm{K}}\} \\ &= F(\mathrm{H} \mid_{\mathrm{K}}) \end{aligned}$$

where $F(\mathrm{H} \mid_{\mathrm{K}})$ is the fixed field of $\mathrm{H} \mid_{\mathrm{K}}$ with respect to the Galois correspondence on the Galois extension $F(\mathrm{H}) < \mathrm{K}$. (Note that since $F(\mathrm{H}) < \mathrm{K}$ is a Galois extension, if $\sigma \in \mathrm{H}$ then σ is an automorphism of E over $F(\mathrm{H})$, whence its restriction $\sigma \mid_{\mathrm{K}}$ is an automorphism of K over $F(\mathrm{H})$. Hence, $\mathrm{H} \mid_{\mathrm{K}}$ is contained in the Galois group $G_{F(\mathrm{H})}(\mathrm{K})$.)

Since $F(\mathrm{H}) = F(\mathrm{H} \mid_{\mathrm{K}})$, the extension $F(\mathrm{H} \mid_{\mathrm{K}}) < \mathrm{K}$ is finite and Galois, implying that $\mathrm{H} \mid_{\mathrm{K}}$ is g-closed in the Galois correspondence of $F(\mathrm{H} \mid_{\mathrm{K}}) < \mathrm{K}$. Hence,

$$\tau \mid_{\mathrm{K}} \in G_{F(\mathrm{H})}(\mathrm{K}) = \mathrm{G}_{F(\mathrm{H} \mid_{\mathrm{K}})}(\mathrm{K}) = \mathrm{H} \mid_{\mathrm{K}}$$

and so $\tau \in \overline{\mathrm{H}}$. It follows that $G_{F(\mathrm{H})}(\mathrm{E}) \subseteq \overline{\mathrm{H}}$. Let us summarize.

Theorem 5.7.2 Let $\mathrm{F} < \mathrm{E}$ be a Galois extension and let H be a subgroup of the Galois group $G_{\mathrm{F}}(\mathrm{E})$. Then the closure $G_{F(\mathrm{H})}(\mathrm{E})$ of H with respect to the Galois correspondence on $\mathrm{F} < \mathrm{E}$ is the closure of H in the Krull topology. □

Let $\mathrm{F} < \mathrm{E}$ be a Galois extension. We leave it to the reader to show that the composition map

$$G_{\mathrm{F}}(\mathrm{E}) \times G_{\mathrm{F}}(\mathrm{E}) \mapsto G_{\mathrm{F}}(\mathrm{E}) : (\sigma, \tau) \mapsto \sigma\tau$$

and the inversion map

$$G_{\mathrm{F}}(\mathrm{E}) \mapsto G_{\mathrm{F}}(\mathrm{E}) : \sigma \mapsto \sigma^{-1}$$

are continuous under the Krull topology. Hence, $G_{\mathrm{F}}(\mathrm{E})$ is a topological group. In fact, it can be shown that $G_{\mathrm{F}}(\mathrm{E})$ is a compact, totally disconnected topological group.

We conclude this section by completing the proof of Theorem 5.5.1 in the infinite case. Recall that $\mathrm{F} < \mathrm{E}$ is Galois and $\mathrm{F} < \mathrm{K}$. The map $\psi : G_{\mathrm{K}}(\mathrm{EK}) \to G_{\mathrm{F}}(\mathrm{E})$ is defined by $\psi\sigma = \sigma \mid_{\mathrm{E}}$ and we wish to show that $Im\ \psi$ is closed with respect to the Galois correspondence on $\mathrm{F} < \mathrm{E}$. Theorem 5.7.2 implies that this is equivalent to showing that $\mathrm{I} = Im\ \psi$

is closed in the Krull topology on $G_F(E)$.

Let $\tau \in \bar{I}$, the Krull-closure of I. We show that $\tau \in I$ by finding a $\sigma \in G_K(EK)$ for which $\sigma \mid_E = \tau$. Let us define σ:EK→EK as follows. Since $K < EK$ is algebraic, any element $\alpha \in EK$ is a finite sum of the form

$$\alpha = \sum e_i k_i$$

where $e_i \in E$ and $k_i \in K$. We set

$$\sigma\alpha = \sum (\tau e_i) k_i$$

The first order of business is to show that this is well-defined.

To this end, note that since $\tau \in \bar{I}$, it follows that for any finite set $U = \{u_1, \ldots, u_n\} \subseteq E$, there exists a $\sigma_U \in G_K(EK)$ that agrees with τ on the elements of U, that is, for which

$$\alpha_U u_i = \tau u_i, \quad \text{for all i}$$

Hence, if $U = \{e_1, \ldots, e_n\}$ then

$$\sigma\alpha = \sum (\tau e_i) k_i = \sum (\sigma_U e_i) k_i$$

Now suppose that α can also be written as

$$\alpha = \sum e_i' k_i'$$

Let $V = \{e_i'\} \subseteq E$ and let $\sigma_{U \cup V}$ agree with τ on $U \cup V$. Then

$$\begin{aligned} \sum (\tau e_i) k_i &= \sum (\sigma_{U \cup V} e_i) k_i = \sigma_{U \cup V}\Big(\sum e_i k_i\Big) \\ &= \sigma_{U \cup V}\Big(\sum e_i' k_i'\Big) = \sum (\sigma_{U \cup V} e_i') k_i' = \sum (\tau e_i') k_i' \end{aligned}$$

Thus, the definition of $\sigma\alpha$ does not depend on the representation of α, and σ is well-defined.

Now suppose that

$$\alpha_1 = \sum e_{1i} k_i, \; \alpha_2 = \sum e_{2i} k_i, \ldots, \; \alpha_n = \sum e_{ni} k_i$$

is any finite set of elements of EK and let $U = \{e_{ij}\}$. If $\sigma' \in G_K(EK)$ agrees with τ on the elements of U, then

$$\sigma'\alpha_j = \sigma' \sum_i e_{ji} k_i = \sum_i \tau(e_{ji}) k_i = \sigma \sum_i e_{ji} k_i = \sigma\alpha_j$$

for all $j = 1,\ldots,n$. In other words, for any finite subset S of EK, there is an element of $G_K(EK)$ that agrees with σ on S.

It follows that σ is a homomorphism of EK, for if α, $\beta \in EK$ then there exists a $\sigma' \in G_K(EK)$ that agrees with σ on α, β, $\alpha+\beta$ and $\alpha\beta$ and since σ' is a homomorphism, we have

$$\sigma(\alpha+\beta) = \sigma'(\alpha+\beta) = \sigma'\alpha + \sigma'\beta = \sigma\alpha + \sigma\beta$$

and

$$\sigma(\alpha\beta) = \sigma'(\alpha\beta) = (\sigma'\alpha)(\sigma'\beta) = (\sigma\alpha)(\sigma\beta)$$

It also follows that σ is injective, for if $\sigma\alpha = 0$ then there is a $\sigma' \in G_K(EK)$ such that $\sigma'\alpha = 0$, whence $\alpha = 0$. The surjectivity of σ follows from that of τ, since if $\alpha \in EK$, then

$$\alpha = \sum e_i k_i = \sum (\tau e_i')k_i = \sigma\Big(\sum e_i' k_i\Big)$$

Finally, it is clear from the definition that $\sigma\alpha = \alpha$ for all $\alpha \in K$ and that $\sigma\alpha = \tau\alpha$ for all $\alpha \in E$. Thus, $\sigma \in G_K(EK)$ and $\sigma\,|_E = \tau$. This completes the proof of Theorem 5.5.1.

Exercises

1. If $\lambda:\mathcal{L}\to\mathcal{M}$ is an order reversing bijection between two lattices, verify that $\lambda(a \wedge b) = \lambda a \vee \lambda b$ and $\lambda(a \vee b) = \lambda a \wedge \lambda b$.
2. With respect to a Galois connection, if P is a complete lattice then $Cl(P)$ is also a complete lattice.
3. If $K < E$ and $L < E$ are Galois extensions, show that $K \cap L < E$ is a Galois extension.
4. Let K and L be subfields of a field E and suppose that $K < E$ and $L < E$ are Galois, with Galois groups G_1 and G_2, respectively. Let G_1G_2 be the join of G_1 and G_2 in the lattice $\mathfrak{G}$ of all subgroups of $G_{K\cap L}(E)$ and let $G_1 \vee G_2$ be the join of G_1 and G_2 in the lattice $\overline{\mathfrak{G}}$ of all closed subgroups of $G_{K\cap L}(E)$. Show that G_1G_2 is finite if and only if $G_{K\cap L}(E)$ is finite, in which case $G_1G_2 = G_1 \vee G_2$.
5. Let $F < E$ be finite with $G = G_F(E)$. Let $G_1 \lhd G_2 < G$, with $F_i = F(G_i)$. Show that $G_{F_2}(F_1) \simeq G_2/G_1$.
6. Find an example of an infinite algebraic extension whose Galois group is finite.
7. Prove Corollary 5.5.2.
8. Let F be a perfect field. Suppose that there is a prime p for which $p \mid [E:F]$ for every proper finite extension E of F. Show that if E is a finite extension of F then $[E:F] = p^n$ for some $n \in \mathbb{N}$. Apply this to the case $F = \mathbb{R}$ to deduce that if $\mathbb{R} < E$ is a finite extension the $[E:\mathbb{R}] = 2^n$ for some $n \in \mathbb{N}$.

9. Let $F < E$ be a finite Galois extension and let $E < K$. Then [EK:K] divides [E:F]. Use the following to show that the assumption that $F < E$ be Galois is essential. Let α be the real cube root of 2, let $\omega \neq 1$ be a cube root of 1. Let $F = \mathbb{Q}$, $E = \mathbb{Q}(\alpha\omega)$ and $K = \mathbb{Q}(\alpha)$.
10. Prove the following statements about abelian and cyclic extensions.
    a) If $F < E$ and $F < K$ are abelian, then $F < EK$ is abelian.
    b) If $F < E$ is abelian (cyclic) and $F < K$, then $K < EK$ is abelian (cyclic).
    c) If $F < K < E$ with $F < E$ abelian (cyclic), then $K < E$ and $F < K$ are abelian (cyclic).
11. Let $F < E$ and $F < K$ be extensions, with E and K contained in a larger field. Show that E and K are linearly disjoint over F if and only if E′ and K′ are linearly disjoint over F for all intermediate fields $F < E' < E$ and $F < K' < K$ with [E′:F] and [K′:F] finite.
12. Let $F < E$ be a normal extension. Show that the separable closure F^{sc} of F in E and the purely inseparable closure F^{ic} of F in E are linearly disjoint over F. Moreover, if $F < K < E$ and if K and F^{ic} are linearly disjoint over F then $F < E$ is separable.
13. Let $f(x) \in F[x]$ and let $F < E$. Let S_E be the splitting field of f(x) over E. Thus, if $\alpha_1, \ldots, \alpha_n$ are the roots of f(x) in S_E, we have $S_E = E(\alpha_1, \ldots, \alpha_n)$. Let $S_F = F(\alpha_1, \ldots, \alpha_n)$ and let $L = S_F \cap F(G_E(S_E))$. Let $\psi: G_E(S_E) \to G_L(S_F)$ be defined by $\psi\sigma = \sigma \mid_{S_F}$. Show that ψ is an isomorphism. This is known as the *Theorem on Natural Irrationalities.*
14. Referring to Theorem 5.5.3, show that if $\mathfrak{F}$ is an arbitrary family then the map ψ is an isomorphism if

$$E_j \cap \Big(\bigvee_{i \neq j} E_i \Big) = F \quad \text{for all } j \in I$$

15. Extend the notion of closure obtained from the Galois extension to all subsets of $G_F(E)$, and show that it is a closure operation in the sense of topology.
16. Prove that $G_F(E)$ is a topological group under the Krull topology. Show that this topological group is totally disconnected.
17. Let $F < E$ and suppose that S is a finite set of elements algebraically independent over E. Then F(S) and E are linearly disjoint over F.
18. a) Show that in every Galois extension $F < E$, there is a largest abelian subextension F^{ab}, that is, $F < F^{ab} < E$, $F < F^{ab}$ is abelian and if $F < K < E$ with $F < K$ abelian then $K < F^{ab}$.
    b) If G is a group, the subgroup G′ generated by all **commutators** $\alpha\beta\alpha^{-1}\beta^{-1}$, for $\alpha, \beta \in G$, is called the **commutator subgroup.** Show that G′ is the smallest subgroup

of G for which G/G' is abelian.

c) If the commutator subgroup $G_F(E)'$ of a Galois group $G_F(E)$ is closed, that is, if $G_F(E)' = G_K(E)$ for some $F < K < E$, then $K = F^{ab}$.

19. Let $F < K$ and let $F < E < L$. Assume that K and L are contained in a larger field. Then K and L are linearly disjoint over F if and only if K and E are linearly disjoint over F and KE and L are linearly disjoint over E.

20. The following concept is analogous to, but weaker than, that of linear disjointness. Let $F < K$ and $F < L$ be extensions, with K and L contained in a larger field. We say that K is **free from L over F** if whenever $S \subseteq K$ is a finite set of algebraically independent elements over F, then S is also algebraically independent over L.

a) The definition given above is not symmetric, but the concept is. Show that if K is free from L over F, then $[KL:L]_t = [K:F]_t$. Let T be a finite F-algebraically independent set of elements of L. Show that T is algebraically independent over K.

b) Let $F < K$ and $F < E$ be field extensions, contained in a larger field. Prove that if K and L are linearly disjoint over F, then they are also free over F.

c) Find an example showing that the converse of part b) does not hold.

Chapter 6
Galois Theory II

In this chapter, we pass from the highly theoretical material of the previous chapter to the somewhat more concrete, where we consider the Galois groups of the splitting fields of specific types of polynomials.

6.1 The Galois Group of a Polynomial

The **Galois group of a polynomial** $p(x) \in F[x]$ is defined to be the Galois group of a splitting field S for $p(x)$ over F. This group is sometimes denoted by $G_F(p(x))$. If

$$p(x) = p_1^{e_1}(x) \cdots p_k^{e_k}(x)$$

is a factorization of $p(x)$ into powers of distinct irreducible polynomials over F, then S is also a splitting field for the polynomial $q(x) = p_1(x) \cdots p_k(x)$. Moreover, the extension $F < S$ is separable (and hence Galois) if and only if each $p_i(x)$ is a separable polynomial. In particular, if $p(x)$ has no multiple roots, then $F < S$ is a Galois extension.

Note that each $\sigma \in G_F(S)$ is uniquely determined by its action on the roots of $p(x)$, which generate S, and that this action is a permutation of the roots. However, not all permutations of the roots of $p(x)$ need correspond to an element of $G_F(S)$. Thus, we have an injective group homomorphism from $G_F(S)$ into the symmetric group S_n, where $n = deg\ p(x)$.

Let $p(x) = f(x)g(x)$ where $deg\ f(x) > 0$ and let S_p be the splitting field for $p(x)$ over F and S_f the splitting field for $f(x)$ over F. We clearly have $F < S_f < S_p$ with each step normal. Hence, by Theorem 5.4.1,

$G_{S_f}(S_p) \triangleleft G_F(S_p)$ and

$$G_F(S_f) \simeq \frac{G_F(S_p)}{G_{S_f}(S_p)}$$

or, in another notation,

$$G_F(f(x)) \simeq \frac{G_F(p(x))}{G_{S_f}(p(x))}$$

Thus, the Galois group of a nontrivial factor of p(x) is isomorphic to a quotient group of the Galois group of p(x).

6.2 Symmetric Polynomials

If F is a field and $t_1,\ldots,t_n$ are algebraically independent over F, the polynomial

$$g(x) = \prod_{i=1}^{n} (x - t_i)$$

is referred to as a **generic polynomial** over F of degree n. Since the roots $t_1,\ldots,t_n$ of the generic polynomial g(x) are algebraically independent, this polynomial is, in some sense, the most general polynomial possible. Accordingly, it should (and does) have the most general Galois group, as we will see.

The generic polynomial can be written in the form

$$g(x) = x^n - s_1 x^{n-1} + \cdots + (-1)^n s_n$$

where the coefficients $s_k \in F(t_1,\ldots,t_n)$ are given by

$$s_1 = t_1 + \cdots + t_n,\ s_2 = \sum_{i<j} t_i t_j\ ,\ldots,\ s_n = \prod_{i=1}^{n} t_i$$

and are called the **elementary symmetric polynomials** in the variables t_i. It follows that the coefficients of any polynomial are the elementary symmetric functions of the roots (in a splitting field) of that polynomial.

Since $F(t_1,\ldots,t_n)$ is the splitting field for g(x) over $F(s_1,\ldots,s_n)$, and since g(x) has no multiple roots, we deduce from the remarks of the previous section that the extension $F(s_1,\ldots,s_n) < F(t_1,\ldots,t_n)$ is Galois of degree at most n!. Moreover, any permutation $\sigma \in S_n$ of $\{1,\ldots,n\}$ induces a unique automorphism of $F(t_1,\ldots,t_n)$ defined by

$$\sigma \frac{p(t_1,\ldots,t_n)}{q(t_1,\ldots,t_n)} = \frac{p(t_{\sigma(1)},\ldots,t_{\sigma(n)})}{q(t_{\sigma(1)},\ldots,t_{\sigma(n)})}$$

Let us denote the group of all such automorphisms by G.

According to Theorem 5.3.5, since G is a finite group of automorphisms of $F(t_1,\ldots,t_n)$, the extension $F(G) < F(t_1,\ldots,t_n)$ is finite and Galois, with Galois group G and so

$$[F(t_1,\ldots,t_n):F(G)] = |G| = |S_n| = n!$$

Since every elementary symmetric function is fixed by the elements of G (hence the name *symmetric* function), we have

$$F(s_1,\ldots,s_n) < F(G) < F(t_1,\ldots,t_n)$$

and since

$$[F(t_1,\ldots,t_n):F(s_1,\ldots,s_n)] \leq n!$$

we have equality above and $F(G) = F(s_1,\ldots,s_n)$.

Theorem 6.2.1 Let $t_1,\ldots,t_n$ be algebraically independent over F and let $s_1,\ldots,s_n$ be the elementary symmetric functions in $t_1,\ldots,t_n$.

1) $F(s_1,\ldots,s_n) < F(t_1,\ldots,t_n)$ is a Galois extension of degree n!, whose Galois group is isomorphic to the symmetric group S_n.
2) The generic polynomial g(x) is irreducible over $F[s_1,\ldots,s_n]$.

Proof. To prove part 2), observe that if $g(x) = a(x)b(x)$ where *deg* $a(x) = d > 0$ and *deg* $b(x) = e > 0$, then the Galois group of g(x) would have size at most $d!e! < (d+e)! = n!$. Hence g(x) is irreducible. ∎

Definition A polynomial $p(t_1,\ldots,t_n) \in F[t_1,\ldots,t_n]$ is **symmetric** if

$$p(t_{\sigma(1)},\ldots,t_{\sigma(n)}) = p(t_1,\ldots,t_n)$$

for all permutations $\sigma \in S_n$. Equivalently, p is symmetric if

$$\sigma[p(t_1,\ldots,t_n)] = p(t_1,\ldots,t_n)$$

for all $\sigma \in G$. □

Thus, a polynomial $p(t_1,\ldots,t_n) \in F(t_1,\ldots,t_n)$ is symmetric if and only if it lies in the fixed field $F(s_1,\ldots,s_n)$, that is, if and only if it is a rational function in $s_1,\ldots,s_n$. However, we can improve considerably upon this statement.

Theorem 6.2.2 Let $t_1,\ldots,t_n$ be algebraically independent over F and let $s_1,\ldots,s_n$ be the elementary symmetric functions in $t_1,\ldots,t_n$. A polynomial $p(t_1,\ldots,t_n) \in F[t_1,\ldots,t_n]$ is symmetric if and only if there exists a *polynomial* $q(x_1,\ldots,x_n)$ over F for which $p(t_1,\ldots,t_n) = q(s_1,\ldots,s_n)$. Moreover, if $p(t_1,\ldots,t_n)$ has integer coefficients, then $q(x_1,\ldots,x_n)$ can be chosen with integer coefficients.

Proof. If $p(t_1,\ldots,t_n)$ has the form $q(s_1,\ldots,s_n)$, then it is clearly symmetric. For the converse, the proof consists of a procedure that can be used to construct the polynomial $q(x_1,\ldots,x_n)$. Unfortunately, while the procedure is quite straightforward, it is recursive in nature and not at all practical.

We use induction on n. The theorem is true for $n = 1$, since $s_1 = t_1$. Assume the theorem is true for any number of variables less than n and let $p(t_1,\ldots,t_n)$ be symmetric. By collecting powers of t_n, we can write

$$p(t_1,\ldots,t_n) = p_0 + p_1 t_n + p_2 t_n^2 + \cdots + p_n t_n^n$$

where each p_i is a polynomial in $t_1,\ldots,t_{n-1}$. Since p is symmetric in $t_1,\ldots,t_{n-1}$ and $t_1,\ldots,t_n$ are independent, each of the coefficients p_i is symmetric in $t_1,\ldots,t_{n-1}$. By the inductive hypothesis, we may express each p_i as a polynomial in the elementary symmetric functions on $t_1,\ldots,t_{n-1}$. If these functions are denoted by $u_1,\ldots,u_{n-1}$, then we have

$$p(t_1,\ldots,t_n) = q_0 + q_1 t_n + q_2 t_n^2 + \cdots + q_n t_n^n \tag{6.2.1}$$

where each q_i is a polynomial in $u_1,\ldots,u_{n-1}$, with integer coefficients if p has integer coefficients.

Note that the symmetric functions s_i can be expressed in terms of the symmetric functions u_i as follows

$$\begin{aligned} s_1 &= u_1 + t_n \\ s_2 &= u_2 + u_1 t_n \\ &\vdots \\ s_{n-1} &= u_{n-1} + u_{n-2} t_n \\ s_n &= u_{n-1} t_n \end{aligned} \tag{6.2.2}$$

These expressions can be solved for the u_i's in terms of the s_i's, giving

$$\begin{aligned} u_1 &= s_1 - t_n \\ u_2 &= s_2 - u_1 t_n = s_2 - s_1 t_n + t_n^2 \end{aligned}$$

$$u_3 = s_3 - u_2 t_n = s_3 - s_2 t_n + s_1 t_n^2 - t_n^3$$
$$\vdots$$
$$u_{n-1} = s_{n-1} - u_{n-2} t_n = s_{n-1} - s_{n-2} t_n + \cdots + (-1)^{n-1} t_n^{n-1}$$

and from the last equation in (6.2.2),

$$0 = s_n - u_{n-1} t_n = s_n - s_{n-1} t_n + \cdots + (-1)^n t_n^n \tag{6.2.3}$$

Substituting these expressions for the u_i's into (6.2.1) gives

$$p(t_1, \ldots, t_n) = r_0 + r_1 t_n + r_2 t_n^2 + \cdots + r_n t_n^n$$

where each r_i is a polynomial in $s_1, \ldots, s_{n-1}$ and t_n, with integer coefficients if p has integer coefficients. Again, we may gather together powers of t_n, to get

$$p(t_1, \ldots, t_n) = g_0 + g_1 t_n + g_2 t_n^2 + \cdots + g_m t_n^m$$

where each g_i is a polynomial in $s_1, \ldots, s_{n-1}$, with integer coefficients if p has integer coefficients. If $m \geq n$, we may reduce the degree in t_n by using (6.2.3), which also introduces the term s_n. Hence,

$$p(t_1, \ldots, t_n) = h_0 + h_1 t_n + h_2 t_n^2 + \cdots + h_{n-1} t_n^{n-1} \tag{6.2.4}$$

where each h_i is a polynomial in $s_1, \ldots, s_n$, with integer coefficients if p has integer coefficients.

Since the left side of (6.2.4) is symmetric in the t_i's, we may replace t_n by t_i, for each $i = 1, \ldots, n-1$, to get

$$p(t_1, \ldots, t_n) = h_0 + h_1 t_i + h_2 t_i^2 + \cdots + h_{n-1} t_i^{n-1}$$

valid for all $i = 1, \ldots, n$. Hence, the polynomial

$$P(x) = h_0 + h_1 x + h_2 x^2 + \cdots + h_{n-1} x^{n-1} - p(t_1, \ldots, t_n)$$

has degree (in x) at most $n-1$ but has n distinct roots $t_1, \ldots, t_n$, whence it must be the zero polynomial. Thus, $h_i = 0$ for $i \geq 1$ and $p(t_1, \ldots, t_n) = h_0 = h_0(s_1, \ldots, s_n)$, as desired. ∎

Example 6.2.1 Let $p(x) = x^n - s_1 x^{n-1} + \cdots + (-1)^n s_n$ be a polynomial with roots $r_1, \ldots, r_n$ in a splitting field. For $k \geq 1$, the polynomials

$$u_k = r_1^k + r_2^k + \cdots + r_n^k$$

are symmetric in the roots of $p(x)$, and so Theorem 6.2.2 implies that they can be expressed as polynomials in the elementary symmetric functions $s_1,\ldots,s_n$ of the roots. One way to derive an expression relating the u_k's to the s_k's is by following the proof of Theorem 6.2.2. In the exercises, we ask the reader to take another approach to obtain the so-called *Newton identities*

$$u_k - u_{k-1}s_1 + u_{k-2}s_2 + \cdots + (-1)^{k-1}u_1s_{k-1} + (-1)^k k s_k = 0$$

for $k \geq 1$. These identities can be used to compute recursively the u_k's in terms of the s_i's. □

Since any symmetric polynomial in the roots of a given polynomial $p(x)$ is a polynomial in the coefficients of $p(x)$ as well, it therefore lies in the base field.

Corollary 6.2.3 Let $p(x) \in F[x]$ have roots $r_1,\ldots,r_n$ in a splitting field. If $f(t_1,\ldots,t_n)$ is a symmetric polynomial, then $f(r_1,\ldots,r_n)$ is a polynomial in the coefficients of $p(x)$, and thus lies in F.

Proof. We know that $f(r_1,\ldots,r_n) = g(s_1,\ldots,s_n)$ where s_i is the i-th elementary symmetric polynomial in the roots $r_1,\ldots,r_n$. But s_i or $-s_i$ is the coefficient of x^{n-i} in $p(x)$, whence f is a polynomial in these coefficients. ∎

Theorem 6.2.4 The elementary symmetric polynomials $s_1,\ldots,s_n$ are algebraically independent over F.

Proof. Since $F(s_1,\ldots,s_n) < F(t_1,\ldots,t_n)$ is algebraic, Theorem 3.3.1 implies that $S = \{s_1,\ldots,s_n\}$ contains a transcendence basis for $F(t_1,\ldots,t_n)$ over F. But $\{t_1,\ldots,t_n\}$ is a transcendence basis and so $[F(t_1,\ldots,t_n):F]_t = n$. Hence, S is a transcendence basis. ∎

6.3 The Discriminant of a Polynomial

We have seen that the Galois group $G_F(p(x))$ of a polynomial of degree n is isomorphic to a subgroup of the symmetric group S_n and that the Galois group of a generic polynomial is isomorphic to S_n itself. A special symmetric function of the roots of $p(x)$, known as the discriminant, provides a useful tool for determining whether or not the Galois group is isomorphic to a subgroup of the alternating group.

Let $p(x)$ be a polynomial over F, with roots $r_1,\ldots,r_n$ in a splitting field E. Let

$$\delta = \prod_{i<j} (r_i - r_j)$$

The **discriminant** of $p(x)$ is $\Delta = \delta^2$. Note that $\Delta \neq 0$ if and only if $p(x)$ has no multiple roots.

Let us assume that $\Delta \neq 0$. Hence $p(x)$ is the product of distinct separable polynomials, implying that $F < E$ is a Galois extension. Each $\sigma \in G_F(p(x))$ acts as a permutation of the roots r_i and so

$$\sigma\delta = (-1)^\sigma \delta$$

where $(-1)^\sigma$ is 1 if σ is an even permutation and -1 if σ is an odd permutation. Hence, $\sigma\Delta = \Delta$, implying that $\Delta \in F$. If $\text{char}(F) = 2$, then $\sigma\delta = \delta$ for all $\sigma \in G_F(p(x))$ and so $\delta \in F$.

If $\text{char}(F) \neq 2$, we have two possibilities. If $\delta \in F$ then all $\sigma \in G_F(p(x))$ fix δ and are therefore even. Hence $G_F(p(x))$ is isomorphic to a subgroup of the alternating group A_n. If $\delta \notin F$ then $G_F(p(x))$ must contain an odd permutation. It is not hard to show that if a subgroup of S_n contains an odd permutation then the subgroup has even order and exactly half of its elements are even. Hence, if $\delta \notin F$ then $G_F(p(x))$ has even order and

$$| G_F(p(x)) \cap A_n | = \tfrac{1}{2} | G_F(p(x)) |$$

If we let $H = G_F(p(x)) \cap A_n$ then $F(H) < E$ is Galois, with Galois group H and so

$$[E:F(H)] = | H | = \tfrac{1}{2} | G_F(p(x)) | = \tfrac{1}{2}[E:F]$$

which implies that $[F(H):F] = 2$. But $[F(\delta):F] = 2$ and $F(\delta) \subseteq F(H)$, whence $F(H) = F(\delta)$. In words, the fixed field of the even permutations in $G_F(p(x))$ is $F(\delta)$. Let us summarize.

Theorem 6.3.1 Let $p(x) \in F[x]$ have splitting field E.

1) $\Delta = 0$ if and only if $p(x)$ has multiple roots in E.
2) Assume that $\Delta \neq 0$ and $\text{char}(F) \neq 2$.
   a) If Δ has a square root in F, then the Galois group $G_F(p(x))$ is isomorphic to a subgroup of the alternating group A_n.
   b) If Δ does not have a square root in F, then the Galois group $G_F(p(x))$ contains half odd and half even permutations of the roots of $p(x)$. In addition, the fixed field of $G_F(p(x)) \cap A_n$ is $F(\sqrt{\Delta})$.
3) Assume that $\Delta \neq 0$ and $\text{char}(F) = 2$. Then Δ has a square root in F, but $G_F(p(x)$ need not be isomorphic to a subgroup of A_n.

Proof. For part 3), observe that the generic polynomial

$$g(x) = (x - t_1)\cdots(x - t_n)$$

has Galois group S_n over $F(s_1,\ldots,s_n)$. ∎

The usefulness of Theorem 6.3.1 comes from the fact that Δ can actually be computed in some cases. To see why this is so, observe that δ is the Vandermonde determinant

$$\delta = \begin{vmatrix} 1 & 1 & 1 & 1 \\ r_1 & r_2 & \cdots & r_n \\ \vdots & \vdots & \cdots & \vdots \\ r_1^{n-1} & r_2^{n-1} & \cdots & r_n^{n-1} \end{vmatrix}$$

Taking the transpose and multiplying gives

$$\Delta = \begin{vmatrix} u_0 & u_1 & \cdots & u_{n-1} \\ u_1 & u_2 & \cdots & u_n \\ \vdots & \vdots & \cdots & \vdots \\ u_{n-1} & u_n & \cdots & u_{2n-2} \end{vmatrix}$$

where $u_i = r_1^i + r_2^i + \cdots + r_n^i$. Newton's identities can then be used to determine the u_i's in terms of the coefficients of the polynomial in question (see Example 6.2.1 and the exercises). We will see some examples of this in the next section.

6.4 The Galois Groups of Some Small Degree Polynomials

Quadratic Polynomials

Quadratic extensions (extensions of degree 2) hold no surprises except perhaps for certain base fields of characteristic 2. Let

$$p(x) = x^2 + bx + c = (x - r)(x - s)$$

be a quadratic over F, with splitting field E. To compute the

discriminant, observe that $u_1 = r + s = b$ and

$$u_2 = r^2 + s^2 = (r+s)^2 - 2rs = b^2 - 2c$$

Hence

$$\Delta = \begin{vmatrix} 2 & b \\ b & b^2-2c \end{vmatrix} = 2(b^2 - 2c) - b^2 = b^2 - 4c$$

a familiar quantity.

If $\Delta = 0$ then $p(x)$ has a double root r and

$$p(x) = (x-r)^2 = x^2 - 2rx + r^2$$

The root r will lie in F for most well-behaved base fields F. In particular, if $\mathrm{char}(F) \neq 2$, then $-2r \in F$ implies $r \in F$. If $\mathrm{char}(F) = 2$ and F is perfect (a finite field, for example) then $r \in F$. However, the following example shows that $p(x)$ may have a multiple root not lying in F. Let $F = \mathbb{Z}_2(t^2)$ where t is transcendental over $\mathbb{Z}_2$ and let

$$p(x) = x^2 - t^2 = (x-t)^2$$

Since $t \notin \mathbb{Z}_2(t^2)$, this polynomial is irreducible over $\mathbb{Z}_2(t^2)$, but has a multiple root $t \notin F$.

If $\Delta \neq 0$ then $p(x)$ has distinct roots and there are two possibilities: (i) the roots lie in F, $p(x)$ is reducible and $G_F(p(x))$ is trivial, or (ii) the roots do not lie in F, $p(x)$ is irreducible and $G_F(p(x)) \simeq \mathbb{Z}_2$ is generated by the map $\sigma: r \to s$. When $\mathrm{char}(F) \neq 2$, we can tell whether or not the roots lie in F by looking at the discriminant, since the quadratic formula gives

$$r, s = \frac{-b \pm \sqrt{b^2 - 4c}}{2} = \frac{-b \pm \sqrt{\Delta}}{2}$$

Hence the roots lie in F if and only if Δ has a square root in F.

Theorem 6.4.1 Let $p(x) \in F[x]$ have degree 2.

1) If $\Delta = 0$ then $p(x) = (x-r)^2$ has a double root r, which may or may not lie in F. In any case, $G_F(p(x))$ is trivial.
2) If $\Delta \neq 0$ then $p(x)$ has distinct roots and there are two possibilities: (i) the roots lie in F, $p(x)$ is reducible and $G_F(p(x))$ is trivial, or (ii) the roots do not lie in F, $p(x)$ is irreducible and $G_F(p(x)) \simeq \mathbb{Z}_2$ is generated by the map $\sigma: r \to s$.
3) If $\mathrm{char}(F) \neq 2$ then all quadratic extensions $F < E$ have the form $E = F(\sqrt{\alpha})$, for some $\alpha \in F$.

Proof. Part 3) follows from the fact that if Δ is the discriminant of $min(\alpha,F)$ then part 2) implies that $\sqrt{\Delta} \notin F$, whence $E = F(\sqrt{\Delta})$. ∎

Let us turn now to a more interesting case.

Cubic Polynomials

Let

$$p(x) = x^3 + bx^2 + cx + d = (x-r)(x-s)(x-t) \in F[x]$$

have splitting field E. Then p(x) is irreducible if and only if none of its roots lie in F. Let us assume that p(x) is irreducible. A straightforward but lengthy computation gives

$$\Delta = -4b^3d + b^2c^2 + 18bcd - 4c^3 - 27d^2$$

Assume first that $\Delta = 0$. Then p(x) has multiple roots and Corollary 1.6.4 implies that $p(x) = q(x^{p^k})$, where $p = expchar(F)$ and $p^k > 1$. Since *deg* p(x) = 3, we must have p = 3, k = 1 and so

$$p(x) = (x-r)^3 = x^3 - r^3$$

has a single root of multiplicity 3. The extension $F < F(r) = E$ is purely inseparable of degree 3 and the Galois group is trivial.

If $\Delta \neq 0$ then p(x) has no multiple roots and is therefore separable. Hence, $F < E$ is Galois and $| G_F(p(x)) | = [E:F]$. Since $r \notin F$, we have $[E:F] > 1$, which leaves the possibilities $[E:F] = 3$ or 6. If p(x) splits in F(r), then $[E:F] = 3$ and the Galois group is isomorphic to $A_3 \simeq \mathbb{Z}_3$. If p(x) does not split in F(r), then $[E:F] = 6$, in which case the Galois group is isomorphic to S_3. When $char(F) \neq 2$, these two cases can be distinguished by examining the discriminant. If $\sqrt{\Delta} \in F$, then $G_F(p(x)) \simeq A_3$ and if $\sqrt{\Delta} \notin F$ then $G_F(p(x)) \simeq S_3$.

Theorem 6.4.2 Let $p(x) \in F[x]$ be irreducible of degree 3.

1) If $\Delta = 0$ then p(x) has a single root of multiplicity 3 and $char(F) = 3$. The Galois group is trivial.
2) If $\Delta \neq 0$ then $G_F(p(x)) \simeq A_3$ or S_3.
2) Let $char(F) \neq 2$. If $0 \neq \sqrt{\Delta} \in F$ then $G_F(p(x)) \simeq A_3$ and adjoining a single root of p(x) to F gives the splitting field for p(x). If $\sqrt{\Delta} \notin F$ then $G_F(p(x)) \simeq S_3$. □

Example 6.4.1 Let $p(x) = x^3 - 2x^2 - x + 1$ over $\mathbb{Q}$. Any rational root of p(x) must be ± 1 (Theorem 1.2.2) and so p(x) is irreducible. The discriminant is $\Delta = 49$ which has a square root in $\mathbb{Q}$ and so

$G_{\mathbb{Q}}(p(x)) \simeq A_3$ is cyclic of order 3. On the other hand, the irreducible polynomial $q(x) = x^3 - x + 1$ has discriminant $\Delta = -23$, which has no square root in $\mathbb{Q}$. Hence, its Galois group is isomorphic to S_3. □

*Quartic Polynomials

Since the Galois group of an irreducible quartic polynomial is isomorphic to a transitive subgroup of S_4, we should begin by determining all such subgroups of S_4. Theorem 0.2.21 implies that if G is a transitive subgroup of S_4 then $|G| = 4$, 8, 12 or 24. Here is a list.

1) The cyclic group $\mathbb{Z}_4$ occurs as a subgroup of S_4, for instance $\langle(1234)\rangle \simeq \mathbb{Z}_4$.
2) The four group $\mathbb{Z}_2 \times \mathbb{Z}_2$ occurs as a subgroup of S_4. In particular

$$V = \{\iota, (12)(34), (13)(24), (14)(23)\}$$

is isomorphic to $\mathbb{Z}_2 \times \mathbb{Z}_2$ and is known as the **viergruppe**. We leave it to the reader to show that V is normal in S_4. This and the previous case exhaust all nonisomorphic groups of order 4.
3) The dihedral group D_4 of symmetries of the square, thought of as permutations of the corners of the square, is a subgroup of S_4 of order 8. Since D_4 is a Sylow 2-subgroup of S_4, all subgroups of S_4 of order 8 are isomorphic to D_4.
4) The alternating group A_4 is the only subgroup of S_4 of index 2, that is, of order 12.
5) Of course, S_4 is the only subgroup of S_4 of order 24.

Let $p(x) = x^4 + ax^3 + bx^2 + cx + d$ be an irreducible quartic over F and let us assume that $\mathrm{char}(F) \neq 2, 3$. This will insure that $4 \neq 0$ and that all irreducible cubic polynomials that we may encounter are separable. Replacing x by $x - a/4$ will eliminate the cubic term, resulting in a polynomial of the form

$$q(x) = x^4 + px^2 + qx + r$$

The polynomials p(x) and q(x) have the same splitting field and hence the same Galois group, so let us work with q(x). Let E be the splitting field of q(x), let $r_1, \ldots, r_4$ be its roots in E and let $G = G_F(E)$ be its Galois group. For convenience, we identify G with its isomorphic image in S_4.

The Quartic $x^4 + bx^2 + c$

In order to get our feet wet, let us first consider the special case

$$q(x) = x^4 + bx^2 + c$$

If we denote the roots of $q(x)$ in E by $\pm\alpha$, $\pm\beta$ then $E = F(\alpha,\beta)$ and

$$b = -(\alpha^2 + \beta^2), \quad c = \alpha^2\beta^2$$

We define the **associated quadratic** to $q(x)$ to be

$$\bar{q}(x) = x^2 + bx + c$$

The roots α^2 and β^2 of $\bar{q}(x)$ are given by

$$\alpha^2, \beta^2 = \frac{-b \pm \sqrt{b^2 - 4c}}{2}$$

The irreducibility of $q(x)$ can be determined as follows. Certainly if $\bar{q}(x)$ is reducible over F, then so is $q(x)$. On the other hand, if $\bar{q}(x)$ is irreducible then its roots α^2 and β^2 do not lie in F, whence $q(x)$ cannot have a linear factor over F and, if reducible, must have the form

$$q(x) = x^4 + bx^2 + c = (x^2 + ux + v)(x^2 - ux + w)$$

where, as seen by equating coefficients, $u(v - w) = 0$. However, if $u = 0$ then

$$q(x) = (x^2 + v)(x^2 + w)$$

which gives

$$\bar{q}(x) = (x + v)(x + w)$$

contradicting the irreducibility of $\bar{q}(x)$. Thus, $u \neq 0$ and $v = w$. We can summarize as follows:

1) If $\sqrt{b^2 - 4c} \in F$ then $\bar{q}(x)$, and therefore $q(x)$, is reducible.

2) If $\sqrt{b^2 - 4c} \notin F$ then $q(x)$ is reducible if and only if it has the form

$$q(x) = x^4 + bx^2 + c = (x^2 + ux + v)(x^2 - ux + v)$$

where $v^2 = c$ and $2v - u^2 = b$.

For example, let $q(x) = x^4 + 6x^2 + 4$ over $\mathbf{Q}$. Then $b^2 - 4c = 20$ and $\sqrt{20} \notin \mathbf{Q}$. From 2) above we have

$$v^2 = 4, \; v = \pm 2$$

and

$$u^2 = 2v - 6 = \pm 4 - 6 = -2, -10$$

and since the latter has no solutions $u \in \mathbb{Q}$, we see that $q(x)$ is irreducible over $\mathbb{Q}$.

Let us now assume that $q(x)$ is irreducible over F and has distinct roots. We have seen that $[E:F] = 4$, 8, 12 or 24. However, not all permutations of the roots are elements of the Galois group G. For instance, if $\sigma \in G$ sends α to β, it must send $-\alpha$ to $-\beta$. The possibilities for elements of G are listed below, where we give the action on α and β, as well as a description as a product of transpositions, assuming that the roots are taken in the order α, β, $-\alpha$, $-\beta$.

1) $\sigma_1: \alpha \to \alpha,\ \beta \to \beta$ (1)
2) $\sigma_2: \alpha \to \alpha,\ \beta \to -\beta$ (24)
3) $\sigma_3: \alpha \to -\alpha,\ \beta \to \beta$ (13)
4) $\sigma_4: \alpha \to -\alpha,\ \beta \to -\beta$ (13)(24)
5) $\sigma_5: \alpha \to \beta,\ \beta \to \alpha$ (12)(34)
6) $\sigma_6: \alpha \to \beta,\ \beta \to -\alpha$ (14)(13)(12)
7) $\sigma_7: \alpha \to -\beta,\ \beta \to \alpha$ (12)(13)(14)
8) $\sigma_8: \alpha \to -\beta,\ \beta \to -\alpha$ (14)(23)

Note that all nonidentity maps have order 2 except α_6 and α_7. In fact, $\{\sigma_1, \ldots, \sigma_8\}$ is isomorphic to the dihedral group D_4, with rotation σ_6 (order 4) and reflection σ_8 (order 2). Thus G is (isomorphic to) a subgroup of D_4 and so $[E:F] = 4$ or 8. In the latter case $G \simeq D_4$. In the former case, $G \simeq \mathbb{Z}_4$ or $G \simeq V$.

The square root of the discriminant of $q(x)$ is

$$\delta = (\alpha - \beta)(\alpha + \alpha)(\alpha + \beta)(\beta + \alpha)(\beta + \beta)(-\alpha + \beta) = -4\alpha\beta(\alpha^2 - \beta^2)^2$$

and since $(\alpha^2 - \beta^2)^2$ is invariant under each σ_i, it must lie in the base field F. Hence, $\delta \in F$ if and only if $\alpha\beta \in F$, or equivalently, $\sqrt{c} \in F$. It follows from Theorem 6.3.1 that

1) If $\sqrt{c} \in F$ then G is isomorphic to a subgroup of A_4. Thus, it contains only even permutations and so

$$G = \{\sigma_1, \sigma_4, \sigma_5, \sigma_8\} = V$$

2) If $\sqrt{c} \notin F$ then G contains half even and half odd permutations and $G \cap A_4$ is $F(\delta) = F(\sqrt{c})$.

Under case 2), we still have the possibilities $|G| = 4$ or $|G| = 8$. In the former case, $G \cap A_4$ must consist of σ_1 and one of the even permutations σ_4, σ_5 or σ_8. The other two elements of G must come from the odd permutations σ_2, σ_3, σ_6 and σ_7. If G has no element of order 4, then we can eliminate σ_6 and σ_7. But it is easy to check that the set $\{\sigma_1, \sigma_i, \sigma_2, \sigma_3\}$, where $i = 4$, 5 or 8, is not transitive on the roots of q(x). Hence, G must contain an element of order 4 and

$$G = \{\sigma_1, \sigma_6, \sigma_6^2 = \sigma_4, \sigma_6^3 = \sigma_7\} \simeq \mathbb{Z}_4$$

To identify the case $G \simeq \mathbb{Z}_4$ directly from the coefficients of q(x), observe that in this case $[E:F(\sqrt{c})] = 2$ and so q(x) has an irreducible quadratic factor over $F(\sqrt{c})$. Thus,

$$q(x) = x^4 + bx^2 + c = (x^2 + ux + v)(x^2 - ux + w)$$

where $r(x) = x^2 + ux + v$ is irreducible over $F(\sqrt{c})$. Since

$$G_{F(\sqrt{c})}(E) = \{\sigma_1, \sigma_4\}$$

it follows that σ_4 must send one root of r(x) to the other root and so the roots of r(x) are $\pm\alpha$ or $\pm\beta$. In either case, $u = 0$ and so

$$q(x) = x^4 + bx^2 + c = (x^2 + v)(x^2 + w) \tag{6.4.1}$$

which implies that $\bar{q}(x)$ is reducible over $F(\sqrt{c})$, that is,

$$\sqrt{b^2 - 4c} \in F(\sqrt{c})$$

or, equivalently,

$$\sqrt{c(b^2 - 4c)} \in F$$

Conversely, if this holds, then $\bar{q}(x)$ is reducible over $F(\sqrt{c})$ and therefore q(x) has the form (6.4.1), where $v, w \in F(\sqrt{c})$. Since $vw = c$, the polynomial q(x) splits over $F(\sqrt{c}, \sqrt{v})$, whence $E = F(\sqrt{c}, \sqrt{v})$. Thus, $[E:F(\sqrt{c})] = 2$ and $[E:F] = 4$. Let us summarize.

Theorem 6.4.3 Let $q(x) = x^4 + bx^2 + c$ be irreducible with distinct roots over F. Let G be the Galois group of q(x). Let V be the viergruppe.

1) If $\sqrt{c} \in F$ then $G = V$.
2) If $\sqrt{c} \notin F$ and $\sqrt{c(b^2 - 4c)} \in F$ then $G \simeq \mathbb{Z}_4$ and $\bar{q}(x)$ is reducible over $F(\sqrt{c})$.

3) If $\sqrt{c} \notin F$ and $\sqrt{c(b^2-4c)} \notin F$ then $G \simeq D_4$ and $\overline{q}(x)$ is irreducible over $F(\sqrt{c})$. □

The General Quartic

To analyze the general quartic polynomial p(x), we consider which elements of the Galois group lie in the viergruppe V. This gives us a subgroup $V \cap G$ of G and hence an intermediate subfield $F(V \cap G)$ of the splitting field E. Since $V \lhd S_4$ we have $V \cap G \lhd G$. Our guide will be Figure 6.4.1.

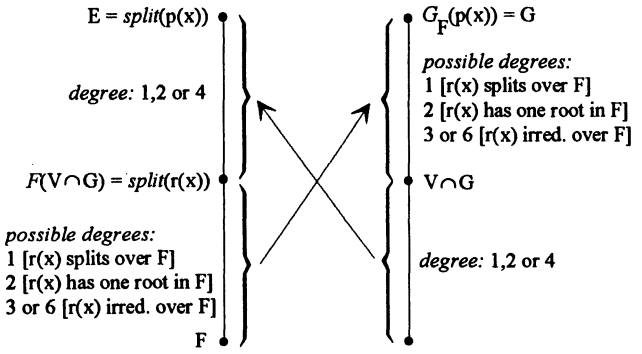

Figure 6.4.1

To determine the fixed field of $V \cap G$, note that each element of V fixes the elements

$$u = (r_1 + r_2)(r_3 + r_4)$$
$$v = (r_1 + r_3)(r_2 + r_4)$$
$$w = (r_1 + r_4)(r_2 + r_3)$$

and so $F(u,v,w) < F(V \cap G)$. By checking each permutation in S_4, it is not hard to see that no permutation outside of V fixes u, v and w. Thus,

$$G_{F(u,v,w)}(E) < V \cap G$$

Taking fixed fields gives $F(V \cap G) < F(u,v,w)$ and so $F(V \cap G) = F(u,v,w)$.

Note also that any element of S_4 permutes the elements u, v and w and so any symmetric function of u, v and w is also a symmetric function of $r_1, \ldots, r_4$.

Definition The **resolvent cubic** of $q(x) = x^4 + px^2 + qx + r$ is the polynomial $r(x) = (x-u)(x-v)(x-w)$. □

To determine the coefficients of r(x), note that since q(x) has no cubic term, it follows that $r_1 + r_2 + r_3 + r_4 = 0$. Hence,

$$(r_1 + r_2)^2 = -(r_1 + r_2)(r_3 + r_4) = -u$$

Thus, r(x) is a polynomial satisfied by $-(r_1 + r_2)^2$. The polynomial q(x) factors into a product of quadratic polynomials over E, say

$$q(x) = (x^2 + ax + b)(x^2 - ax + c)$$

where the linear coefficients are negatives of each other since q(x) has no cubic term. We can always renumber so that the roots of the first factor are r_1 and r_2, whence $a = -(r_1 + r_2)$. Multiplying out the expression for q(x) and equating coefficients gives

$$\begin{aligned} b + c - a^2 &= p \\ ac - ab &= q \\ bc &= r \end{aligned}$$

Solving the first two for b and c and substituting into the third gives

$$a^6 + 2pa^4 + (p^2 - 4r)a^2 - q^2 = 0$$

and so $a^2 = (r_1 + r_2)^2 = -u$ satisfies the polynomial

$$s(x) = x^3 + 2px^2 + (p^2 - 4r)x - q^2$$

Thus u satisfies the polynomial

$$t(x) = x^3 - 2px^2 + (p^2 - 4r)x + q^2$$

Since we will get the same polynomial by repeating this argument using $r_1 + r_3$ or $r_1 + r_4$ in place of $r_1 + r_2$, we deduce that t(x) is the resolvent cubic of q(x).

Theorem 6.4.4 The resolvent cubic of $q(x) = x^4 + px^2 + qx + r$ is

$$r(x) = x^3 - 2px^2 + (p^2 - 4r)x + q^2$$

The splitting field of r(x) over F is the fixed field $F(V \cap G)$. Hence,

$$| G_F(r(x)) | = [F(V \cap G):F] = (G:V \cap G) \qquad \square$$

Let us put all of the pieces together.

Theorem 6.4.5 Let $p(x) = x^4 + ax^3 + bx^2 + cx + d$ be an irreducible quartic over a field F, with $\mathrm{char}(F) \neq 2, 3$. Let $q(x) = x^4 + px^2 + qx + r$ be obtained from p(x) by substituting $x - a/4$ for x and let $r(x) = x^3 - 2px^2 + (p^2 - 4r)x + q^2$ be the resolvent cubic of q(x). Let Δ_r be the discriminant of r(x) and let E be the splitting field for p(x) over F.

1) If r(x) is irreducible over F and $\sqrt{\Delta_r} \in F$ then $G_F(p(x)) \simeq A_4$.
2) If r(x) is irreducible over F and $\sqrt{\Delta_r} \notin F$ then $G_F(p(x)) \simeq S_4$.
3) If r(x) splits over F then $G_F(p(x)) \simeq V$.
4) If r(x) has a single root in F there are two possibilities: (i) if p(x) is reducible over $F(V \cap G)$ it has an irreducible quadratic factor and $G_F(p(x)) \simeq \mathbb{Z}_4$, (ii) if p(x) is irreducible over $F(V \cap G)$ then $G_F(p(x)) \simeq D_4$.

Proof. Let $G = G_F(p(x))$. The situation is described in Figure 6.4.1. We begin by observing that $V \cap G < V$ and so

$$|V \cap G| = 1, 2 \text{ or } 4, \quad (G:V \cap G) = 1, 2, 3 \text{ or } 6$$

and

$$|V \cap G| \times (G:V \cap G) = |G| = 4, 8, 12 \text{ or } 24$$

This shows immediately that $|V \cap G| \neq 1$. Let us write the possibilities as follows

$$|V \cap G| \times (G:V \cap G) = |G|$$
$$(2/4) \times (1/2/3/6) = (4/8/12/24)$$

Now we can use Theorem 6.4.2. Let S be the splitting field of r(x) over F.

1) If r(x) is irreducible and $\sqrt{\Delta_r} \in F$ then $G_F(r(x)) \simeq A_3$. Theorem 6.4.4 gives $(G:V \cap G) = 3$, which implies that $|V \cap G| = 4$ and so $|G| = 12$. Thus $G \simeq A_4$.
2) If r(x) is irreducible and $\sqrt{\Delta_r} \notin F$ then $G_F(r(x)) \simeq S_3$. Hence $(G:V \cap G) = 6$. If $|V \cap G| = 2$ then $|G| = 12$ so $G \simeq A_4$. But $V \subseteq A_4$ then implies that $|V \cap G| = 4$. Thus, $|V \cap G| \neq 2$, leaving the only other possibility: $|V \cap G| = 4$. Hence $|G| = 24$ and $G \simeq S_4$.
3) If r(x) splits over F then $(G:V \cap G) = [S:F] = 1$ and so $|V \cap G| = 4$, whence $V \subseteq G$ and $G \simeq V$.
4) Suppose that r(x) has a single root in F. Then $(G:V \cap G) = [S:F] = 2$. There are two possibilities. If $|V \cap G| = 2$ then

$|G| = 4$ and so $G \simeq \mathbb{Z}_4$ or V. We leave it to the reader to show that since G acts transitively, $G \simeq V$ is not possible. Hence, $G \simeq \mathbb{Z}_4$. Note that, in this case, since E is the splitting field for p(x) over S and $[E:S] = 2$ the polynomial p(x) must have an irreducible quadratic factor over S. If $|V \cap G| = 4$ then $|G| = 8$ and $G \simeq D_4$. In this case, p(x) is irreducible over S. ∎

Exercises

1. Let $p(x) = x^n - a_1x^{n-1} + \cdots + a_n$ where $a_1, \ldots, a_n$ are algebraically independent over F. Show that p(x) is irreducible over $F(a_1, \ldots, a_n)$, separable and its Galois group is isomorphic to S_n.
2. Give an example to show that separability is required in Corollary 6.2.3.
3. If p(x) is a quartic polynomial then its discriminant is the negative of the discriminant of its resolvent cubic. *Hint*: $u - v = -(r_1 - r_4)(r_2 - r_3)$.
4. Find the Galois groups of the following polynomials: (i) $x^4 - 10x^2 + 1$; (ii) $x^4 - 4x + 2$; (iii) $x^4 + 8x - 12$ (iv) $x^4 + x^2 + x + 1$
5. If $p(x) \in F[x]$ has roots $r_1, \ldots, r_n$ then $\Delta = (-1)^{n(n-1)/2} \prod_i p'(r_i)$.
6. Let $p(x) \in \mathbb{Q}[x]$ have degree 3. Show that $\Delta < 0$ if and only if p(x) has exactly one real root.
7. Show that the splitting field for an irreducible cubic polynomial over F is given by $F(\sqrt{\Delta}, r)$, where r is a root of f(x) and Δ is the discriminant.
8. Let $p(x) = (x - r)(x - s)(x - t)$, where r, s and t are algebraically independent over $\mathbb{Z}_2$. Let s_1, s_2, s_3 be the elementary symmetric functions on r, s and t. Show that $\sqrt{\Delta} \in F(s_1, s_2, s_3)$ but the Galois group of p(x) over $F(s_1, s_2, s_3)$ is isomorphic to S_3.
9. Let
$$p(x) = x^n - s_1x^{n-1} + \cdots + (-1)^n s_n$$
have roots $r_1, \ldots, r_n$ in a splitting field E over F. Let $u_i = r_1^i + r_2^i + \cdots + r_n^i$. Since the u_i's are symmetric polynomials in the roots of p(x), Theorem 6.2.2 implies that they can be expressed as symmetric polynomials in the elementary symmetric functions $s_1, \ldots, s_n$. One way to derive an expression relating the u_i's to the s_i's is by following the proof of Theorem 6.2.2. Here is another way. Let $p(x) = (x - r_i)q_i(x)$ in E[x].

   a) Show that $D^{k+1}p(x) = \sum_i D^k q_i(x)$.

b) Write

$$q_i(x) = \frac{p(x) - p(r_i)}{x - r_i}$$

and use part a) to derive *Newton's identities*:

$$u_k - u_{k-1}s_1 + u_{k-2}s_2 + \cdots + (-1)^{k-1}u_1 s_{k-1} + (-1)^k k s_k = 0$$

for $k = 1, 2, 3, \ldots$.

c) Let $p(x) = a + bx + x^n$. Find the values of u_i and find the discriminant of $p(x)$.

10. Show that the viergruppe V is normal in S_4. Find another subgroup of S_4 besides V that is isomorphic to V.

11. This exercise concerns the issue of when a real number that is expressed in terms of nested radicals

$$\alpha = \sqrt{r + s\sqrt{t}}$$

where $r, s, t \in F$ can be written in terms of at most two unnested radicals. For instance, we have

$$\sqrt{5 + \sqrt{21}} = \tfrac{1}{2}(\sqrt{6} + \sqrt{14})$$

but the number $\sqrt{7 + 2\sqrt{5}}$ cannot be so written. Note that α is a root of the quartic

$$q(x) = x^4 - 2rx^2 + (r^2 - s^2 t) = [x^2 - (r + s\sqrt{t})][x^2 - (r - s\sqrt{t})]$$

Assume that $q(x)$ is irreducible over F. The question we are interested in is whether $\alpha \in F(\sqrt{p}, \sqrt{q})$ for some p and q in F. Show that the answer to this question is yes if and only if $F(\sqrt{p}, \sqrt{q})$ is the splitting field E for $q(x)$ over F. Then show that $E = F(\sqrt{p}, \sqrt{q})$ if and only if the Galois group G of $q(x)$ over F is the viergruppe V. Hence, $\alpha \in F(\sqrt{p}, \sqrt{q})$ if and only if

$$\sqrt{r^2 - s^2 t} \in F$$

Find a way to compute the unnested expression for α in terms of $\sqrt{p}$ and $\sqrt{q}$.

12. Let $p(x) = x^4 + bx^3 + cx^2 + dx + 1 \in \mathbb{Q}[x]$ have Galois group G.
(i) If $u = c^2 + 4c + 4 - 4b^2$ has a square root in $\mathbb{Q}$ then $G \simeq V$.
(ii) If u does not have a square root in $\mathbb{Q}$ but $u(b^2 - 4c + 8)$ does have a square root in $\mathbb{Q}$ then $G \simeq \mathbb{Z}_4$.
(iii) If neither u nor $u(b^2 - 4c + 8)$ has a square root in $\mathbb{Q}$ then $G \simeq D_4$.

Chapter 7
A Field Extension as a Vector Space

In this chapter, we take a closer look at a finite field extension $F < E$ from the point of view that E is a vector space over F. It is clear, for instance, that any $\sigma \in G_F(E)$ is a linear operator on E over F. However, there are many linear operators that are not field automorphisms. One of the most important is multiplication by a fixed element of E, which we study next.

7.1 The Norm and the Trace

Let $F < E$ be finite and let $\alpha \in E$. The multiplication map $\hat{\alpha}:E \to E$ defined by $\hat{\alpha}\beta = \alpha\beta$ is an F-linear operator from E to E, since

$$\hat{\alpha}(u\beta + v\gamma) = u\hat{\alpha}\beta + v\hat{\alpha}\gamma$$

for all $u, v \in F$ and $\beta, \gamma \in E$. We wish to find a basis for E over F under which the matrix of $\hat{\alpha}$ has a nice form.

Note that if $r(x) \in F[x]$, then $r(\hat{\alpha})\beta = r(\alpha)\beta$ for all $\beta \in E$ and so $r(\alpha) = 0$ as an element of E if and only if $r(\hat{\alpha})$ is the zero operator on E. Hence, the set of polynomials over F satisfied by $\hat{\alpha}$ is precisely the same as the set of polynomials satisfied by α. In particular, they have the same minimal polynomial over F.

The vector subspace $F(\alpha)$ of E is invariant under $\hat{\alpha}$, since $\hat{\alpha}(p(\alpha)) = \alpha p(\alpha) \in F(\alpha)$. If $\mathfrak{B} = \{\beta_1, \ldots, \beta_d\}$ is an ordered basis for $F(\alpha)$ over F and if

$$\hat{\alpha}\beta_i = \sum_{j=1}^{d} b_{i,j}\beta_j$$

then the matrix of $\hat{\alpha}\,|_{F(\alpha)}$ with respect to $\mathfrak{B}$ is $M = (b_{i,j})$. If $\{\gamma_1,\ldots,\gamma_e\}$ is a basis for E over $F(\alpha)$ where $e = [E:F(\alpha)]$, then the set of products

$$\mathfrak{C} = \{\gamma_1\beta_1,\gamma_1\beta_2,\ldots,\gamma_1\beta_d,\ldots,\ldots,\gamma_e\beta_1,\gamma_e\beta_2,\ldots,\gamma_e\beta_d\}$$

is a basis for E over F. Since

$$\hat{\alpha}(\gamma_k\beta_i) = \sum_{j=1}^{d} b_{i,j}\gamma_k\beta_j$$

it follows that each of the subspaces $V_k = \langle\gamma_k\beta_1,\gamma_k\beta_2,\ldots,\gamma_k\beta_d\rangle$ is invariant under $\hat{\alpha}$ and the matrix of $\hat{\alpha}\,|_{V_k}$ is also equal to M. Hence, the matrix of $\hat{\alpha}$ with respect to the ordered basis $\mathfrak{C}$ has the block diagonal form

$$\mathcal{M}_{\mathfrak{C}}(\hat{\alpha}) = \begin{bmatrix} M & 0 & 0 & 0 \\ 0 & M & 0 & 0 \\ 0 & 0 & \ddots & 0 \\ 0 & 0 & 0 & M \end{bmatrix} \tag{7.1.1}$$

Thus, if the characteristic polynomial of $\hat{\alpha}\,|_{F(\alpha)}$ is $q(x)$, then the characteristic polynomial of $\hat{\alpha}$ (on E) is

$$q_\alpha(x) = q(x)^{[E:F(\alpha)]}$$

But $q(x) \in F[x]$ has degree $[F(\alpha):F] = deg\ min(\alpha,F)$, is monic and is also satisfied by α, whence $q(x) = min(\alpha,F)$.

Theorem 7.1.1 Let $F < E$ be finite and let $\alpha \in E$. If $\hat{\alpha}:E\to E$ is the F-linear operator on E defined by $\hat{\alpha}\beta = \alpha\beta$ then the characteristic polynomial of $\hat{\alpha}$ is

$$q_\alpha(x) = [min(\alpha,F)]^{[E:F(\alpha)]}$$ □

We recall from linear algebra that if $\tau:V\to V$ is a linear operator on a finite dimensional vector space V over F, the *trace* of τ is the sum of the eigenvalues of τ and the *norm* (*determinant*) of τ is the product of the eigenvalues of τ, in both cases counting multiplicities. Recall also that the trace and the norm both lie in the base field F. We are motivated to make the following definition.

Definition Let $F < E$ be finite and let $\alpha \in E$. The **trace** of α over $F < E$, denoted by $Tr_{E/F}(\alpha)$, is the trace of the F-linear operator $\hat{\alpha}:E\to E$ and the **norm** of α over $F < E$, denoted by $N_{E/F}(\alpha)$, is the norm of $\hat{\alpha}:E\to E$. □

Note that the trace and norm of α depend on the extension field E, and not just on the element α itself.

Since the trace of a linear operator is the sum of the roots of its characteristic polynomial and the norm is the product of these roots, Theorem 7.1.1 allows us to express the trace and norm in terms of the roots of the minimal polynomial. Let $F < E$ be finite, let $\alpha \in E$ and let

$$p(x) = min(\alpha,F) = x^d + a_{d-1}x^{d-1} + \cdots + a_0$$

have roots $r_1,\ldots,r_d$ in a splitting field. It follows from Theorem 7.1.1 that

$$Tr_{E/F}(\alpha) = [E:F(\alpha)] \sum_{i=1}^{d} r_i = -[E:F(\alpha)]a_{d-1}$$

and

$$N_{E/F}(\alpha) = \prod_{i=1}^{d} r_i^{[E:F(\alpha)]} = [(-1)^d a_0]^{[E:F(\alpha)]}$$

We remark that many authors simply define the trace and norm of α directly from these formulas.

Alternate expressions for the trace and the norm can be obtained as follows. Let $r_1,\ldots,r_s$ be the *distinct* roots of $p(x)$. Each of these roots appears with multiplicity $[F(\alpha):F]_i$ (Theorem 4.6.1) and so

$$Tr_{E/F}(\alpha) = [E:F(\alpha)][F(\alpha):F]_i \sum_{i=1}^{s} r_i = [E:F(\alpha)]_s[E:F]_i \sum_{i=1}^{s} r_i$$

and

$$N_{E/F}(\alpha) = \prod_{i=1}^{s} r_i^{[E:F(\alpha)][F(\alpha):F]_i} = \prod_{i=1}^{s} r_i^{[E:F(\alpha)]_s[E:F]_i}$$

Now let us take a look at the trace and the norm from the perspective of embeddings of E into an algebraic closure. Let $F < E$ be finite and let $Hom_F(E,\overline{F}) = \{\sigma_1,\ldots,\sigma_n\}$ be the set of all embeddings of E into $\overline{F}$ over F. If $\alpha \in E$ and $p(x) = min(\alpha,F)$, then $\sigma_1\alpha,\ldots,\sigma_n\alpha$ is a list of the roots of $p(x)$ in $\overline{F}$. However, each root may appear more than once in this list.

To see how many times each root appears, consider the tower $F < F(\alpha) < E$. Each embedding σ_i is obtained by extending to E an F-embedding τ of $F(\alpha)$ into $\overline{F}$, and this can be done in $[E:F(\alpha)]_s$ different ways. Each extension of τ has the same value on α and each embedding τ of $F(\alpha)$ into $\overline{F}$ has a different value on α. Hence, the list $\sigma_1\alpha,\ldots,\sigma_n\alpha$ contains exactly $[E:F(\alpha)]_s$ copies of each root of $p(x)$. Thus, if $r_1,\ldots,r_s$ are the distinct roots of $p(x)$ in $\overline{F}$, then

$$\sum_{i=1}^{n} \sigma_i \alpha = [E:F(\alpha)]_s \sum_{i=1}^{s} r_i$$

and

$$\prod_{i=1}^{n} \sigma_i \alpha = \prod_{i=1}^{s} r_i^{[E:F(\alpha)]_s}$$

These formulas give another expression for the norm and the trace. Let us summarize.

Theorem 7.1.2 Let $F < E$ be finite and let $\alpha \in E$ with $p(x) = min(\alpha,F) = x^d + a_{d-1}x^{d-1} + \cdots + a_0$.

1) If $p(x)$ has roots $r_1,\ldots,r_d$ then

$$Tr_{E/F}(\alpha) = [E:F(\alpha)] \sum_{i=1}^{d} r_i = -[E:F(\alpha)]a_{d-1}$$

and

$$N_{E/F}(\alpha) = \prod_{i=1}^{d} r_i^{[E:F(\alpha)]} = [(-1)^d a_0]^{[E:F(\alpha)]}$$

2) If $p(x)$ has distinct roots $r_1,\ldots,r_s$ then

$$Tr_{E/F}(\alpha) = [E:F(\alpha)]_s [E:F]_i \sum_{i=1}^{s} r_i$$

and

$$N_{E/F}(\alpha) = \prod_{i=1}^{s} r_i^{[E:F(\alpha)]_s [E:F]_i}$$

3) If $\mathrm{Hom}_F(E,\overline{F}) = \{\sigma_1,\ldots,\sigma_n\}$ then

$$Tr_{E/F}(\alpha) = [E:F]_i \sum_{i=1}^{n} \sigma_i \alpha$$

and

$$N_{E/F}(\alpha) = \prod_{i=1}^{n} (\sigma_i \alpha)^{[E:F]_i}$$

□

Theorem 7.1.2 can be used to derive some basic properties of the trace and the norm. We leave proof of the following to the reader.

Theorem 7.1.3 Let $F < E$ be finite.

1) The trace is an F-linear functional on E, that is, for all $\alpha, \beta \in E$ and $a, b \in F$,

$$Tr_{E/F}(a\alpha+b\beta) = a\,Tr_{E/F}(\alpha)+b\,Tr_{E/F}(\beta)$$

2) For all $\alpha, \beta \in E$ and $a \in F$

$$N_{E/F}(\alpha\beta) = N_{E/F}(\alpha)N_{E/F}(\beta) \quad \text{and} \quad N_{E/F}(a\alpha) = a^{[E:F]}\,N_{E/F}(\alpha)$$

3) If $a \in F$ then

$$Tr_{E/F}(a) = [E:F]a \quad \text{and} \quad N_{E/F}(a) = a^{[E:F]}$$

3) If $F < E < L$ are finite and if $\alpha \in L$ then

$$Tr_{L/F}(\alpha) = Tr_{E/F}(Tr_{L/E}(\alpha)), \quad N_{L/F}(\alpha) = N_{E/F}(N_{L/E}(\alpha)) \qquad \square$$

*7.2 The Discriminant of Field Elements

Our goal in this section is to describe conditions that guarantee that a given set $\{\alpha_1,\ldots,\alpha_n\}$ of elements of E is a basis for E over F. We begin with a few remarks on metric vector spaces. (For more details, see Roman, *Advanced Linear Algebra*, Springer-Verlag, Graduate Texts in Mathematics Vol. 135, 1992.)

Definition Let V be a vector space over a field F. A mapping $\langle,\rangle: V \times V \to F$ is called a **bilinear form** if it is a linear function of each coordinate, that is, if for all $x,y \in V$ and $\alpha,\beta \in F$

$$\langle \alpha x + \beta y, z\rangle = \alpha\langle x,z\rangle + \beta\langle y,z\rangle \quad \text{and} \quad \langle z, \alpha x + \beta y\rangle = \alpha\langle z,x\rangle + \beta\langle z,y\rangle$$

The pair $(V,\langle,\rangle)$ is called a **metric vector space**. A bilinear form is **symmetric** if $\langle x,y\rangle = \langle y,x\rangle$ for all $x, y \in V$. $\square$

If $S \subseteq V$, we let $\langle x,S\rangle = \{\langle x,s\rangle \mid s \in S\}$.

Definition A metric vector space is **nonsingular** if $\langle x,V\rangle = \{0\}$ implies that $x = 0$. A metric vector space V is **null** if $\langle x,y\rangle = 0$ for all $x, y \in V$. $\square$

If $\mathfrak{B} = \{b_i\}$ is a basis for V over F and if $x = \sum x_i b_i \in V$, we will denote the coordinate (row) matrix $(x_1,\ldots,x_n)$ by the boldface notation $\mathbf{x}$. The **matrix of the form** $\langle,\rangle$ with respect to $\mathfrak{B}$ is

$$M_{\mathcal{B}} = (\langle b_i, b_j \rangle)$$

Here are some key facts about the matrix of a form. We leave proof to the reader.

Theorem 7.2.1

1) If $M_{\mathcal{B}}$ is the matrix of a bilinear form on V then
$$\langle x, y \rangle = x M_{\mathcal{B}} y^T$$
for all $x, y \in V$.
2) Two matrices M and N represent the same bilinear forms on V, with respect to possibly different bases, if and only if they are **congruent**, that is, if and only if $M = PNP^T$ for some invertible matrix P.
3) A metric vector space is nonsingular if and only if any, and hence all, of the matrices that represent the form are nonsingular. □

Now we can return to the business at hand. Let $F < E$ be a finite extension and let

$$\langle \alpha, \beta \rangle = \mathrm{Tr}_{E/F}(\alpha\beta) \tag{7.2.1}$$

for all $\alpha, \beta \in E$. This is easily verified to be a symmetric bilinear form on E over F. If $\mathcal{B} = \{\beta_1, \ldots, \beta_n\}$ is a basis for E over F, then the matrix of the form $\langle , \rangle$ is

$$M_{\mathcal{B}} = (\langle \beta_i, \beta_j \rangle) = (\mathrm{Tr}_{E/F}(\beta_i \beta_j))$$

This form has rather special properties, due to the fact that

$$\langle \gamma\alpha, \beta \rangle = \langle \alpha, \gamma\beta \rangle$$

for all $\alpha, \beta, \gamma \in E$.

Theorem 7.2.2 Let $F < E$ be finite, with form given by (7.2.1). Then either

1) E is null and the trace map is identically zero, or
2) E is nonsingular and every matrix representing $\langle , \rangle$ is nonsingular.

Proof. If E is singular then $\langle \alpha, E \rangle = 0$ for some $\alpha \neq 0$ and so $\langle 1, E \rangle = \{0\}$. It follows that $\langle , \rangle$ is null and the trace map is identically zero. ∎

Thus, any matrix representing the form (7.2.1) is either the zero matrix or it is nonsingular. Note that, if $\mathrm{char}(F) = p \neq 0$, then the zero

matrix will arise when $p \mid \mathrm{Tr}_{E/F}(\alpha)$ for all $\alpha \in E$. Referring to part 3) of Theorem 7.1.2, we see that this happens when $[E:F]_i > 1$, since $[E:F]_i$ is a power of p. In other words, if $F < E$ is not separable, then E is null. The converse also holds.

Theorem 7.2.3 Let $F < E$ be finite, with form (7.2.1). Then E is nonsingular if and only if $F < E$ is separable.

Proof. We have just seen that if $F < E$ is not separable then E is singular. For the converse, suppose that $F < E$ is finite and separable. Then there exists a primitive element $\alpha \in E$. If $E = F(\alpha)$ has degree n over F then the elements $1, \alpha, \ldots, \alpha^{n-1}$ form a basis for E over F. Referring to part 3) of Theorem 7.1.2, and letting $\alpha_i = \sigma_i\alpha$ be the roots of $min(\alpha,F)$ and $\boldsymbol{\alpha}^k = (\alpha_1^k, \ldots, \alpha_n^k)$, we have

$$\mathrm{Tr}_{E/F}(\alpha^k\alpha^j) = \sum_{i=1}^{n} \sigma_i(\alpha^k\alpha^j) = \sum_{i=1}^{n} \alpha_i^k\alpha_i^j = \boldsymbol{\alpha}^k(\boldsymbol{\alpha}^j)^T$$

Thus, if V is the Vandermonde matrix

$$V = \begin{bmatrix} \boldsymbol{\alpha}^0 \\ \boldsymbol{\alpha}^1 \\ \boldsymbol{\alpha}^2 \\ \vdots \\ \boldsymbol{\alpha}^{n-1} \end{bmatrix} = \begin{bmatrix} 1 & 1 & \cdots & 1 \\ \alpha_1 & \alpha_2 & \cdots & \alpha_{n-1} \\ \alpha_1^2 & \alpha_2^2 & \cdots & \alpha_{n-1}^2 \\ \vdots & \vdots & \cdots & \vdots \\ \alpha_1^{n-1} & \alpha_2^{n-1} & \cdots & \alpha_{n-1}^{n-1} \end{bmatrix}$$

then

$$[\mathrm{Tr}_{E/F}(\alpha^k\alpha^j)] = VV^T$$

and so

$$\det(\mathrm{Tr}_{E/F}(\alpha^k\alpha^j)) = (\det V)^2$$

It is well-known that

$$\det V = \prod_{i<j} (\alpha_i - \alpha_j)$$

Since α is separable, the α_i's, being the roots of the separable polynomial $min(\alpha,F)$, are distinct and so $\det V \neq 0$. Hence $\langle , \rangle$ is nonsingular. ∎

In view of the previous results, the trace map and the form (7.2.1) are interesting only when the form is nonsingular, that is, only when $F < E$ is separable.

Definition Let $F < E$ be finite and let $\alpha_1,\ldots,\alpha_n \in E$. The **discriminant** of $\alpha_1,\ldots,\alpha_n$ is the determinant

$$\Delta_{E/F}(\alpha_1,\ldots,\alpha_n) = |\langle\alpha_i,\alpha_j\rangle| = |\mathrm{Tr}_{E/F}(\alpha_i\alpha_j)|$$

Thus, if $\alpha_1,\ldots,\alpha_n$ is a basis for E over F then the discriminant is the determinant of the matrix that represents the form (7.2.1) with respect to this basis. □

When $F < E$ is finite and separable, the discriminant can be used to determine whether or not a set of vectors is a basis for E over F.

Theorem 7.2.4 If $F < E$ is finite and separable of degree n, then $\{\alpha_1,\ldots,\alpha_n\}$ is a basis for E over F if and only if $\Delta_{E/F}(\alpha_1,\ldots,\alpha_n) \neq 0$.

Proof. Since E is nonsingular, if $\{\alpha_1,\ldots,\alpha_n\}$ is a basis for E over F, then $(\langle\alpha_i,\alpha_j\rangle)$ is nonsingular and so $\Delta_{E/F}(\alpha_1,\ldots,\alpha_n) \neq 0$. Conversely, assume that $\Delta_{E/F}(\alpha_1,\ldots,\alpha_n) \neq 0$ and that

$$\sum_i a_i\alpha_i = 0$$

for $a_i \in F$. Multiplying by α_k and taking the trace gives

$$\sum_i a_i\mathrm{Tr}_{E/F}(\alpha_i\alpha_k) = 0$$

and since the rows of the matrix $(\mathrm{Tr}_{E/F}(\alpha_i\alpha_j))$ are linearly independent, we have $a_i = 0$ for all i, whence $\{\alpha_1,\ldots,\alpha_n\}$ is a basis for E over F. ∎

We next derive an alternate expression for the discriminant. Let $F < E$ be finite and separable and let $\alpha_1,\ldots,\alpha_n \in E$. Let $\mathrm{Hom}(E,\overline{F}) = \{\sigma_1,\ldots,\sigma_n\}$ and consider the matrix

$$M(\alpha_1,\ldots,\alpha_n) = \begin{bmatrix} \sigma_1\alpha_1 & \sigma_2\alpha_1 & \cdots & \sigma_n\alpha_1 \\ \sigma_1\alpha_2 & \sigma_2\alpha_2 & \cdots & \sigma_n\alpha_2 \\ \vdots & \vdots & \cdots & \vdots \\ \sigma_1\alpha_n & \sigma_2\alpha_n & \cdots & \sigma_n\alpha_n \end{bmatrix} \tag{7.2.2}$$

If $A = M(\alpha_1,\ldots,\alpha_n)$ and $B = M(\beta_1,\ldots,\beta_n)$ is the corresponding matrix for $\beta_1,\ldots,\beta_k \in E$ then the (i,j)-th entry of AB^T is

$$(AB^T)_{i,j} = \sum_k \sigma_k\alpha_i\sigma_k\beta_j = \sum_k \sigma_k(\alpha_i\beta_j) = \mathrm{Tr}_{E/F}(\alpha_i\beta_j)$$

and so

$$M(\alpha_1,\ldots,\alpha_n)M(\beta_1,\ldots,\beta_n)^T = (\mathrm{Tr}_{E/F}(\alpha_i\beta_j))$$

In particular, if $\beta_i = \alpha_i$ for all i, then

$$M(\alpha_1,\ldots,\alpha_n)M(\alpha_1,\ldots,\alpha_n)^T = (\mathrm{Tr}_{E/F}(\alpha_i\alpha_j))$$

Taking determinants gives the following.

Theorem 7.2.5 Let $F < E$ be finite and let $\alpha_1,\ldots,\alpha_n \in E$. Then

$$\Delta_{E/F}(\alpha_1,\ldots,\alpha_n) = |M(\alpha_1,\ldots,\alpha_n)|^2$$

Thus, $\{\alpha_1,\ldots,\alpha_n\}$ is a basis for E over F if and only if

$$|M(\alpha_1,\ldots,\alpha_n)| \neq 0$$ □

*7.3 Algebraic Independence of Embeddings

Let E and L be fields. Recall that the Dedekind Independence Theorem (Corollary 2.8.7) says that any set $\{\sigma_1,\ldots,\sigma_n\}$ of distinct embeddings of E into L is linearly independent over L. To put this another way, let $\lambda_i \in L$ and consider the polynomial $p(x_1,\ldots,x_n) = \sum \lambda_i x_i$. Then the Dedekind Independence Theorem says that if $p(\sigma_1,\ldots,\sigma_n)$ is the zero map, then $p(x_1,\ldots,x_n)$ must be the zero polynomial. Under certain circumstances, we can strengthen this result considerably.

If $\sigma_1,\ldots,\sigma_n$ are embeddings of E into L and if $p(x_1,\ldots,x_n)$ is a polynomial with coefficients in L then $p(\sigma_1,\ldots,\sigma_n)$ is a function from E into L, defined by

$$p(\sigma_1,\ldots,\sigma_n)\alpha = p(\sigma_1\alpha,\ldots,\sigma_n\alpha)$$

Note that we are dealing here with the product of maps, and not the composition. Thus, for instance, if $n = 1$ and $p(x) = x^2$, we have

$$p(\sigma)\alpha = p(\sigma\alpha) = (\sigma\alpha)^2$$

and *not* $p(\sigma)\alpha = \sigma^2\alpha = \sigma(\sigma\alpha)$.

Definition Let $F < E$. A set of distinct F-embeddings $\{\sigma_1,\ldots,\sigma_n\}$ of E into a field L is **algebraically independent** over L if the only polynomial $p(x_1,\ldots,x_n) \in L[x_1,\ldots,x_n]$ for which $p(\sigma_1,\ldots,\sigma_n)$ is the zero function is the zero polynomial. □

Theorem 7.3.1 Let F be an infinite field, let $F < E$ be finite and separable of degree n. Then any set $\{\sigma_1,\ldots,\sigma_n\}$ of distinct F-embeddings of E into any field L is algebraically independent over L.

Proof. Suppose that $p(x_1,\ldots,x_n)$ is a polynomial over L for which $p(\sigma_1,\ldots,\sigma_n)\alpha = 0$ for all $\alpha \in E$. Let $\{\alpha_i\}$ be a basis for E over F. Then for all $a_i \in F$, we have

$$p(\sigma_1 \sum_i a_i\alpha_i,\ldots,\sigma_n \sum_i a_i\alpha_i) = p(\sum_i a_i\sigma_1\alpha_i,\ldots,\sum_i a_i\sigma_n\alpha_i) = 0$$

This implies that the polynomial

$$q(x_1,\ldots,x_n) = p(\sum_i x_i\sigma_1\alpha_i,\ldots,\sum_i x_i\sigma_n\alpha_i)$$

over L satisfies $q(a_1,\ldots,a_n) = 0$ for all $a_i \in F$. It follows from Theorem 1.3.4 that $q(x_1,\ldots,x_n) = 0$, that is,

$$p(\sum x_i\sigma_1\alpha_i,\ldots,\sum x_i\sigma_n\alpha_i) = 0$$

Now, the matrix $M(\alpha_1,\ldots,\alpha_n) = (\sigma_i\alpha_j)$ is nonsingular by Theorem 7.2.5 and so for any $\beta_1,\ldots,\beta_n \in L$, there exists $x_1,\ldots,x_n \in E$ such that

$$\beta_1 = \sum x_i\sigma_1\alpha_i\ ,\ldots,\ \beta_n = \sum x_i\sigma_n\alpha_i$$

Hence $p(\beta_1,\ldots,\beta_n) = 0$ for all $\beta_i \in L$, implying that $p(x_1,\ldots,x_n) = 0$. ∎

*7.4 The Normal Basis Theorem

Let $F < E$ be a finite Galois extension of degree n. Since $F < E$ is finite and separable, there exists a $\lambda \in E$ such that $E = F(\lambda)$. As we know, the set $\{1,\lambda,\ldots,\lambda^{n-1}\}$ is a basis for E over F. This type of basis is called a **polynomial basis.** If $G_F(E) = \{\sigma_1,\ldots,\sigma_n\}$ then the elements $\sigma_1\lambda,\ldots,\sigma_n\lambda$ are precisely the roots of $min(\lambda,F)$ and so they are distinct. If they are linearly independent, then they also form a basis for E over F, called a **normal basis.** Put succinctly, a normal basis is a basis for E

over F consisting of the roots of some minimal polynomial $min(\lambda,F)$, for $\lambda \in E$.

We wish to show that any finite Galois extension has a normal basis. Theorem 7.2.5 can be reworded for finite Galois extensions as follows.

Theorem 7.4.1 If $F < E$ is finite and Galois, with $G_F(E) = \{\sigma_1,\ldots,\sigma_n\}$ then $\{\lambda_1,\ldots,\lambda_n\}$ is a basis for E over F if and only if $\det(\sigma_i\lambda_j) \neq 0$.

Proof. We give a proof that does not use the notions of Section 7.2. Let $\sigma = \sum \beta_i\sigma_i$ for $\beta_i \in E$. Since distinct F-automorphisms of E are linearly independent over E, it follows that $\sigma = 0$ if and only if $\beta_i = 0$ for all i. Now suppose that $B = \{\lambda_1,\ldots,\lambda_n\}$ is a basis for E over F. Then $\sigma = 0$ if and only if $\sigma\lambda_j = 0$ for all j, that is, if and only if $\sum_i \beta_i\sigma_i\lambda_j = 0$, for all $j = 1,\ldots,n$. It follows that $\sum_i \beta_i\sigma_i\lambda_j = 0$ for all $j = 1,\ldots,n$ if and only if $\beta_i = 0$ for all $i = 1,\ldots,n$. Hence, $\det(\sigma_i\lambda_j) \neq 0$.

Conversely, suppose that $\det(\sigma_i\lambda_j) \neq 0$ and let $\sum_j \beta_j\lambda_j = 0$. Then

$$0 = \sigma_i 0 = \sum_j \beta_j\sigma_i\lambda_j$$

for all $i = 1,\ldots,n$. It follows that $\beta_j = 0$ for all $j = 1,\ldots,n$ and so $\{\lambda_i\}$ is a basis for E over F. ∎

Theorem 7.4.1 implies that $\{\sigma_j\lambda\}$ is a (normal) basis for E over F if and only if $\det(\sigma_i\sigma_j\lambda) \neq 0$. Our goal is to find such an element $\lambda \in E$, when $F < E$ is finite and Galois.

Consider the matrix

$$M = \begin{bmatrix} \sigma_1\sigma_1 & \sigma_1\sigma_2 & \cdots & \sigma_1\sigma_n \\ \sigma_2\sigma_1 & \sigma_2\sigma_2 & \cdots & \sigma_2\sigma_n \\ \vdots & \vdots & \cdots & \vdots \\ \sigma_n\sigma_1 & \sigma_n\sigma_2 & \cdots & \sigma_n\sigma_n \end{bmatrix}$$

For each i, the product $\sigma_i\sigma_j$ runs through $\sigma_1,\ldots,\sigma_n$ as j runs through $1,\ldots,n$, and so each row of M is a distinct permutation of $\sigma_1,\ldots,\sigma_n$. The same applies to the columns of M. Thus, we may write

$$M = \begin{bmatrix} \sigma_{1_1} & \sigma_{1_2} & \cdots & \sigma_{1_n} \\ \sigma_{2_1} & \sigma_{2_2} & \cdots & \sigma_{2_n} \\ \vdots & \vdots & \cdots & \vdots \\ \sigma_{n_1} & \sigma_{n_2} & \cdots & \sigma_{n_n} \end{bmatrix}$$

where $(1_i,2_i,\ldots,n_i)$ is a distinct permutation of $\{1,\ldots,n\}$, for $i = 1,\ldots,n$ and $(j_1,j_2,\ldots,j_n)$ is a distinct permutation of $\{1,\ldots,n\}$, for $j = 1,\ldots,n$. Replacing each σ_i by an independent variable x_i gives the matrix

$$N(x_1,\ldots,x_n) = \begin{bmatrix} x_{1_1} & x_{1_2} & \cdots & x_{1_n} \\ x_{2_1} & x_{2_2} & \cdots & x_{2_n} \\ \vdots & \vdots & \cdots & \vdots \\ x_{n_1} & x_{n_2} & \cdots & x_{n_n} \end{bmatrix}$$

We claim that the polynomial $p(x_1,\ldots,x_n) = \det(N(x_1,\ldots,x_n))$ is nonzero. Each row of N is a distinct permutation of the variables $x_1,\ldots,x_n$ and similarly for each column. Thus $N(1,0,\ldots,0)$ is a *permutation matrix*, that is, each row and each column of N contains one 1 and the rest 0's. Since permutation matrices are nonsingular

$$p(1,0,\ldots,0) = \det(N(1,0,\ldots,0)) \neq 0$$

Hence, $p(x_1,\ldots,x_n) \neq 0$.

If F is an infinite field, Theorem 7.3.1 implies that the distinct embeddings $\sigma_1,\ldots,\sigma_n$ of E into L are algebraically independent over L and so there exists a $\lambda \in L$ for which

$$\det(\sigma_i\sigma_j\lambda) = (\det M)(\lambda) = p(\sigma_1,\ldots,\sigma_n)\lambda \neq 0$$

Thus, we have proven the following.

Theorem 7.4.2 If F is an infinite field then any finite Galois extension $F < E$ has a normal basis. □

This result holds for finite fields as well and the proof will be given in Chapter 8.

Exercises

1. Let $F < E$ be finite. For all $\alpha, \beta \in E$,

$$Tr_{E/F}(\alpha+\beta) = Tr_{E/F}(\alpha)+Tr_{E/F}(\beta),\ N_{E/F}(\alpha\beta) = N_{E/F}(\alpha)N_{E/F}(\beta)$$

2. Let $F < E$ be finite. If $\alpha \in F$ then $Tr_{E/F}(\alpha) = [E:F]\alpha$ and $N_{E/F}(\alpha) = \alpha^{[E:F]}$.

3. If $F < E < L$ are finite and if $\alpha \in L$ then

$$Tr_{L/F}(\alpha) = Tr_{E/F}(Tr_{L/E}(\alpha)), \quad N_{L/F}(\alpha) = N_{E/F}(N_{L/E}(\alpha))$$

4. Let $F < E$ be finite and let $\sigma \in Hom_F(E,L)$. If $\alpha \in E$ then $N_{\sigma E/\sigma F}(\sigma\alpha) = \sigma(N_{E/F}(\alpha))$. State and prove a similar statement for the trace.
5. Find a normal basis for the splitting field of $p(x) = x^4 - 5x^2 + 6$ over $\mathbb{Q}$.
6. If F is a finite field of characteristic 2 show that every element of F has a square root in F.
7. If F is a finite field of characteristic $p \neq 2$ then exactly half the nonzero elements of F have square roots in F and that if $\alpha \in F$ has a square root in F then the set of all squares in F is $\{\beta^2\alpha \mid \beta \in F\}$.
8. Let $F < E$ be a finite separable extension, with $E = F(\alpha)$. Let $p(x) = min(\alpha,F)$ have degree n. Show that the discriminant $\Delta_{E/F}(1,\alpha,\ldots,\alpha^{n-1})$ is given by $(-1)^{n(n-1)/2}N_{E/F}(p'(\alpha))$.
9. Let $F < E$ be finite and separable with form (7.2.1) and let $\{\alpha_i\}$ be a basis for E over F. The **dual basis** $\{\beta_i\}$ to $\{\alpha_i\}$ is a basis with the property that

$$Tr_{E/F}(\alpha_i\beta_j) = \langle\alpha_i,\beta_j\rangle = \delta_{i,j}$$

where $\delta_{i,j} = 1$ if $i = j$ and 0 otherwise. In matrix terms, $\{\alpha_i\}$ and $\{\beta_i\}$ are dual bases if

$$M(\alpha_1,\ldots,\alpha_n)M(\beta_1,\ldots,\beta_n)^T = I$$

where M is defined by (7.2.2). A basis for E over F is called a **polynomial basis** if it has the form $\{1, \alpha,\ldots,\alpha^{n-1}\}$ for some $\alpha \in E$. Any simple algebraic extension $E = F(\alpha)$ has a polynomial basis. Let $F < E$ be finite and separable, with polynomial basis $\{1,\alpha,\ldots,\alpha^{n-1}\}$. Let

$$p(x) = min(\alpha,F) = (x - \alpha)(a_0 + a_1x + \cdots + a_{n-1}x^{n-1})$$

Prove that the dual basis for $\{1,\alpha,\ldots,\alpha^{n-1}\}$ is

$$\left\{\frac{a_0}{p'(\alpha)}, \frac{a_1}{p'(\alpha)}, \cdots, \frac{a_{n-1}}{p'(\alpha)}\right\}$$

10. If V is a vector space, let V^* denote the algebraic dual space of all linear functionals on V. Note that if *dim* V is finite then *dim* V = *dim* V^*.
    a) Prove the *Riesz Representation Theorem* for nonsingular metric vector spaces: Let V be a finite dimensional nonsingular metric vector space over F and let $f \in V^*$ be a linear functional on V. Then there exists a unique vector $x \in$

V such that $fx = \langle y,x \rangle$ for all $y \in V$. *Hint*: Let $\psi_x: V \to F$ be defined by $\psi_x(y) = \langle y,x \rangle$. Define a map $\tau: V \to V^*$ by $\tau x = \psi_x$. Show that τ is an isomorphism.

b) Let $F < E$ be finite and separable, with form (7.2.1). Prove that, for any linear functional $\tau: E \to F$ there exists a unique $\alpha \in E$ for which $\tau\beta = \mathrm{Tr}_{E/F}(\alpha\beta)$ for all $\beta \in E$.

Chapter 8
Finite Fields I: Basic Properties

In this chapter and the next, we study finite fields, which play an important role in the applications of field theory, especially to coding theory, cryptology and combinatorics. For a thorough treatment of finite fields, the reader should consult the book *Introduction to Finite Fields and Their Applications*, by Lidl and Niederreiter, Cambridge University Press, 1986.

8.1 Finite Fields

If F is a field, then F^* will denote the multiplicative group of all nonzero elements of F. Let us recall some facts about finite fields that have already been established.

Theorem 8.1.1 Let F be a finite field.

1) F has prime characteristic. (Theorem 0.3.2)
2) F^* is cyclic. (Corollary 1.3.5)
3) Any finite extension of F is simple. (Corollary 4.4.5)
4) F is perfect, and so every algebraic extension of F is separable. (Theorem 4.8.2) □

Lemma 8.1.2 If F is a finite field and $[E:F] = d$ then $|E| = |F|^d$.

Proof. If $\{\alpha_1, \ldots, \alpha_d\}$ is a basis for E over F, then each element of E has a *unique* representation of the form $a_1\alpha_1 + \cdots + a_d\alpha_d$, where $a_i \in F$. Since there are $|F|$ possibilities for each coefficient a_i, we deduce that $|E| = |F|^d$. ∎

Since a finite field F has prime characteristic p, we have $\mathbb{Z}_p < F$ and so Lemma 8.1.2 gives

Corollary 8.1.3 If F is a finite field with $\text{char}(F) = p$, then F has p^n elements for some positive integer n. □

From now on, unless otherwise stated, p will represent a prime number, and q will represent a power of p.

8.2 Finite Fields as Splitting Fields

We have seen that every finite field of characteristic p has p^n elements for some $n > 0$. Let us now show that there is, up to isomorphism, exactly one field of size p^n, for each prime p and each integer $n > 0$.

Let $q = p^n$ and let S be the splitting field for the polynomial

$$f_q(x) = x^q - x$$

over $\mathbb{Z}_p$. If R is the set of roots of $f_q(x)$ in S, then $\alpha, \beta \in R$ imply that $\alpha^q = \alpha$ and $\beta^q = \beta$, whence

$$(\alpha \pm \beta)^q = \alpha^q \pm \beta^q = \alpha \pm \beta \quad \text{and} \quad (\alpha\beta^{-1})^q = \alpha^q(\beta^q)^{-1} = \alpha\beta^{-1}$$

Hence $\alpha \pm \beta \in R$ and $\alpha\beta^{-1} \in R$. It follows that R is a field and $R = S$. Furthermore, since

$$f_q'(x) = qx^{q-1} - 1 = -1$$

the polynomial $f_q(x)$ has no multiple roots in S and so $|S| = q$. Thus, there exists a finite field S of size $q = p^n$ for every prime p and every positive integer n. It is customary to denote such a field by F_q, or $GF(q)$. (The symbol *GF* stands for *Galois Field*, in honor of Evariste Galois.)

To establish uniqueness, observe that if F is a field of size $q = p^n$, then F^* is a multiplicative group of order $q - 1$ and so every $\alpha \in F^*$ satisfies $\alpha^{q-1} = 1$. Thus, every $\alpha \in F$ is a root of the polynomial $f_q(x) = x^q - x$. Since this polynomial has exactly q roots, F is the set of roots of $f_q(x)$ and is therefore the splitting field for $f_q(x)$ over $\mathbb{Z}_p$. Since any two splitting fields for $f_q(x)$ are isomorphic, we conclude that any two finite fields of size q are isomorphic.

Theorem 8.2.1

1) Every finite field has size $q = p^n$, for some prime p and integer $n > 0$.
2) For every $q = p^n$ there is, up to isomorphism, a unique field $GF(q)$ of size q, which is both the set of roots of $f_q(x) = x^q - x$ and the splitting field for $f_q(x)$ over $\mathbb{Z}_p$. □

In view of this theorem, we will often refer to *the* finite field $GF(q)$.

Corollary 8.2.2 The extension $GF(q) < GF(q^n)$ is a Galois extension. □

8.3 The Subfields of a Finite Field

It is easy to determine the subfields of a finite field. If $F < GF(p^n)$ then Lemma 8.1.2 implies that $|F| = p^d$ for some $d \mid n$. On the other hand, we have

$$d \mid n \Rightarrow p^d - 1 \mid p^n - 1 \Rightarrow x^{p^d-1} - 1 \mid x^{p^n-1} - 1 \Rightarrow f_{p^d}(x) \mid f_{p^n}(x)$$

and since $f_{p^n}(x)$ splits over $GF(p^n)$, so does $f_{p^d}(x)$. Thus $GF(p^n)$ contains a splitting field for $f_{p^d}(x)$, that is, $GF(p^n)$ contains a subfield of size p^d. Certainly, $GF(p^n)$ cannot contain more than one such subfield, for then there would be more than p^d roots of the polynomial $f_{p^d}(x)$ in $GF(p^n)$.

Theorem 8.3.1 The field $GF(p^n)$ has exactly one subfield of size p^d, for each $d \mid n$. This accounts for all of the subfields of $GF(p^n)$. □

8.4 The Multiplicative Structure of a Finite Field

Since $GF(q)^*$ is cyclic, Theorem 0.2.11 implies the following theorem.

Theorem 8.4.1 There are exactly $\phi(d)$ elements of $GF(q)^*$ of order d for each $d \mid q - 1$ and this accounts for all of the elements of $GF(q)^*$. □

It is customary to refer to any element of $GF(q)$ that generates the cyclic group $GF(q)^*$ as a *primitive element* of $GF(q)$. However, this brings us into conflict with the term primitive as used earlier to denote any element of a field that generates the field using *both* field operations (addition and multiplication). Accordingly, we adopt the following definition.

Definition Any element of $GF(q)$ that generates the cyclic group $GF(q)^*$ is called a **group primitive element** of $GF(q)$. In contrast, if $F < E$ then any element $\alpha \in E$ for which $E = F(\alpha)$ is called a **field primitive element** of E over F. □

If $\beta \in GF(q)$, we may wish to know when the equation

$$x^k = \beta \tag{8.4.1}$$

has a solution in $GF(q)$, that is, when β has a k-th root in $GF(q)$. This question has a simple answer in view of the fact that $GF(q)^*$ is cyclic. If α is a group primitive element of $GF(q)$ then $\beta = \alpha^i$ for some i and so (8.4.1) has a solution $x = \alpha^j$ if and only if

$$\alpha^{kj} = \alpha^i$$

for some integer j. This is equivalent to

$$kj \equiv i \bmod (q-1)$$

or

$$i = kj + n(q-1)$$

for some integers n and j. But this holds if and only if

$$(k,q-1) \mid i$$

where $(k,q-1)$ is the greatest common divisor of k and $q-1$. Thus, equation (8.4.1) has a solution for all $\beta \in GF(q)$ if and only if $(k,q-1) = 1$.

Theorem 8.4.2

1) Let α be a group primitive element of $GF(q)$. The equation $x^k = \alpha^i$ has a solution in $GF(q)$ if and only if $(k,q-1) \mid i$.
2) The equation $x^k = \beta$ has a solution for all $\beta \in GF(q)$ if and only if $(k,q-1) = 1$, in which case the solution is unique. □

Theorem 8.4.2 says that if $(k,q-1) = 1$, the function $\alpha \mapsto \alpha^k$ is a permutation of the elements of $GF(q)$. For this reason, in this case the polynomial $p(x) = x^k$ is called a **permutation polynomial.**

8.5 The Galois Group of a Finite Field

Since the extension $GF(q) < GF(q^n)$ is Galois, if G is the Galois group of $GF(q^n)$ over $GF(q)$ then

$$|G| = [GF(q^n):GF(q)] = n$$

The structure of G could not be simpler, as we now show.

Theorem 8.5.1 The Galois group G of $GF(q^n)$ over $GF(q)$ is cyclic of order n, generated by the Fröbenius automorphism $\sigma_q:\alpha\mapsto\alpha^q$.

Proof. Since $\alpha^q = \alpha$ for all $\alpha \in GF(q)$, we have $\sigma_q \in G$. Moreover, the n automorphisms

$$\iota, \sigma_q, \sigma_q^2, \ldots, \sigma_q^{n-1}$$

are distinct elements of G, for if $\sigma_q^k = \iota$ then $\alpha^{q^k} = \alpha$ for all $\alpha \in GF(q^n)$, which implies that $k \geq n$. Since $|G| = n$, we see that $G = \langle\sigma_q\rangle$. ∎

8.6 Irreducible Polynomials over Finite Fields

The following theorem gives some key facts about irreducible polynomials over a finite field.

Theorem 8.6.1 For every finite field $GF(q)$, and every positive integer d, there exists an irreducible polynomial p(x) of degree d over $GF(q)$. Let α be a root of p(x) in some extension field.

1) (**Splitting Field**) The splitting field of p(x) is $GF(q)(\alpha) = GF(q^d)$.

2) (**Roots**) The roots of p(x) in a splitting field are

$$\alpha, \alpha^q, \alpha^{q^2}, \ldots, \alpha^{q^{d-1}} \tag{8.6.1}$$

3) (**Degree**) d is the smallest positive integer for which $\alpha^{q^d} = \alpha$.

4) (**Degree**) $p(x) \mid x^{q^k} - x$ if and only if $d \mid k$. Hence, d is the smallest positive integer for which $p(x) \mid x^{q^d} - x$.

5) (**Order of Roots**) All roots of p(x) have the same multiplicative order in $GF(q^d)^*$.

Proof. Note first that since $GF(q) < GF(q^d)$ is simple, we have $GF(q^d) = GF(q)(\beta)$ and so $min(\beta, GF(q))$ is an irreducible polynomial of degree d over $GF(q)$. For part 1), since $GF(q) < GF(q)(\alpha)$ is normal, p(x) splits in $GF(q)(\alpha)$, whence it is the splitting field for p(x). Also,

$$[GF(q)(\alpha):GF(q)] = deg\ p(x) = d$$

and so $GF(q)(\alpha) = GF(q^d)$.

To prove part 2), recall that the Galois group of $GF(q^d)$ over $GF(q)$ is the cyclic group

$$\langle \sigma_q \rangle = \{\iota, \sigma_q, \sigma_q^2, \ldots, \sigma_q^{d-1}\}$$

Applying these maps to α gives the complete list (8.6.1) of roots of $p(x)$, with no duplicates since any automorphism of $GF(q^d)$ over $GF(q)$ is completely determined by its value on α.

For part 3), since $\alpha \in GF(q^d)$ we have $\alpha^{q^d} = \alpha$ and it is clear from part 2) that no smaller power of q can have this property. Part 4) follows from the fact that $p(x) \mid x^{q^k} - x$ if and only if the splitting field for $p(x)$ is a subfield of the splitting field for $x^{q^k} - x$, that is, if and only if $GF(q^d) < GF(q^k)$. Part 5) follows from the fact that since σ_q is an automorphism of $GF(q^d)$, it preserves multiplicative order and so the order of $\sigma_q^k \alpha$ is equal to the order of α. ∎

Definition If $p(x)$ is irreducible over $GF(q)$ then the multiplicative order of any root of $p(x)$ in its splitting field is called the **order** of $p(x)$ and is denoted by $o(p(x))$ or $o(p)$. □

Definition A polynomial $p(x)$ over $GF(q)$ of degree d is said to be **primitive** over $GF(q)$ if it is the minimal polynomial of a group primitive element of $GF(q^d)$, that is, if its order is $q^d - 1$. □

According to part 5) of Theorem 8.6.1, an irreducible polynomial over $GF(q)$ of degree d is primitive if and only if *all* of its roots are group primitive in $GF(q^d)$. Primitive polynomials play an important role in finite field arithmetic, as we shall see in the next chapter.

The following theorem provides a characterization of order. (*cf.* Theorem 8.6.1, part 4).)

Theorem 8.6.2 Let $p(x) \in GF(q)$ be irreducible of order ν. Then $p(x) \mid x^k - 1$ if and only if $\nu \mid k$. Hence, ν is the smallest positive integer for which $p(x) \mid x^\nu - 1$.

Proof. Suppose first that $\nu \mid k$. Each root α of $p(x)$ satisfies $\alpha^\nu - 1 = 0$ and therefore also $\alpha^k - 1$. Since $p(x)$ is separable, we conclude that $p(x) \mid x^k - 1$. Conversely, if $p(x) \mid x^k - 1$ then any root of $p(x)$ is a root of $x^k - 1$ and therefore has order dividing k, whence $\nu \mid k$. ∎

Relationship Between Order and Degree

There is a simple relationship between the order and degree of an irreducible polynomial p(x) over $GF(q)$. Let $o(p(x)) = \nu$ and $deg\ p(x) = d$ and suppose that $\alpha \in GF(q^d)$ is a root of p(x). Since

$$\alpha^{q^k} = \alpha \text{ if and only if } \nu \mid q^k - 1$$

and since d is the smallest positive integer for which $\alpha^{q^d} = \alpha$, we conclude that d is the smallest positive integer for which $\nu \mid q^d - 1$. Put another way, $d = deg\ p(x)$ is the order of q modulo ν, written $o_\nu(q)$. Since $(\nu,q) = 1$, the residue $\bar{q}$ of q modulo ν lies in $\mathbb{Z}_\nu^*$, the multiplicative group of elements of $\mathbb{Z}_\nu$ that are relatively prime to ν and so $deg\ p(x) = o(\bar{q})$ in the group $\mathbb{Z}_\nu^*$.

By way of converse, suppose that f(x) is a polynomial over $GF(q)$ and α is a root of order ν in a splitting field. If $deg\ f(x) = o_\nu(q)$ then f(x) must be irreducible, since it has the same degree as $p(x) = min(\alpha, GF(q))$ and is divisible by p(x).

Theorem 8.6.3 Let p(x) be a polynomial over $GF(q)$ of degree d, let α be a root of p(x) of order ν in a splitting field. Then p(x) is irreducible if and only if any of the following equivalent conditions holds.

1) d is the smallest positive integer for which $\nu \mid q^d - 1$.

2) d is the smallest positive integer for which $\alpha^{q^d} = \alpha$.

3) $d = o_\nu(q)$ is the order of q modulo ν. □

Theorem 8.6.3 tells us that the degree of an irreducible polynomial is completely determined by its order. It is not true that the order of an irreducible polynomial is determined by its degree, as we will see in a moment.

If $p(x) \in GF(q)$ is irreducible and has degree d, then $GF(q^d)$ is the splitting field for p(x). Of course, we may view p(x) as a polynomial over any intermediate field $GF(q^k)$ where $1 < k < d$, in which case it may no longer be irreducible. Let α be a root of p(x) of order ν in $GF(q^d)$, and suppose that α is a root of the irreducible factor q(x) of p(x) over $GF(q^k)$. Since q^k has order $\delta = d/(k,d)$ in $\mathbb{Z}_\nu^*$, we deduce from Theorem 8.6.3 that $deg\ q(x) = \delta$.

Theorem 8.6.4 Let p(x) be irreducible of degree d over $GF(q)$. When thought of as a polynomial over $GF(q^k)$, where $1 \leq k \leq d$, the polynomial p(x) can be factored into (k,d) irreducible factors, each of which has degree d/(k,d). In particular, p(x) is irreducible over $GF(q^k)$ if and only if (k,d) = 1. □

Computing the Order of a Polynomial

We now present a procedure for finding the order ν of an irreducible polynomial f(x) of degree d. Let p be a prime dividing $q^d - 1$ and suppose that $q^d - 1 = p^t u$ with $p \nmid u$ and $\nu = p^s v$ with $p \nmid v$. Since $\nu \mid q^d - 1$ we have $s \leq t$ and $p^w \nu \mid q^d - 1$ if and only if $w \leq t - s$. Hence, the largest w for which $p^w \nu \mid q^d - 1$ satisfies $w = t - s$, that is, $s = t - w$. Thus, the largest value of w for which

$$\nu \left| \frac{q^d - 1}{p^w} \right.$$

or equivalently by Theorem 8.6.2,

$$f(x) \left| x^{(q^d-1)/p^w} - 1 \right.$$

gives the largest power p^{t-w} of p dividing ν. Doing this for all primes dividing $q^d - 1$ gives the value of ν.

Example 8.6.1 Consider the irreducible polynomial $f(x) = x^6 + x + 1$ over $GF(2)$. Since $q = 2$, we have

$$q^6 - 1 = 63 = 3^2 \cdot 7$$

Let $p = 3$. Division shows that

$$f(x) \nmid x^{63/9} - 1, \quad f(x) \nmid x^{63/3} - 1, \quad f(x) \mid x^{63} - 1$$

and so $w = 0$, $s = t - w = 2 - 0 = 2$, whence 3^2 is the largest power of 3 dividing ν. For $p = 7$ division gives

$$f(x) \nmid x^{63/7} - 1, \quad f(x) \mid x^{63} - 1$$

and so 7 is the largest power of 7 dividing ν. Thus $\nu = 3^2 \cdot 7 = 63$ showing that f(x) is primitive over $GF(2)$.

The polynomial $g(x) = x^6 + x^4 + x^2 + x + 1$ is also irreducible over $GF(2)$. In this case for $p = 3$ we have

$$g(x) \nmid x^{63/9} - 1, \quad f(x) \mid x^{63/3} - 1$$

and so $w = 1$, whence $3 \mid \nu$ but $3^2 \nmid \nu$. For $p = 7$ we have

$$f(x) \nmid x^{63/7} - 1, \quad f(x) \mid x^{63} - 1$$

hence $7 \mid \nu$ and $\nu = 21$. Note that both of these polynomials have degree

6 but they have different orders. This shows that the degree of an irreducible polynomial does not determine its order. □

*8.7 Normal Bases

We saw in Chapter 7 that if $F < E$ is a finite Galois extension and F is an infinite field, then E has a normal basis over F. To prove an analogous theorem when E is a finite field, we require a result from linear algebra, which we will not prove here. If $T:V \to V$ is a linear operator on an n-dimensional vector space V over a field F, then the *minimal polynomial* $m_T(x)$ for T is the unique monic polynomial over F of smallest degree for which $m_T(T) = 0$. Since T satisfies its *characteristic polynomial* $c_T(x) = \det(xI - \mathrm{Mat}(T))$, we have $m_T(x) \mid c_T(x)$. A vector $v \in V$ is said to be **cyclic** for T if the vectors

$$\{v, Tv, T^2v, \ldots, T^{n-1}v\}$$

form a basis for V. Here is the result that we need.

Theorem 8.7.1 Let $T:V \to V$ be a linear operator on a finite-dimensional vector space V over a field F. Then V contains a cyclic vector for T if and only if the minimal polynomial $m_T(x)$ and the characteristic polynomial $c_T(x)$ are the same. □

Now we can establish the existence of normal bases for finite fields.

Theorem 8.7.2 There exists a normal basis $\{\alpha, \alpha^q, \ldots, \alpha^{q^{n-1}}\}$ for $GF(q^n)$ over $GF(q)$.

Proof. If $n = 1$, there is nothing to prove, so assume that $n > 1$. The Galois group of $GF(q^n)$ over $GF(q)$ is

$$G = \{\iota, \sigma_q, \sigma_q^2, \ldots, \sigma_q^{n-1}\}$$

where $\sigma_q: \alpha \to \alpha^q$. By the Dedekind Independence Theorem, these maps are linearly independent over $GF(q^n)$. Thus, thinking of σ_q as a linear operator on the n-dimensional vector space $GF(q^n)$ over $GF(q)$, we see that σ_q satisfies the polynomial $x^n - 1$ and no polynomial over $GF(q)$ of smaller degree. Hence $x^n - 1$ is the minimal polynomial of σ_q over $GF(q)$. On the other hand, the characteristic polynomial of σ_q has degree n, is monic, and is divisible by $x^n - 1$, and so it must also be $x^n - 1$. By the previous theorem, there exists a cyclic vector α for σ_q and so

$$\alpha, \sigma_q\alpha, \ldots, \sigma_q^{n-1}\alpha$$

is a normal basis for $GF(q^n)$ over $GF(q)$. ∎

*8.8 The Algebraic Closure of a Finite Field

In this section, we determine the algebraic closure of a finite field $GF(q)$. Since $GF(q) < GF(q^n)$ is algebraic for all positive integers n, an algebraic closure of $GF(q)$ must contain all of the fields $GF(q^n)$. Since $n! \mid (n+1)!$, it follows that

$$GF(q^{n!}) < GF(q^{(n+1)!})$$

and so the union

$$\Gamma(q) = \bigcup_{n=0}^{\infty} GF(q^{n!})$$

is an extension field of $GF(q)$ that contains $GF(q^n)$, for all $n \geq 1$.

Theorem 8.8.1 The field $\Gamma(q)$ is the algebraic closure of $GF(q)$.

Proof. Every element of $\Gamma(q)$ lies in some $GF(q^{n!})$, whence it is algebraic over $GF(q)$. Thus $\Gamma(q)$ is algebraic over $GF(q)$. Now suppose that $\Gamma(q) < E$ is algebraic and let $\alpha \in E$ have minimal polynomial $p(x)$ over $GF(q)$. If $deg\ p(x) = d$, then $p(x)$ splits in $GF(q^d)$, which is contained in $\Gamma(q)$. Hence $\alpha \in \Gamma(q)$ and so $E < \Gamma(q)$. Thus, $\Gamma(q)$ has no proper algebraic extensions. ∎

Steinitz Numbers

We wish now to describe the subfields of the algebraic closure $\Gamma(q)$. Recall that a field K is a subfield of $GF(q^n)$ if and only if $K = GF(q^d)$ where $d \mid n$. The set $\mathbb{N}^+$ of positive integers is a complete lattice where $m \wedge n = \gcd(m,n)$ and $m \vee n = \text{lcm}(m,n)$. If we denote by $\mathfrak{F}_q$ the set of all finite fields (or more properly the set of all isomorphism classes of finite fields) that contain $GF(q)$, then $\mathfrak{F}_q$ is also a complete lattice where $E \wedge F = E \cap F$ and $E \vee F = EF$.

Theorem 8.8.2 The map $\psi: \mathbb{N}^+ \to \mathfrak{F}_q$ defined by $\psi(n) = GF(q^n)$ is an order-preserving bijection. Hence, it is an isomorphism of lattices, that is,

1) $n \mid m$ if and only if $GF(q^n) < GF(q^m)$,

2) $GF(q^n) \cap GF(q^m) = GF(q^{n \wedge m})$,

3) $GF(q^n)GF(q^m) = GF(q^{n \vee m})$.

Proof. Left to the reader. ∎

It is clear that the lattice of intermediate fields between $GF(q)$ and $GF(q^n)$ is isomorphic to the sublattice of $\mathbb{N}^+$ consisting of all positive integers dividing n. In order to describe the lattice of intermediate fields between $GF(q)$ and $\Gamma(q)$, we make the following definition.

Definition A **Steinitz number** is an expression of the form

$$S = \prod_{i=1}^{\infty} p_i^{e_i}$$

where p_i is the i-th prime and $e_i \in \{0,1,2,\dots\} \cup \{\infty\}$. We denote the set of all Steinitz numbers by **S**. Two Steinitz numbers are equal if and only if the exponents of corresponding prime numbers p_i are equal. □

We will denote arbitrary Steinitz numbers using upper case letters and reserve lower case letters strictly for ordinary positive integers. We will take certain obvious liberties when writing Steinitz numbers, such as omitting factors with a 0 exponent. Thus, any positive integer is a Steinitz number. We next define the algebra of Steinitz numbers.

Definition Let $S = \prod p_i^{e_i}$ and $T = \prod p_i^{f_i}$ be Steinitz numbers.

1) The **product** and **quotient** of S and T are defined by

$$ST = \prod_{i=1}^{\infty} p_i^{e_i+f_i} \quad \text{and} \quad S/T = \prod_{i=1}^{\infty} p_i^{e_i-f_i}$$

where $\infty - \infty = 0$.

2) We say that S **divides** T and write $S \mid T$ if $e_i \leq f_i$ for all i. □

Theorem 8.8.3 Under the relation of "divides" given in the previous definition, the set **S** is a complete distributive lattice, with meet and join given by

$$S \wedge T = \prod_{i=1}^{\infty} p_i^{\min(e_i,f_i)} \quad \text{and} \quad S \vee T = \prod_{i=1}^{\infty} p_i^{\max(e_i,f_i)}$$

Moreover, the set of positive integers is a sublattice of **S**. □

Subfields of the Algebraic Closure

We can now describe the subfields of $\Gamma(q)$. Let $\mathfrak{P}(\Gamma(q))$ denote the lattice of all subfields of $\Gamma(q)$ that contain $GF(q)$.

Definition If S is a Steinitz number, let

$$GF(q^S) = \bigcup_{d \mid S} GF(q^d)$$

where, as indicated by the notation, d is an ordinary positive integer. □

If $\alpha, \beta \in GF(q^S)$ then $\alpha \in GF(q^k)$ for some $k \mid S$ and $\beta \in GF(q^n)$ for some $n \mid S$. Thus $\alpha, \beta \in GF(q^m)$ where $m = \text{lcm}(k,n)$. It follows that $GF(q^S)$ is a subfield of $\Gamma(q)$ containing $GF(q)$.

Theorem 8.8.4 The map $\psi: \mathbf{S} \to \mathfrak{I}(\Gamma(q))$ defined by $\psi(S) = GF(q^S)$ is an order preserving bijection. Hence, it is an isomorphism of lattices, that is,

1) $S \mid T$ if and only if $GF(q^S) < GF(q^T)$,

2) $GF(q^S) \cap GF(q^T) = GF(q^{S \wedge T})$,

3) $GF(q^S)GF(q^T) = GF(q^{S \vee T})$.

In addition, $GF(q^S)$ is finite if and only if S is a positive integer.

Proof. We begin by showing that $n \mid S$ if and only if $GF(q^n) < GF(q^S)$. One direction follows immediately from the definition: if $n \mid S$ then $GF(q^n) < GF(q^S)$. Suppose that $GF(q^n) < GF(q^S)$. Let α be a field primitive element of $GF(q^n)$ over $GF(q)$. Then $\alpha \in GF(q^S)$ and so $\alpha \in GF(q^d)$ for some $d \mid S$. Hence $GF(q^n) = GF(q)(\alpha) < GF(q^d)$, which implies that $n \mid d$, whence $n \mid S$.

To see that ψ is injective, suppose that $S \neq T$. We may assume that there exists an integer $n > 1$ such that $n \mid S$ but $n \nmid T$. Then $GF(q^n) < GF(q^S)$ but $GF(q^n) \not< GF(q^T)$ and so $GF(q^S) \neq GF(q^T)$.

To see that ψ is surjective, let $GF(q) < F < \Gamma(q)$. We must find an S for which $GF(q^S) = F$. For each prime p_i, let e_i be the largest power of p_i for which

$$GF(q^{p_i^{e_i}}) < F \tag{8.8.1}$$

where $e_i = \infty$ if (8.8.1) holds for all positive integers e_i. Let

$$S = \prod_{i=1}^{\infty} p_i^{e_i}$$

If $d \mid S$ then

$$d = \prod_{i=1}^{m} p_i^{f_i}$$

for some $m \in \mathbb{N}^+$, where $f_i \leq e_i$ and $f_i < \infty$. Hence

$$GF(q^{p_i^{f_i}}) < GF(q^{p_i^{e_i}}) < F$$

for $i = 1,\ldots,m$ and so

$$GF(q^d) = \vee\, GF(q^{p_i^{f_i}}) < F$$

It follows that $GF(q^S) < F$. Now, if $\alpha \in F$ then $\alpha \in GF(q^n) < F$ for some n. If

$$n = \prod_{i=1}^{r} p_i^{g_i}$$

then

$$GF(q^{p_i^{g_i}}) < GF(q^n) < F$$

and so $g_i \leq e_i$ for all i, by the maximality of e_i. Hence $n \mid S$ and so $\alpha \in GF(q^n) < GF(q^S)$. This shows that $F < GF(q^S)$. Hence $F = GF(q^S)$ and so ψ is surjective. We leave the rest of the proof to the reader. ∎

Exercises

1. Show that
$$d \mid n \;\Rightarrow\; p^d - 1 \mid p^n - 1 \;\Rightarrow\; f_{p^d}(x) \mid f_{p^n}(x)$$
2. Is $\mathbb{Z}_2 \approx F_2$? Is $\mathbb{Z}_4 \approx F_4$? When is $\mathbb{Z}_{q^n} \approx F_{q^n}$?
3. Determine the number of subfields of F_{1024}. Determine the number of subfields of F_{729}.
4. Show that, except for the case of F_2, the sum of all of the elements in a finite field is equal to 0.
5. Find all group primitive elements of F_7.
6. Show that the polynomial $x^4 + x^3 + x^2 + x + 1$ is irreducible over F_2. Is it primitive?
7. Let F be an arbitrary field. Prove that if F^* is cyclic then F must be a finite field.
8. Consider the irreducible polynomial $p(x) = x^4 - 2$ over $\mathbb{Q}$. Show that adjoining one root of p(x) to $\mathbb{Q}$ does not produce the splitting field for p(x). What is the degree of the splitting field for p(x) over $\mathbb{Q}$?

Find the order of the following irreducible polynomials.

9. $x^4 + x^3 + x^2 + x + 1$ over $GF(2)$.
10. $x^4 + x + 1$ over $GF(2)$.
11. $x^8 + x^4 + x^3 + x^2 + 1$ over $GF(2)$.
12. $x^8 + x^5 + x^4 + x^3 + 1$ over $GF(2)$.
13. $x^8 + x^7 + x^5 + x + 1$ over $GF(2)$.
14. $x^4 + x + 2$ over $GF(3)$.

15. $x^4 + x^3 + x^2 + 1$ over $GF(3)$.
16. $x^5 - x + 1$ over $GF(3)$.
17. Show that every element in $GF(q^n)$ has a unique q^i-th root, for $i = 1, \ldots, n-1$.
18. If $2 \nmid q$, show that exactly one-half of the nonzero elements of $GF(q)$ have square roots. *Hint.* Let β be a primitive element of $GF(q)$. If $\beta = \alpha^2$, then $\alpha^{2k} = \alpha$ for some k.
19. Show that if $\alpha \in GF(q)$ and n is a positive integer, then $x^{q^n} - x + \alpha$ divides $x^{q^n} - x + n\alpha$. *Hint*: show that roots of the former are roots of the latter.
20. Find a normal basis for $GF(8)$ over $GF(2)$. *Hint.* Let α be a root of the irreducible polynomial $x^3 + x^2 + 1$.
21. Show that $\Gamma(q) = \bigcup_{n=0}^{\infty} GF(q^n)$.
22. Show that $\Gamma(q^n) = \Gamma(q^m)$.
23. Let F be a field F satisfying $GF(q) < F < \Gamma(q)$. Show that all of the proper subfields of F are finite if and only if F is finite or $F = GF(q^S)$ where $S = p^\infty$ for some prime p.
24. Show that $\Gamma(q)$ has no maximal subfields.
25. Show that $[\Gamma(q):F]$ is not finite for any proper subfield $F < \Gamma(q)$.
26. Show that $\Gamma(q)$ has an uncountable number of nonisomorphic subfields.
27. Let $S \mid T$. Show that $[GF(q^T):GF(q^S)]$ is finite if and only if T/S is finite, in which case the two numbers are equal. *Hint*: consider the intermediate fields.

Chapter 9
Finite Fields II: Additional Properties

9.1 Finite Field Arithmetic

There are several ways in which to represent the elements of a finite field. One way is to use a factor ring $GF(q)[x]/\langle p(x)\rangle$, where $p(x)$ is irreducible. Another is to use the fact that $GF(q)^*$ is cyclic, and so its elements are all powers of a group primitive element. It is clear that addition is more easily performed when field elements are written as polynomials and multiplication is more easily performed when all elements are written as a power of a single group primitive element. Fortunately, the two methods can be combined to provide an effective means for doing finite field arithmetic.

Example 9.1.1 Consider the finite field $GF(16)$ as an extension of $GF(2)$. The polynomial

$$p(x) = x^4 + x + 1$$

is irreducible over $GF(2)$. To see this, note that if $p(x)$ is reducible, it must have either a linear or a quadratic factor. But since $p(0) \neq 0$ and $p(1) \neq 0$, it has no linear factors. To see that $p(x)$ has no quadratic factors, note that there are precisely four quadratic polynomials over $GF(2)$, namely,

$$x^2,\ x^2 + 1,\ x^2 + 1,\ x^2 + x + 1$$

and it is easy to check that no product of any two of these polynomials equals $p(x)$. Since $deg\ p(x) = 4$, we have

$$\frac{GF(2)[x]}{\langle x^4+x+1\rangle} = GF(16)$$

Thus, letting α be a root of $p(x)$, we can represent the elements of $GF(16)$ as the 16 binary polynomials of degree 3 or less in α:

Constant: $0, 1,$

Linear: $\alpha, \alpha+1$

Quadratic: $\alpha^2, \alpha^2+1, \alpha^2+\alpha, \alpha^2+\alpha+1$

Cubic: $\alpha^3, \alpha^3+1, \alpha^3+\alpha, \alpha^3+\alpha^2, \alpha^3+\alpha+1,$
$\alpha^3+\alpha^2+1, \alpha^3+\alpha^2+\alpha, \alpha^3+\alpha^2+\alpha+1$

Addition of elements of $GF(16)$ is quite simple, since it is just addition of polynomials, but multiplication requires reduction modulo $p(\alpha)$, that is, using the relation $\alpha^4 = \alpha+1$. On the other hand, observe that

$$\begin{aligned}\alpha^{15} &= (\alpha^5)^3 = (\alpha\cdot\alpha^4)^3 = (\alpha\cdot(\alpha+1))^3 = \alpha^3(\alpha+1)^3\\ &= \alpha^3\cdot(\alpha^3+\alpha^2+\alpha+1) = \alpha^6+\alpha^5+\alpha^4+\alpha^3\\ &= (\alpha^3+\alpha^2)+(\alpha^2+\alpha)+(\alpha+1)+\alpha^3\\ &= (\alpha^3+\alpha^2)+(\alpha^2+\alpha)+(\alpha+1)+\alpha^3 = 1\end{aligned}$$

and so $o(\alpha) \mid 15$. Since $\alpha^3 \neq 1$ and $\alpha^5 \neq 1$, we conclude that α is group primitive. Hence

$$GF(16) = \{0,1,\alpha,\ldots,\alpha^{14}\}$$

With this representation, multiplication is all but trivial, but addition is cumbersome.

We can link the two representations of $GF(16)$ by computing a table showing how each element α^k can be represented as a polynomial in α of degree at most 3. Using the fact that $\alpha^4 = 1+\alpha$, we have

$$\begin{aligned}\alpha^4 &= \alpha+1\\ \alpha^5 &= \alpha\cdot\alpha^4 = \alpha(\alpha+1) = \alpha^2+\alpha\\ \alpha^6 &= \alpha\cdot\alpha^5 = \alpha^3+\alpha^2\\ \alpha^7 &= \alpha\cdot\alpha^6 = \alpha^4+\alpha^3 = \alpha^3+\alpha+1\end{aligned}$$

and so on. The complete list, given in Table 9.1.1, is known as a **field table** for $GF(16)$. As is customary, we write only the exponent k for α^k, and $a_3a_2a_1a_0$ for the polynomial $a_3\alpha^3+a_2\alpha^2+a_1\alpha+a_0$.

Table 9.1.1	
0	0001
1	0010
2	0100
3	1000
4	0011
5	0110
6	1100
7	1011
8	0101
9	1010
10	0111
11	1110
12	1111
13	1101
14	1001

Computations using this table are quite straightforward; for example,

$$\begin{aligned}(\alpha^8+\alpha^4+1)(\alpha^3+\alpha) &= (0101+0011+0001)(1000+0010)\\ &= (0111)(1010)\\ &= \alpha^{10}\cdot\alpha^9 = \alpha^{19} = \alpha^4 = \alpha+1\end{aligned}$$

Thus, the key to doing arithmetic in a finite field is having a group primitive element, along with its minimal (primitive) polynomial. In general, the task of finding primitive polynomials is not easy. There are various methods that achieve some measure of success in certain cases, and we mention one such method at the end of Section 11.2. Fortunately, extensive tables of primitive polynomials and field tables have been constructed.

Let us use the primitive polynomial p(x) and the field table for $GF(16)$ (Table 9.1.1) to compute the minimal polynomial over $GF(2)$ for each element of $GF(16)$. We begin by computing sets of conjugates using Theorem 8.6.1 and the fact that $\alpha^{16} = \alpha$,

Conjugates of α: $\alpha, \alpha^2, \alpha^4, \alpha^8$

Conjugates of α^3: $\alpha^3, \alpha^6, \alpha^{12}, \alpha^{24} = \alpha^9$

Conjugates of α^5: α^5, α^{10}

Conjugates of α^7: $\alpha^7, \alpha^{14}, \alpha^{28} = \alpha^{13}, \alpha^{56} = \alpha^{11}$

Letting $m_k(x)$ be the minimal polynomial for α^k, we have, for example

$$m_5(x) = m_{10}(x) = (x - \alpha^5)(x - \alpha^{10}) = x^2 - (\alpha^5 + \alpha^{10})x + \alpha^{15}$$

The field table for $GF(16)$ gives

$$\alpha^5 + \alpha^{10} = (0110) + (0111) = (0001) = \alpha^0 = 1$$

and since $\alpha^{15} = 1$, we have

$$m_5(x) = m_{10}(x) = x^2 + x + 1$$

The other minimal polynomials are computed similarly. The complete list is

$$m_0(x) = x + 1$$
$$m_1(x) = m_2(x) = m_4(x) = m_8(x) = x^4 + x + 1$$
$$m_3(x) = m_6(x) = m_9(x) = m_{12}(x) = x^4 + x^3 + x^2 + x + 1$$
$$m_5(x) = m_{10}(x) = x^2 + x + 1$$
$$m_7(x) = m_{11}(x) = m_{13}(x) = m_{14}(x) = x^4 + x^3 + 1$$

Being able to factor polynomials of the form $x^n - 1$ is important for a variety of applications of finite field theory, especially to coding theory. Since the roots of $x^{15} - 1$ over $GF(2)$ are precisely the elements of $GF(16)^*$, we have

$$x^{15} - 1 = m_0(x)m_1(x)m_3(x)m_5(x)m_7(x)$$

Of course, in order to obtain this factorization, we worked in the splitting field $GF(16)$. In Chapter 10, we will see how to factor a polynomial of the form $x^n - 1$ into a product of not necessarily irreducible factors, working only within the base field. □

*9.2 The Number of Irreducible Polynomials

Of course, if F is a finite field, then there are only a finite number of polynomials of a given degree d over F. It is possible to obtain an explicit formula for the number of irreducible polynomials of a degree d over $GF(q)$ by using Möbius inversion. (See the appendix for a discussion of Möbius inversion.) First, we need the following result.

Theorem 9.2.1 Let $GF(q)$ be a finite field, and let n be a positive integer. Then the product of all monic irreducible polynomials over $GF(q)$, whose degrees divide n, is

$$f_{q^n}(x) = x^{q^n} - x$$

Proof. According to Theorem 8.6.1, an irreducible polynomial p(x) divides $f_{q^n}(x)$ if and only if *deg* $p(x) \mid n$. Hence, $f_{q^n}(x)$ is a product of irreducible polynomials whose degrees divide n and every irreducible polynomial whose degree divides n divides $f_{q^n}(x)$. Since no two such irreducible polynomials have any roots in common and since $f_{q^n}(x)$ has no multiple roots, the result follows. ∎

Let us denote the number of monic irreducible polynomials of degree d over $GF(q)$ by $N_q(d)$. By counting degrees, Theorem 9.2.1 gives the following.

Corollary 9.2.2 For all positive integers d and n, we have

$$q^n = \sum_{d \mid n} d\,N_q(d) \qquad \square$$

Now we can apply Möbius inversion to get an explicit formula for $N_q(d)$. Classical Möbius inversion is

$$(9.2.1) \qquad g(n) = \sum_{d \mid n} f(d) \quad \Rightarrow \quad f(n) = \sum_{d \mid n} g(d)\mu\left(\frac{n}{d}\right)$$

where the Möbius function μ is defined by

$$\mu(m) = \begin{cases} 1 & \text{if } m = 1 \\ (-1)^k & \text{if } m = p_1 p_2 \cdots p_k \text{ for } \textit{distinct} \text{ primes } p_i \\ 0 & \text{otherwise} \end{cases}$$

Corollary 9.2.3 The number $N_q(n)$ of monic irreducible polynomials of degree n over $GF(q)$ is

$$N_q(n) = \frac{1}{n} \sum_{d \mid n} \mu\left(\frac{n}{d}\right) q^d = \frac{1}{n} \sum_{d \mid n} \mu(d) q^{n/d}$$

Proof. Letting $g(n) = q^n$ and $f(d) = dN_q(d)$ in (9.2.1), we get the formula above. ∎

Example 9.2.1 The number of monic irreducible polynomials of degree 12 over $GF(q)$ is

$$N_q(12) = \frac{1}{12}\left(\mu(1)q^{12} + \mu(2)q^6 + \mu(3)q^4 + \mu(4)q^3 + \mu(6)q^2 + \mu(12)q\right)$$
$$= \frac{1}{12}\left(q^{12} - q^6 - q^4 + q^2\right)$$

The number of monic irreducible polynomials of degree 4 over $GF(2)$ is

$$N_2(4) = \frac{1}{4}\left(\mu(1)2^4 + \mu(2)2^2 + \mu(4)2^1\right) = 3$$

as we would expect from the results of Example 9.1.1. □

Möbius inversion can be used to find not only the number of monic irreducible polynomials of degree d over $GF(q)$ but also the product of all such polynomials. Let us denote this product by I(q,d;x). Then Theorem 9.2.1 is equivalent to

$$x^{q^n} - x = \prod_{d \mid n} I(q,d;x)$$

Applying the multiplicative version of Möbius inversion gives the following.

Corollary 9.2.4 The product I(q,n;x) of all monic irreducible polynomials of degree n over $GF(q)$ is

$$I(q,n;x) = \prod_{d \mid n}\left(x^{q^d} - x\right)^{\mu(n/d)} = \prod_{d \mid n}\left(x^{q^{n/d}} - x\right)^{\mu(d)}$$ □

Example 9.2.2 For $q = 2$ and $n = 4$, we get

$$I(2,4;x) = (x^{16} - x)^{\mu(1)}(x^4 - x)^{\mu(2)}(x^2 - x)^{\mu(4)}$$

$$= \frac{x^{16} - x}{x^4 - x} = \frac{x^{15} - 1}{x^3 - 1} = x^{12} + x^9 + x^6 + x^3 + 1$$ □

*9.3 Polynomial Functions

Finite fields have the special property that *any* function from a finite field F to itself can be represented by a polynomial. As a matter of fact,

this property actually *characterizes* finite fields from among all commutative rings (finite and infinite)!

Since $GF(q)$ has size q, there are precisely q^q functions from $GF(q)$ to itself. Among these functions are the *polynomial functions* $\alpha \mapsto p(\alpha)$ where $p(x) \in GF(q)[x]$. We will denote this polynomial function by $p(x)$ as well. If $p(x)$ and $q(x)$ are polynomial functions on $GF(q)$ then $p(x) = q(x)$ as functions if and only if $p(\alpha) = q(\alpha)$ for all $\alpha \in GF(q)$, which holds if and only if

$$x^q - x \mid p(x) - q(x)$$

Thus, two polynomials represent the same function if and only if they are congruent modulo $x^q - x$. Since every polynomial is congruent modulo $x^q - x$ to precisely one polynomial of degree less than q (namely, its remainder after dividing by $x^q - x$), and since there are q^q polynomials of degree less than q, we have the following theorem. (Proof of the last statement in part 2 of the theorem is left to the reader.)

Theorem 9.3.1

1) Two polynomials over $GF(q)$ represent the same polynomial function on $GF(q)$ if and only if they are congruent modulo $x^q - x$.
2) Every function $f: GF(q) \to GF(q)$ is a polynomial function, for a unique polynomial of degree less than q. In fact, the unique polynomial of degree less than q that represents f is

$$p_f(x) = \sum_{\alpha \in GF(q)} f(\alpha)(1 - (x - \alpha)^{q-1}) \qquad \square$$

Note that the representation of f given in part 2) above is the *Lagrange interpolation formula* as applied to finite fields. Part 2) has a very interesting converse as well.

Theorem 9.3.2 If R is a commutative ring and if every function $f: R \to R$ is a polynomial function, for some $p(x) \in R[x]$, then R is a finite field.

Proof. First, we show that R must be finite. Suppose that $|R| = \lambda$. The number of functions from R to itself is λ^λ and the number of polynomials over R is the same as the number of finite sequences with elements from R, which is $\aleph_0 \lambda$. Since distinct functions are represented by distinct polynomials we must have $\lambda^\lambda \leq \aleph_0 \lambda$, which only happens when λ is finite. Thus, R is a finite set.

Now let $r, a \in R$ with $r \neq 0$. Define a function $f_{r,a}: R \to R$ by

$$f_{r,a}(x) = \begin{cases} a & \text{if } x = r \\ 0 & \text{if } x \neq r \end{cases}$$

By hypothesis, there exists a polynomial $a_0 + a_1x + \cdots + a_nx^n$ for which

$$a_0 + a_1r + \cdots + a_nr^n = a$$

and

$$a_0 + a_1x + \cdots + a_nx^n = 0, \quad \text{for } x \neq r$$

Setting $x = 0$ gives $a_0 = 0$ and so

$$r(a_1 + a_2r + \cdots + a_nr^{n-1}) = a$$

Thus, we conclude that for any $r \neq 0$ and any $a \in R$, there is a $u \in R$ for which $ru = a$. In other words, the map $\psi_r: R \to R$ defined by $\psi_r s = rs$ is surjective. Since R is a finite set, ψ_r must also be injective. Hence, $rs = 0$, $r \neq 0$ implies that $s = 0$ and so R has no zero divisors. In addition, since ψ_r is surjective, there exists a $u \in R$ for which $\psi_r u = r$, that is, $ru = r$. If $a \in R$ then $aru = ar$ and since R is commutative and has no zero divisors, we may cancel r to get $au = a$. Thus $u \in R$ is the multiplicative identity of R. Hence R is a finite integral domain, that is, a finite field. ∎

*9.4 Linearized Polynomials

We now turn to a discussion of linear operators on $GF(q^n)$ over $GF(q)$. We will see that all such linear operators can be expressed as polynomial functions of a very special type.

Definition A polynomial of the form

$$L(x) = \sum_{i=0}^{m} \alpha_i x^{q^i}$$

with coefficients $\alpha_i \in GF(q^n)$ is called a **linearized polynomial**, or a **q-polynomial**, over $GF(q^n)$. □

The term *linearized polynomial* comes from the following theorem, whose proof is left to the reader.

Theorem 9.4.1 Let L(x) be a linearized polynomial over $GF(q^n)$. If α, $\beta \in GF(q^n)$ and a, b $\in GF(q)$, then

$$L(a\alpha + b\beta) = aL(\alpha)b + L(\beta)$$

Thus, the polynomial function $L(x):GF(q^n) \to GF(q^n)$ is a linear operator on $GF(q^n)$ over $GF(q)$. □

The roots of a q-polynomial in a splitting field have some rather special properties, which we give in the next two theorems.

Theorem 9.4.2 Let L(x) be a nonzero q-polynomial over $GF(q^n)$, with splitting field $GF(q^s)$. Then each root of L(x) in $GF(q^s)$ has the same multiplicity, which must be either 1 or else a power of q. Furthermore, the roots of L(x) form a vector subspace of $GF(q^s)$ over $GF(q)$.

Proof. Since $L'(x) = \alpha_0$, if $\alpha_0 \neq 0$ then all roots of L(x) are simple. On the other hand, suppose that $\alpha_0 = \alpha_1 = \cdots = \alpha_{k-1} = 0$ but $\alpha_k \neq 0$. Then since $\alpha_i \in GF(q^n)$, we have

$$\alpha_i^{q^{nk}} = \alpha_i$$

and so

$$L(x) = \sum_{i=k}^{m} \alpha_i x^{q^i} = \sum_{i=k}^{m} \alpha_i^{q^{nk}} x^{q^i} = \left(\sum_{i=k}^{m} \alpha_i^{q^{(n-1)k}} x^{q^{i-k}} \right)^{q^k}$$

which is the q^k-th power of a linearized polynomial with nonzero constant term, and therefore only simple roots. Hence, each root of L(x) has multiplicity q^k. We leave proof of the fact that the roots form a vector subspace of $GF(q^s)$ to the reader. ∎

The following theorem, whose proof we omit, is a sort of converse to Theorem 9.4.1. (For a proof of this theorem, and more on q-polynomials, see the book by Lidl and Niederreiter (1986).)

Theorem 9.4.3 Let U be a vector subspace of $GF(q^n)$ over $GF(q)$. Then for any nonnegative integer k, the polynomial

$$L(x) = \prod_{\alpha \in U} (x - \alpha)^{q^k}$$

is a q-polynomial over $GF(q^n)$. □

If L(x) is a q-polynomial, then as a function, we have

$$L:\alpha \mapsto L(\alpha) = \sum_{i=0}^{m} \alpha_i \alpha^{q^i} = \sum_{i=0}^{m} \alpha_i \sigma_q^i \alpha$$

where σ_q is the Frobenius automorphism. Thus, as an operator

$$L = \sum_{i=0}^{m} \alpha_i \sigma_q^i$$

is a linear combination over $GF(q^n)$ of the automorphisms σ_q^i. Since $\sigma_q^n = \iota$ we may reduce the expression for L to a polynomial in σ_q of degree at most $n-1$. In fact, adding 0 coefficients if necessary, we can say that every q-polynomial function on $GF(q^n)$ has the **standard form**

$$L = \sum_{i=0}^{n-1} \alpha_i \sigma_q^i$$

for $\alpha_i \in GF(q^n)$. There are q^{n^2} such q-polynomial functions on $GF(q^n)$, and this happens also to be the number of linear operators on $GF(q^n)$ over $GF(q)$. Moreover, since the maps σ_q^i are linearly independent over $GF(q^n)$, we deduce that each q-polynomial in standard form represents a unique linear operator. Thus, we have characterized the linear operators on $GF(q^n)$ over $GF(q)$.

Theorem 9.4.4 Every linear operator on $GF(q^n)$ over $GF(q)$ can be represented by a unique q-polynomial in standard form

$$L(x) = \sum_{i=0}^{n-1} \alpha_i x^{q^i}$$

for some $\alpha_i \in GF(q^n)$. □

Exercises

1. Factor $x^5 - 1$ over
   (a) F_2 (b) F_3
2. Factor $x^7 - 1$ over
   (a) F_2 (b) F_3 (c) F_5
3. Factor $x^8 - 1$ over
   (a) F_2 (b) F_3 (c) F_4 (d) F_5
4. Factor $x^{10} - 1$ over
   (a) F_2 (b) F_3
5. Factor $x^{13} - 1$ over
   (a) F_2 (b) F_3
6. Calculate $N_q(20)$.
7. Show that

$$N_q(n) \leq \tfrac{1}{n}(q^n - q)$$

and

$$q^n = \sum_{d \mid n} dN_q(d) \leq nN_q(n) + \sum_{k=0}^{\lfloor n/2 \rfloor} q^k \leq nN_q(n) + q^{1+n/2}$$

Hence, $N_q(n) \geq \frac{1}{n}(q^n - q^{1+n/2})$. Finally, show that $N_q(n) \approx q^n/n$.

8. Show that the unique polynomial of degree less than q that represents the function $f: GF(q) \to GF(q)$ is

$$p_f(x) = \sum_{\alpha \in GF(q)} f(\alpha)(1 - (x - \alpha)^{q-1})$$

9. Prove that a linearized polynomial over $GF(q^n)$ is a linear operator on $GF(q^n)$ over $GF(q)$.
10. Prove that the roots of a q-polynomial over $GF(q^n)$ form a vector subspace of the splitting field $GF(q^s)$ over $GF(q)$.
11. Prove that the greatest common divisor of two q-polynomials over $GF(q^n)$ is a q-polynomial, but the least common multiple need not be a q-polynomial.

Part 3

The Theory of Binomials

Chapter 10
The Roots of Unity

Polynomials of the form $x^n - u$, where $0 \neq u \in F$, are known as **binomials.** Even though binomials have a simple form, their study is quite involved, as is evidenced by the fact that the Galois group of a binomial is often nonabelian. As we will see, an understanding of the binomial $x^n - 1$ is key to an understanding of all binomials.

We can illustrate the interplay between the binomials $x^n - 1$ and $x^n - u$, for $0 \neq u \in F$ as follows. Let E be the splitting field for $x^n - 1$ (with n odd) over F and let S be the splitting field for $x^n - u$ over F. It is not hard to show that

$$F < E < S$$

for if r and s are roots of $x^n - u$ then r/s is a root of $x^n - 1$. We will see in a later chapter that if $E = F$, that is, if $x^n - 1$ splits over F, then $F < S$ is abelian (in fact, cyclic). On the other hand, in the opposite extreme where [E:F] is as large as possible, then $F < S$ is abelian if and only if $S = E$, that is, if and only if $x^n - u$ splits over E.

10.1 Roots of Unity

The roots of the binomial $x^n - 1$ over a field F are referred to as the **n-th roots of unity over** F. Throughout this section, we will let F be a field with $p = \text{expchar}(F)$, S a splitting field for $x^n - 1$ over F and U_n the set of n-th roots of unity over F in S. Notice that if $n = kp$ then

$$x^n - 1 = x^{kp} - 1 = (x^k - 1)^p$$

and so the n-th roots of unity are the same as the k-th roots of unity, taken with a higher multiplicity. *Thus, from now on, we assume that* $(n,p) = 1$.

Theorem 10.1.1 The set U_n of n-th roots of unity over F is a cyclic group of order n under multiplication. Moreover, if $(m,n) = 1$ then

$$U_{mn} = U_m \times U_n$$

where $\times$ is the internal direct product of groups.

Proof. Clearly $\alpha, \beta \in U_n$ implies $\alpha\beta, \alpha^{-1} \in U_n$. Hence, U_n is a subgroup of the abelian group S^* of nonzero elements of S. Since $D(x^n - 1) = nx^{n-1} \neq 0$, we deduce that $x^n - 1$ is separable and therefore has n distinct roots, whence $|U_n| = n$. If $m \leq n$ is the smallest positive integer for which $\alpha^m = 1$ for all $\alpha \in U_n$, then all n elements of U_n are roots of $x^m - 1$, implying that $m \geq n$, whence $m = n$. Thus, the smallest exponent of U_n is $|U_n|$ and Theorem 0.2.11 implies that U_n is cyclic.

For the second part, if $\alpha \in U_m \cap U_n$ then $\alpha^m = 1 = \alpha^n$ and since $(m,n) = 1$ there exist $a, b \in \mathbb{Z}$ such that $am + bn = 1$, whence

$$\alpha = \alpha^{am+bn} = \alpha^{am}\alpha^{bn} = 1$$

which shows that $U_m \cap U_n = \{1\}$. It follows that the mn products in the set U_mU_n are distinct. Since $U_mU_n \subseteq U_{mn}$ and $|U_mU_n| = mn = |U_{mn}|$, we have $U_{mn} = U_mU_n$ and thus $U_{mn} = U_n \times U_m$. ∎

Definition An element $\omega \in U_n$ of order n, that is, a generator of U_n, is called a **primitive n-th root of unity** over F. We shall denote the set of all primitive n-th roots of unity over F by Ω_n and reserve the notation ω_n for a primitive n-th root of unity. □

Note that a primitive n-th root of unity ω is a field primitive element of S, since $F(\omega) = F(U_n) = S$. However, in general, S has field primitive elements that are not primitive n-th roots of unity.

Theorem 10.1.2

1) If $\omega \in \Omega_n$ then $\Omega_n = \{\omega^k \mid 1 \leq k < n, (n,k) = 1\}$ and $|\Omega_n| = \phi(n)$.
2) If $d \mid n$ then $\Omega_n^d = \Omega_{n/d}$.
3) If $(n,m) = 1$ then $\Omega_{mn} = \Omega_m\Omega_n$.

Proof. Part 1) follows from the theory of cyclic groups (see Theorem

0.2.10). For part 2), if $d = n$ the result is trivial, so assume that $d < n$. If $\omega_n \in \Omega_n$ then

$$o(\omega_n^d) = \frac{n}{(n,d)} = \frac{n}{d}$$

and so $\omega_n^d \in \Omega_{n/d}$. Thus $\Omega_n^d \subseteq \Omega_{n/d}$. For the reverse inclusion, let $\beta \in \Omega_{n/d}$. Then $\beta \in U_n$ and so $\beta = \omega^k$ for some k, where $\omega \in \Omega_n$. Since $o(\beta) = n/d$, Theorem 0.2.11 implies that $k = rd$ for some r satisfying $(r,n/d) = 1$ and so $\beta = \omega^{rd}$. Now, if every prime dividing n also divides r, then we would have $n/d = 1$, contrary to assumption. Hence, we may let $b = r + a(n/d)$, where $a > 1$ is the product of all primes dividing n but not r. Then $(b,n) = 1$. To see this, suppose that p is a prime and $p \mid n$. There are two possibilities: (i) if $p \mid r$ then $p \nmid a$ and $p \nmid (n/d)$, whence $p \nmid a(n/d)$. Hence, p cannot divide $r + a(n/d) = b$; (ii) if $p \nmid r$ then $p \mid a$ and so $p \mid a(n/d)$, and again p cannot divide $r + a(n/d) = b$. Thus, $(b,n) = 1$ and so $\omega^b \in \Omega_n$. Finally,

$$\beta = \omega^{rd} = \omega^{rd+an} = \omega^{bd} = (\omega^b)^d \in \Omega_n^d$$

For part 3), clearly $\omega_m\omega_n \in U_{mn}$. If $(\omega_m\omega_n)^k = 1$ then since $(m,n) = 1$, we have

$$\omega_m^k = \omega_n^{-k} \in U_m \cap U_n = \{1\}$$

and so $m \mid k$ and $n \mid k$, whence $mn \mid k$. Thus $o(\omega_m\omega_n) = mn$ and $\Omega_m\Omega_n \subseteq \Omega_{mn}$. Since all of the products in U_mU_n are distinct, so are all of the products in $\Omega_m\Omega_n$ and so

$$|\Omega_m\Omega_n| = \phi(m)\phi(n) = \phi(mn) = |\Omega_{mn}|$$

Hence, $\Omega_m\Omega_n = \Omega_{mn}$. ∎

10.2 Cyclotomic Extensions

Definition Let F be a field. The splitting field S of $x^n - 1$ over F is called a **cyclotomic extension of order n** of F. □

(*Cyclotomy* is the process of dividing a circle into equal parts, which is precisely the effect obtained by plotting the n-th roots of unity over **Q** in the complex plane.)

To determine the degree of S over F, note that $S = F(\omega_n)$ and so

$$[S:F] = deg\ min(\omega_n,F)$$

Since S is the splitting field of a separable polynomial, it follows that $F < S$ is a finite Galois extension and we can get a better handle on its degree by looking at the Galois group $G_F(S)$.

Any $\sigma \in G_F(S)$ is uniquely determined by its value on any $\omega \in \Omega_n$, and since σ preserves order, $\sigma\omega$ must be one of the $\phi(n)$ primitive roots of unity in S, that is,

$$\sigma\omega = \omega^{k(\sigma)}$$

where $k(\sigma) \in \mathbb{Z}_n^*$, the multiplicative group of integers in $\mathbb{Z}_n$ that are relatively prime to n.

Thus, we may define a map $\psi: G_F(S) \to \mathbb{Z}_n^*$ by

$$\psi\sigma = k(\sigma) \tag{10.2.1}$$

Since

$$(\sigma\tau)\omega = \sigma(\omega^{k(\tau)}) = (\sigma\omega)^{k(\tau)} = \omega^{k(\sigma)k(\tau)}$$

we have

$$\psi(\sigma\tau) = k(\sigma)k(\tau) = (\psi\sigma)(\psi\tau)$$

and so ψ is a homomorphism. Since $k(\sigma) = 1$ implies that $\sigma = \iota$, the map ψ is a monomorphism and thus $G_F(S)$ is isomorphic to a subgroup of $\mathbb{Z}_n^*$.

Theorem 10.2.1 If $F < S$ is a cyclotomic extension of order n then $G_F(S)$ is isomorphic to a subgroup of $\mathbb{Z}_n^*$. Hence, $G_F(S)$ is abelian and $[S:F]$ divides $\phi(n)$. □

Since the structure of $\mathbb{Z}_n^*$ is clearly important, we record the following theorem, whose proof is left as an exercise.

Theorem 10.2.2 Let $n = \prod r_i$, where the $r_i = p_i^{e_i}$ are powers of distinct prime numbers. Then

$$\mathbb{Z}_n^* \simeq \prod \mathbb{Z}_{r_i}^*$$

Moreover, $\mathbb{Z}_n^*$ is cyclic if and only if $n = p^e$, $2p^e$ or 4, where p is an odd prime. □

Corollary 10.2.3 A cyclotomic extension $F < S$ is abelian and if $n = p^e$, $2p^e$ or 4, where p is an odd prime, then $F < S$ is cyclic. □

Finite Fields

For finite fields, we can improve upon Theorem 10.2.1. In particular, if $F = GF(q)$ is a finite field then S is also a finite field and the Galois group $G_F(S)$ is cyclic with generator $\sigma_q: \alpha \to \alpha^q$. Hence, if ψ is defined by (10.2.1), then $Im\ \psi$ is the cyclic subgroup of $\mathbb{Z}_n^*$ generated by $\psi\sigma_q$. Since

$$\sigma_q \omega = \omega^q = \omega^{\bar{q}}$$

where $\bar{q}$ is the residue of q modulo n, we have $\psi\sigma_q = \bar{q}$ and $Im\ \psi = \langle \bar{q} \rangle < \mathbb{Z}_n^*$ and so $\psi: G_F(S) \to \langle \bar{q} \rangle$ is an isomorphism. In particular,

$$[S:F] = |\ G_F(S)\ | = o(\bar{q})$$

Note that we already knew this from Theorem 8.6.3, since $min(\omega, GF(q))$ has order n, and therefore degree $o(\bar{q})$.

Theorem 10.2.4 Let S be the splitting field for $x^n - 1$ over $GF(q)$, where $(q,n) = 1$. Then

1) $S = GF(q^{o_n(\bar{q})})$,

2) $G_F(S) = \langle \sigma_q \rangle$ is isomorphic to the cyclic subgroup $\langle \bar{q} \rangle$ of $\mathbb{Z}_n^*$. □

We should make a remark about the relationship between group primitive elements of S and primitive n-th roots of unity. A group primitive element β generates S_n^*

$$S_n^* = \{1, \beta, \beta^2, \ldots\}$$

whereas a primitive n-th root of unity ω generates U_n

$$U_n = \{1, \omega, \omega^2, \ldots\}$$

If β is a group primitive element of S then $o(\beta) = q^{o(\bar{q})} - 1$ and so

$$o(\beta^k) = \frac{q^{o(\bar{q})} - 1}{(k, q^{o(\bar{q})} - 1)}$$

Since $n \mid q^{o(\bar{q})} - 1$, we may write $q^{o(\bar{q})} - 1 = nr$ and so

$$o(\beta^k) = \frac{nr}{(k,nr)}$$

Hence β^k is a primitive n-th root of unity if and only if $nr/(k,nr) = n$,

that is, if and only if $r = (k,nr)$. But this holds if and only if $k = ur$ where $(u,n) = 1$.

Theorem 10.2.5 Let β be a group primitive element of the cyclotomic extension $F < S$. Then β^k is a primitive n-th root of unity if and only if

$$k = u\,\frac{q^{o_n(\bar{q})} - 1}{n}$$

where $1 \leq u < n$ and $(u,n) = 1$. □

The General Case

Returning to the general case, we can at least say some interesting things about when the Galois group is isomorphic to $\mathbb{Z}_n^*$. Let ω be a primitive n-th root of unity over F. Since $S = F(\omega)$, each $\sigma \in GF(S)$ is uniquely determined by its value on ω and so the elements $\sigma\omega$ are distinct and are the roots of $min(\omega,F)$. Hence,

$$min(\omega,F) = \prod_{\sigma \in G_F(S)} (x - \sigma\omega)$$

Since $\sigma\omega = \omega^k$ for some $k \in \mathbb{Z}_n^*$ and since $G_F(S)$ is isomorphic to $\mathbb{Z}_n^*$ if and only if there is a $\sigma \in G_F(S)$ satisfying $\sigma\omega = \omega^k$ for every $k \in \mathbb{Z}_n^*$, it follows that $G_F(S)$ is isomorphic to $\mathbb{Z}_n^*$ if and only if

$$min(\omega,F) = \prod_{(k,n)\,=\,1} (x - \omega^k) \stackrel{def}{=} Q_n(x)$$

where $Q_n(x)$ is the polynomial whose roots are the primitive n-th roots of unity in S. Since $Q_n(\omega) = 0$, this holds if and only if $Q_n(x)$ is irreducible over F. The polynomial $Q_n(x)$ is called the **n-th cyclotomic polynomial** over F. Note that it is defined only for $(n,p) = 1$ where $p =$ expchar(F).

Theorem 10.2.6 Let S be the splitting field for $x^n - 1$ over F. Then $G_F(S)$ is isomorphic to $\mathbb{Z}_n^*$ if and only if the n-th cyclotomic polynomial $Q_n(x)$ is irreducible over F. □

Here are some basic facts about cyclotomic polynomials.

Theorem 10.2.7 Let $Q_n(x)$ be the n-th cyclotomic polynomial over F.

1) $deg\ Q_n(x) = \phi(n)$.

2) $Q_n(x)$ is monic and has coefficients in the prime subfield of F.

3) If $F = \mathbb{Q}$ then the coefficients of $Q_n(x)$ are integers.

4) The following product formula holds

$$x^n - 1 = \prod_{d \mid n} Q_d(x) \tag{10.2.2}$$

Proof. Part 1) follows directly from the definition of $Q_n(x)$. Part 4) follows from the fact that U_n is the disjoint union of Ω_d over all $d \mid n$ and $Q_d(x)$ has no multiple roots. Hence, the factorizations of both sides of (10.2.2) into a product of linear factors are identical.

Let F' be the prime field of F. It is clear from the definition that $Q_n(x)$ is monic. We prove parts 2) and 3) together by induction on n. Since $Q_1(x) = x - 1$, the result is true for $n = 1$. If p is a prime then

$$Q_p(x) = \frac{x^p - 1}{x - 1} = x^{p-1} + x^{p-2} + \cdots + x + 1$$

and the result holds for $n = p$. Assume that 2) and 3) hold for all proper divisors of n. Then

$$x^n - 1 = Q_n(x) \prod_{\substack{d \mid n \\ d < n}} Q_d(x) = Q_n(x)R(x)$$

By the induction hypothesis, $R(x)$ has coefficients in F', whence so does $Q_n(x) = (x^n - 1)/R(x)$. Moreover, if $F = \mathbb{Q}$ then $R(x)$ has integer coefficients and since $R(x)$ is monic, Theorem 1.2.1 implies that $Q_n(x)$ has integer coefficients. ∎

Example 10.2.1 Formula (10.2.2) can be used to compute cyclotomic polynomials rather readily, starting from the fact that

$$Q_1(x) = x - 1$$

and

$$Q_p(x) = x^{p-1} + x^{p-2} + \cdots + x + 1$$

for p prime. Thus, for example,

$$Q_4(x) = \frac{x^4 - 1}{Q_1(x)Q_2(x)} = \frac{x^4 - 1}{(x-1)(x+1)} = x^2 + 1$$

$$Q_6(x) = \frac{x^6 - 1}{Q_1(x)Q_2(x)Q_3(x)} = \frac{x^6 - 1}{(x-1)(x+1)(x^2+x+1)} = x^2 - x + 1$$

and

$$Q_{15}(x) = \frac{x^{15}-1}{Q_1(x)Q_2(x)Q_3(x)Q_5(x)} = x^8 - x^7 + x^5 - x^4 + x^3 - x + 1$$

This gives us, for instance, the following a factorization of $x^{15}-1$ into cyclotomic polynomials over $GF(2)$

$$x^{15}-1 = (x+1)(x^2+x+1)(x^4+x^3+x^2+x+1)(x^8+x^7+x^5+x^4+x^3+x+1) \quad \square$$

Part 4) of Theorem 10.2.7 describes a factorization of x^n-1 within the prime subfield of F (*cf.* Example 9.1.1). In general, however, this is not a prime factorization since $Q_n(x)$ is not irreducible. For instance, comparing Examples 10.2.1 and 9.1.1 shows that $Q_{15}(x)$ is reducible over $GF(2)$.

With regard to the irreducibility of cyclotomic polynomials, we do have the following important results.

Theorem 10.2.8 All cyclotomic polynomials $Q_n(x)$ over $\mathbb{Q}$ are irreducible over $\mathbb{Q}$. Therefore, $G_{\mathbb{Q}}(S) \simeq \mathbb{Z}_n^*$ and $[S:\mathbb{Q}] = \phi(n)$.

Proof. Suppose that $Q_n(x) = f(x)g(x)$, where we may assume (by Theorem 1.2.2) that $f(x)$ and $g(x)$ are monic and have integer coefficients. Assume that $f(x)$ is irreducible and that ω is a root of $f(x)$ and hence a primitive n-th root of unity. We claim that ω^p is also a root of $f(x)$, for any prime $p \nmid n$. For if not then ω^p, being a primitive n-th root of unity, must be a root of $g(x)$. Hence, ω is a root of $g(x^p)$, which implies that $f(x) \mid g(x^p)$ and we can write

$$g(x^p) = h(x)f(x)$$

where $h(x)$ is monic and has integer coefficients. Since $a^p \equiv a \bmod p$, for any integer a, we conclude that $g(x^p) \equiv g(x)^p \bmod p$ and so, taking residues gives

$$g(x)^p \equiv h(x)f(x) \bmod p$$

If we denote the residue of a polynomial $p(x)$ modulo p by $\bar{p}(x)$, we get

$$\bar{g}(x)^p = \bar{h}(x)\bar{f}(x)$$

in $\mathbb{Z}_p[x]$ and so any irreducible factor of $\bar{f}(x)$ in $\mathbb{Z}_p[x]$ is also a factor of $\bar{g}(x)$. This shows that $\bar{f}(x)$ and $\bar{g}(x)$ are not relatively prime, and therefore have a common root in some extension of $\mathbb{Z}_p$. However, $\bar{f}(x)\bar{g}(x) = x^n - \bar{1}$, which has no multiple roots in any extension. This

contradiction implies that ω^p is a root of f(x). In other words, if ω is a root of f(x) then so is $\sigma_p\omega$, where σ_p is the Frobenius map.

Now we observe that any primitive n-th root of unity ν over $\mathbb{Q}$ has the form ω^r, for some integer $r > 0$. Writing r as a product of prime numbers, we see that ν can be obtained from ω by applying a finite number of Frobenius maps σ_p, where p is prime. Hence, ν is also a root of f(x). Thus all roots of $Q_n(x)$ are roots of f(x), implying that $f(x) = Q_n(x)$, whence $Q_n(x)$ is irreducible over $\mathbb{Q}$. ∎

Theorem 10.2.9 Let n be an odd positive integer. Then $[F(\omega_n):F] = \phi(n)$ implies $[F(\omega_d):F] = \phi(d)$ for all $d \mid n$. In the language of cyclotomic polynomials, if $Q_n(x)$ is irreducible over F then $Q_d(x)$ is irreducible over F for all $d \mid n$.

Proof. Let p be a prime dividing n. Since n is odd, $p \neq 2$. Let $n = pm$. Then

$$\phi(pm) = [F(\omega_n):F(\omega_n^p)][F(\omega_n^p):F] = ab$$

where $a = [F(\omega_n):F(\omega_n^p)] \leq p$ and $b = [F(\omega_n^p):F] \mid \phi(m)$, since $\omega_n^p \in \Omega_m$.

If $p \nmid m$ then $\phi(pm) = \phi(p)\phi(m) = (p-1)\phi(m)$ and so

$$(p-1)\phi(m) = ab$$

If $a = p$, then $b = (p-1)\phi(m)/p$ cannot divide $\phi(m)$ since $p \neq 2$. Since $b \leq \phi(m)$, it follows that $a = p - 1$ and $b = \phi(m)$. On the other hand, if $p \mid m$ then $\phi(pm) = p\phi(m)$ and so

$$p\phi(m) = ab$$

whence $a = p$ and $b = \phi(m)$. In either case, $b = \phi(m)$, and since $\omega_n^p = \omega_{n/p}$, we have

$$[F(\omega_{n/p}):F] = \phi\left(\frac{n}{p}\right) \tag{10.2.3}$$

Repeated use of (10.2.3) gives the desired result. ∎

Let us return briefly to finite fields. If p(x) is monic and irreducible over $GF(q)$ and has order ν, then each root of p(x) has order ν and thus $p(x) \mid Q_\nu(x)$. Since every monic irreducible factor of $Q_\nu(x)$ has order ν, we conclude that $Q_\nu(x)$ is the product of all monic irreducible polynomials of order ν. According to Theorem 8.6.3, the degree of any such factor p(x) is $o_\nu(q)$, the order of q modulo ν. Hence, the number of monic irreducible polynomials of order ν is $\phi(\nu)/o_\nu(q)$.

Theorem 10.2.10 Let ν be a positive integer.

1) The cyclotomic polynomial $Q_\nu(x)$ over $GF(q)$ is the product of all monic irreducible polynomials of order ν over $GF(q)$.
2) The number of monic irreducible polynomials over $GF(q)$ of order ν is $\phi(\nu)/o_\nu(q)$, where $o_\nu(q)$ is the order of q mod ν. □

Equation (10.2.2) is a prime candidate for Möbius inversion. (See the appendix for a discussion of Möbius inversion.) Applying the multiplicative version gives

$$Q_n(x) = \prod_{d \mid n} (x^d - 1)^{\mu(n/d)} = \prod_{d \mid n} (x^{n/d} - 1)^{\mu(d)}$$

where the Möbius function μ is defined by

$$\mu(d) = \begin{cases} 1 & \text{if } d = 1 \\ (-1)^k & \text{if } d = p_1 p_2 \cdots p_k \text{ for } \textit{distinct} \text{ primes } p_i \\ 0 & \text{otherwise} \end{cases}$$

Note that some of the exponents $\mu(d)$ may be equal to -1, and so a little additional algebraic manipulation may be required to obtain $Q_n(x)$ as a product of polynomials.

Finally, let us mention that, according to the definition, if $\nu = q^n - 1$, then the roots of the ν-th cyclotomic polynomial $Q_\nu(x)$ over $GF(q)$ are the primitive ν-th roots of unity over $GF(q)$. Hence, they are the group primitive elements of $GF(q^n)$. In other words, the monic irreducible factors of $Q_\nu(x)$ are precisely the primitive polynomials of $GF(q^n)$ over $GF(q)$. Thus, one way to find primitive polynomials is to factor this cyclotomic polynomial.

*10.3 Normal Bases and Roots of Unity

Recall that a normal basis for $F < E$ is a basis for E over F that consists of the roots of an irreducible polynomial p(x) over F. (See Section 7.4.) We have seen that, in some important cases (especially $F = \mathbb{Q}$), the cyclotomic polynomials $Q_n(x)$ are irreducible over F, which leaves open the possibility that the primitive n-th roots of unity Ω_n might form a normal basis for S over F. Indeed, if $Q_n(x)$ is irreducible then $Q_n(x) = min(\omega_n, F)$ and so

$$deg\ Q_n(x) = [S:F]$$

and since the roots of $Q_n(x)$ are distinct, there are the right number of primitive n-th roots of unity and they will form a basis for S over F if and only if they span S over F. It happens that Ω_n spans S if and only if n has a certain simple form.

Theorem 10.3.1 Let F be a field with the property that $Q_m(x)$ is irreducible over F for all m. Then Ω_n is a normal basis for the cyclotomic extension S over F if and only if n is the product of distinct primes.

Proof. We prove first that if n is a product of distinct primes then Ω_n is a (normal) basis for S over F. Let $\omega \in \Omega_n$. If $n = p$ is prime then $\Omega_p = \{\omega, \omega^2, \ldots, \omega^{p-1}\}$. Since $S = F(\omega)$ and $min(\omega, F) = Q_p(x)$ has degree $p-1$, the set $\{1, \omega, \ldots, \omega^{p-2}\}$ is a (polynomial) basis for S over F. Since

$$1 + \omega + \cdots + \omega^{p-1} = \frac{\omega^p - 1}{\omega - 1} = 0$$

the set $\Omega_p = \{\omega, \ldots, \omega^{p-1}\}$ is also a basis for S over F. Hence, the result is true if n is prime.

For the purposes of induction, suppose the result is true for all proper divisors of n and let $n = km$ with $k < n$, $m < n$ and $(k,m) = 1$. If $\omega_k \in \Omega_k$ and $\omega_m \in \Omega_m$ then Ω_k is a basis for $F(\omega_k)$ over F and Ω_m is a basis for $F(\omega_m)$ over F. Since $\omega_k \omega_m \in \Omega_{km}$ and $(k,m) = 1$, it follows that

$$(\omega_k \omega_m)^k = \omega_m^k \in \Omega_m \quad \text{and} \quad (\omega_k \omega_m)^m = \omega_k^m \in \Omega_k$$

whence $F(\omega_k, \omega_m) = F(\omega_k \omega_m) = F(\omega_{km})$ where $\omega_{km} \in \Omega_{km}$. Hence,

$$[F(\omega_k, \omega_m) : F(\omega_m)][F(\omega_m) : F] = [F(\omega_k, \omega_m) : F] = [F(\omega_{km}) : F]$$

$$= \phi(km) = \phi(k)\phi(m) = \phi(k)[F(\omega_m) : F]$$

and so $[F(\omega_k, \omega_m) : F(\omega_m)] = \phi(k)$. Since Ω_k spans $F(\omega_k, \omega_m)$ over $F(\omega_m)$ and $|\Omega_k| = \phi(k)$, it follows that Ω_k is a basis for $F(\omega_k, \omega_m)$ over $F(\omega_m)$, whence $\Omega_{km} = \Omega_k \Omega_m$ is a basis for $F(\omega_k, \omega_m)$ over F. This proves that if n is the product of distinct primes, then Ω_n is a basis for $F(\omega_n)$.

For the converse, let $n = mp^k$ for $k \geq 2$. Since

$$Q_n(x) = Q_{mp^k}(x) = Q_{mp}(x^{p^{k-1}})$$

(an exercise) the coefficient of $x^{\phi(n)-1}$ in $Q_n(x)$ is 0, whence the sum of the roots of $Q_n(x)$, that is, the sum of the primitive n-th roots of unity, is 0, showing that these roots are linearly dependent. Hence, they cannot form a basis for S over F. ∎

*10.4 Wedderburn's Theorem

In this section, we present an important result whose proof uses the properties of cyclotomic polynomials.

Theorem 10.4.1 (Wedderburn's Theorem) If D is a finite division ring then D is a field.

Proof. We begin by recalling Example 0.2.1, which describes an instance of the class equation. Let the group D^* act on itself by conjugation. The stabilizer of $\beta \in D^*$ is the centralizer

$$C^*(\beta) = \{\alpha \in D^* \mid \alpha\beta = \beta\alpha\}$$

and the class equation is

$$|D^*| = |Z(D^*)| + \sum \frac{|D^*|}{|C^*(\beta)|}$$

where the sum is taken over one representative β from each conjugacy class $o(\beta) = \{\alpha\beta\alpha^{-1} \mid \alpha \in G\}$ of size greater than 1. If we assume for the purposes of contradiction that $Z(D^*) \neq D^*$, then the sum on the far right is not an empty sum and $|C^*(\beta)| < |D^*|$ for some $\beta \in D^*$.

The sets

$$Z(D) = \{\beta \in D \mid \beta\alpha = \alpha\beta \text{ for all } \alpha \in D\}$$

and

$$C(\beta) = \{\alpha \in D \mid \alpha\beta = \beta\alpha\}$$

are subrings of D and, in fact, Z(D) is a commutative division ring; that is, a field. Moreover, $Z(D)^* = Z(D^*)$ and $C(\beta)^* = C^*(\beta)$ for $\beta \neq 0$. Let $|Z(D)| = z$. Since $Z(D) \subseteq C(\beta)$, we may view $C(\beta)$ and D as vector spaces over Z(D) and so

$$|C(\beta)| = z^b \quad \text{and} \quad |D| = z^n$$

for integers $1 \leq b < n$. The class equation now gives

$$z^n - 1 = z - 1 + \sum_b \frac{z^n - 1}{z^b - 1}$$

and since $z^b - 1 \mid z^n - 1$, it follows that $b \mid n$.

If $Q_n(x)$ is the n-th cyclotomic polynomial over $\mathbf{Q}$, then $Q_n(z)$ divides $z^n - 1$. But $Q_n(z)$ also divides each summand on the far right above, since for $b \mid n$, $b < n$ we have

$$\frac{x^n-1}{x^b-1} = \prod_{k \mid n} Q_k(x) \Big/ \prod_{j \mid b} Q_j(x)$$

and $Q_n(x)$ divides the right hand side. It follows that $Q_n(z) \mid z-1$. On the other hand,

$$Q_n(z) = \prod_{\omega \in \Omega_n} (z-\omega)$$

and since $\omega \in \Omega_n$ implies that $|z-\omega| > |z| - |\omega| = z-1$, we have a contradiction. Hence $Z(D^*) = D^*$ and D is commutative, that is, D is a field. ∎

*10.5 Realizing Groups as Galois Groups

A group G is said to be **realizable** over a field F if there is an extension $F < E$ for which $G_F(E) \simeq G$. Since any finite group of order n is isomorphic to a subgroup of a symmetric group S_n, we have the following.

Theorem 10.5.1 Let F be a field. Every finite group is realizable over some extension of F.

Proof. Let G be a group of order n. Let $t_1,\ldots,t_n$ be algebraically independent over F and let $s_1,\ldots,s_n$ be the elementary symmetric functions in the t_i's. Then $K = F(t_1,\ldots,t_n) > F(s_1,\ldots,s_n) = E$ is a Galois extension whose Galois group is isomorphic to S_n. (See Theorem 6.2.1.) We may assume that G is a subgroup of $G_E(K)$ and since G is closed in the Galois correspondence, it is the Galois group of $F(G) < K$. ∎

It is a major unsolved problem to determine which finite groups are realizable over the rational numbers $\mathbb{Q}$. We shall prove that any finite abelian group is realizable over $\mathbb{Q}$. It is also true that for any n, the symmetric group S_n is realizable over $\mathbb{Q}$, but we shall prove this only when $n = p$ is a prime.

Realizing Finite Abelian Groups over Q

We shall have use for a special case of a famous theorem of Dirichlet, which says that if n and m are relatively prime positive integers then there are infinitely many prime numbers of the form $nk + m$. We need the case $m = 1$. First a lemma on cyclotomic polynomials.

Lemma 10.5.2 Let p be a prime and let $(n,p) = 1$. Let $Q_n(x)$ be the n-th cyclotomic polynomial over $\mathbb{Q}$ and let $P_n(x)$ be the n-th cyclotomic

polynomial over $\mathbb{Z}_p$. If $\overline{Q}_n(x)$ is the polynomial obtained from $Q_n(x)$ by taking the residue of each coefficient modulo p, then $\overline{Q}_n(x) = P_n(x)$.

Proof. If $n = r$ is a prime then $Q_r(x)$, $P_r(x)$ and $\overline{Q}_r(x)$ are all equal to

$$x^{r-1} + x^{r-2} + \cdots + 1$$

and so the result holds for n prime. Suppose the result holds for all proper divisors of n. Since

$$x^n - 1 = \prod_{d \mid n} Q_d(x)$$

taking residues modulo p gives

$$x^n - 1 = \prod_{d \mid n} \overline{Q}_d(x)$$

over $\mathbb{Z}_p$. But

$$x^n - 1 = \prod_{d \mid n} P_d(x)$$

over $\mathbb{Z}_p$ and since $P_d(x) = \overline{Q}_d(x)$ for all $d \mid n$, $d < n$, we have $P_n(x) = \overline{Q}_n(x)$. ∎

Theorem 10.5.3 Let n be a positive integer. Then there are infinitely many prime numbers of the form $nk + 1$, for $k \in \mathbb{Z}^+$.

Proof. Suppose to the contrary that $p_1, \ldots, p_s$ is a complete list of all primes of the form $nk + 1$. Let $m = p_1 \cdots p_s n$. Let $Q_m(x)$ be the m-th cyclotomic polynomial over $\mathbb{Q}$ and consider the polynomial $Q_m(mx)$. Since $Q_n(x)$ has integer coefficients, $Q_m(mk)$ is an integer for all $k \in \mathbb{Z}^+$. Since $Q_m(mk)$ can equal 0, 1 or −1 for only a finite number of positive integers k, there exists a positive integer k for which $|Q_m(mk)| > 1$. Let p be a prime dividing $Q_m(mk)$. Since $Q_m(x) \mid x^m - 1$, we have

$$p \mid (mk)^m - 1$$

which implies that $p \nmid m$, hence $p \neq p_i$ for $i = 1, \ldots, s$.

If $P_m(x)$ is the m-th cyclotomic polynomial over $\mathbb{Z}_p$ then it follows from the fact that $p \mid Q_m(mk)$, and the previous lemma, that

$$P_m(\overline{mk}) = \overline{Q}_m(\overline{mk}) = \overline{Q_m(mk)} = 0$$

in $\mathbb{Z}_p$, where $\overline{mk}$ is the residue of mk modulo p. Thus, $\overline{mk}$ is a primitive m-th root of unity over Z_p. In other words, $\overline{mk}$ has order m in $\mathbb{Z}_p^*$ and since the order of any element must divide the order of the group, we

get $m \mid p-1$. It follows that $n \mid p-1$, that is, $p = nk+1$, which is a contradiction, proving the theorem. ∎

Theorem 10.5.4 Let G be a finite abelian group. Then there exists an integer n and a field E such that $\mathbb{Q} < E < \mathbb{Q}(\omega)$, where ω is a primitive n-th root of unity, and such that $G_{\mathbb{Q}}(E) \simeq G$.

Proof. By Theorem 10.2.8, the Galois group of $\mathbb{Q}(\omega)$ is isomorphic to $\mathbb{Z}_n^*$. Since $\mathbb{Z}_n^*$ is abelian, any subgroup K of $\mathbb{Z}_n^*$ is normal in $\mathbb{Z}_n^*$ and so $\mathbb{Q} < F(K)$ is a Galois extension, with Galois group

$$G_{\mathbb{Q}}(K) \simeq \mathbb{Z}_n^*/K$$

Thus, we need only show that any finite abelian group G is isomorphic to a quotient group $\mathbb{Z}_n^*/K$, for some integer n.

Since G is finite and abelian, we have

$$G \simeq C(n_1) \times \cdots \times C(n_s)$$

where $C(n_i)$ is cyclic of degree n_i. According to Theorem 10.5.3, we may choose *distinct* primes $p_1, \ldots, p_s$ of the form $n_1 \cdots n_s k + 1$ and so $n_i \mid p_i - 1$ for $i = 1, \ldots, s$. Since the cyclic group

$$\mathbb{Z}_{p_i}^*$$

has order $p_i - 1$, it has a subgroup of any order dividing $p_i - 1$, in particular, a subgroup K_i of order $(p_i - 1)/n_i$, whence the quotient

$$\mathbb{Z}_{p_i}^*/K_i$$

is cyclic of order n_i, and is therefore isomorphic to $C(n_i)$. Hence, if $K = K_1 \times \cdots \times K_s$ and $n = p_1 \cdots p_s$ then

$$G \simeq \frac{\mathbb{Z}_{p_1}^*}{K_1} \times \cdots \times \frac{\mathbb{Z}_{p_s}^*}{K_s} \simeq \frac{\mathbb{Z}_{p_1}^* \times \cdots \times \mathbb{Z}_{p_s}^*}{K_1 \times \cdots \times K_s} \simeq \frac{\mathbb{Z}_{p_1 \cdots p_s}^*}{K} \simeq \frac{\mathbb{Z}_n^*}{K}$$

as desired. ∎

Realizing S_p over Q

We begin by discussing a sometimes useful tool for showing that the Galois group of a polynomial is a symmetric group.

Let G be the Galois group of an irreducible polynomial $f(x) \in F[x]$, thought of as a group of permutations on the set R of roots of f(x). Then G acts transitively on R. Let us define an equivalence relation on R by saying that $r \sim s$ if and only if either $r = s$ or the transposition

(r,s) is an element of G (more properly, an element of G acts as the transposition (r,s) on R.) It is easy to see that this is an equivalence relation on R.

Let [r] be the equivalence class containing r, and assume there exists s, $r \in R$ such that $s \neq r$ and $s \sim r$. In other words, assume that G contains a transposition (r,s). If $\sigma \in G$ then $\sigma(r,s)\sigma^{-1}$ sends σr to σs, σs to σr and fixes all other elements of R, whence $\sigma(r,s)\sigma^{-1} = (\sigma r, \sigma s)$. Thus, $s \sim r$ implies $\sigma s \sim \sigma r$ and so $\sigma[r] = [\sigma r]$. This shows that [r] and $[\sigma r]$ have the same cardinality and since G acts transitively on R, all equivalence classes have the same cardinality.

It follows that if $|R|$ is prime, then there can be only one equivalence class, which implies that $(r,s) \in G$ for all $r, s \in R$. Since G contains every transposition, it must be the symmetric group on R. We have proved the following.

Theorem 10.5.5 If $f(x) \in F[x]$ is a separable polynomial of prime degree p and if the Galois group G of f(x) contains a transposition, then G is isomorphic to the symmetric group S_p. □

Corollary 10.5.6 If $f(x) \in \mathbb{Q}[x]$ is irreducible of prime degree p and if f(x) has precisely two nonreal roots, then the Galois group of f(x) is isomorphic to the symmetric group S_p.

Proof. Complex conjugation on $\mathbb{C}$ is an automorphism of $\mathbb{C}$ leaving $\mathbb{Q}$ fixed. Since the splitting field S for f(x) over $\mathbb{Q}$ is Galois, conjugation is a $\mathbb{Q}$-automorphism of S, and therefore belongs to $G_{\mathbb{Q}}(S)$. Since it leaves the $p-2$ real roots of f(x) fixed, it is a transposition on the roots of f(x). Thus, the theorem applies. ∎

Example 10.5.1 Consider the polynomial $f(x) = x^5 - 5x + 2$, which is irreducible over $\mathbb{Q}$ by Eisenstein's criterion. A quick sketch of the graph reveals that f(x) has precisely 3 real roots and so its Galois group is isomorphic to S_5. □

Corollary 10.5.6 is just what we need to establish that S_p is realizable over $\mathbb{Q}$.

Theorem 10.5.7 Let p be a prime. There exists an irreducible polynomial p(x) over $\mathbb{Q}$ of degree p such that p(x) has precisely two nonreal roots. Hence, the symmetric group S_p is realizable over $\mathbb{Q}$.

Proof. The result is easy for $p = 2$ and 3, so let us assume that $p \geq 5$. Let n be a positive integer and $m \geq 5$ be an odd integer. Let $k_1, \ldots, k_{m-2}$ be even integers and let

$$q(x) = (x^2 + n)(x - k_1)\cdots(x - k_{m-2})$$

It is easy to see from the graph that $q(x)$ has $(m-3)/2$ relative maxima. Moreover, if k is an odd integer, then

$$|\, q(k)\,| \geq 2\,|\, k^2 + n\,| > 2$$

Let $p(x) = q(x) - 2$. Since the relative maxima of $q(x)$ are all greater than 2 and since $q(-\infty) = -\infty$ and $q(\infty) = \infty$, we deduce that $p(x)$ has the same number $m-2$ of real roots as $q(x)$.

We wish to choose a value of n for which $p(x)$ has at least one nonreal root z, for then the complex conjugate $\bar{z}$ is also a root, implying that $p(x)$ has two nonreal roots and $m-2$ real roots. Let the roots of $p(x)$ in a splitting field be $\alpha_1, \ldots, \alpha_m$. Then

$$p(x) = \prod_{i=1}^{m} (x - \alpha_i) = (x^2 + n)(x - k_1)\cdots(x - k_{m-2}) - 2$$

Equating coefficients of x^{m-1} and x^{m-2} gives

$$\sum_{i=1}^{m} \alpha_i = \sum_{i=1}^{m-2} k_i \quad \text{and} \quad \sum_{i<j} \alpha_i \alpha_j = \sum_{i<j} k_i k_j + n$$

and so

$$\sum_{i=1}^{m} \alpha_i^2 = \Big(\sum_{i=1}^{m} \alpha_i\Big)^2 - 2\sum_{i<j} \alpha_i \alpha_j = \Big(\sum_{i=1}^{m-2} k_i\Big)^2 - 2\Big(\sum_{i<j} k_i k_j + n\Big)$$

$$= \sum_{i=1}^{m-2} k_i^2 - 2n$$

If n is sufficiently large, then $\sum \alpha_i^2$ is negative, whence at least one of the roots α_i must be nonreal, as desired.

It is left to show that $p(x)$ is irreducible, which we do using Eisenstein's criterion. Let us write

$$q(x) = (x^2 + n)(x - k_1)\cdots(x - k_{m-2}) = x^m + a_{m-1}x^{m-1} + \cdots + a_0$$

In the product $(x - k_1)\cdots(x - k_{m-2})$, each coefficient except the leading one is divisible by 2. Hence, we may write

$$(x - k_1)\cdots(x - k_{m-2}) = x^{m-2} + 2f(x)$$

Multiplying by $x^2 + n$ gives

$$q(x) = x^m + 2x^2 f(x) + nx^{m-2} + 2nf(x)$$

Taking n to be even, we deduce that all nonleading coefficients of q(x) are even. In addition, the constant term of q(x) is divisible by 4 since $m \geq 5$. It follows that $p(x) = q(x) - 2$ is monic, all nonleading coefficients are divisible by 2, but the constant term is not divisible by $2^2 = 4$. Therefore p(x) is irreducible and the proof is complete. ∎

Exercises

All cyclotomic polynomials are assumed to be over fields for which they are defined.

1. Prove that if $x^n - 1 = Q_n(x)p(x)$ where $p(x) \in \mathbb{Z}[x]$ then $Q_n(x) \in \mathbb{Z}[x]$.
2. When is a group primitive element of the cyclotomic extension S_n also a primitive n-th root of unity over *GF*(q)?
3. If $(n,q) \neq 1$, how many n-th roots of unity are there over *GF*(q)?
4. What is the splitting field for $x^4 - 1$ over *GF*(3)? Find the primitive 4-th roots of unity in this splitting field. Do the same for the 8-th roots of unity over *GF*(3).
5. If $\alpha_1, \ldots, \alpha_n$ are the n-th roots of unity over *GF*(q) show that $\alpha_1^k + \alpha_2^k + \cdots + \alpha_n^k = 0$ for $1 < k < n$.
6. Show that $Q_n(x) \in GF(q)[x]$ is irreducible if and only if $o_n(q) = \phi(n)$.
7. If $(n,q) = 1$, prove that $x^{n-1} + x^{n-2} + \cdots + x + 1$ is irreducible over *GF*(q) if and only if n is prime and $Q_n(x)$ is irreducible.
8. Show that if r is a prime, then $Q_{r^n}(x) = (x^{r^n} - 1)/(x^{r^{n-1}} - 1)$.
9. Evaluate $Q_n(1)$.
10. Evaluate $Q_n(-1)$.
11. Show that $\mathbb{Q}(\omega_n) \cap \mathbb{Q}(\omega_m) = \mathbb{Q}$ if $(m,n) = 1$.

Verify the following properties of the cyclotomic polynomials. As usual, p is a prime number.

12. $Q_{np}(x) = Q_n(x^p)/Q_n(x)$ for $p \nmid n$.
13. $Q_{np}(x) = Q_n(x^p)$ for all $p \mid n$.
14. $Q_{np^k}(x) = Q_{np}(x^{p^{k-1}})$
15. $Q_n(0) = 1$ for $n \geq 2$.
16. $Q_n(x^{-1})x^{\phi(n)} = Q_n(x)$ for $n \geq 2$.
17. If $n = p_1^{e_1} \cdots p_k^{e_k}$ is the decomposition of n into a product of powers of distinct primes, then

$$Q_n(x) = Q_{p_1 \cdots p_k}(x^{p_1^{e_1-1} \cdots p_k^{e_k-1}})$$

On the structure of $\mathbb{Z}_n^*$.

18. If $n = \prod r_i$ where $r_i = p_i^{e_i}$ are distinct prime powers then

$$\mathbb{Z}_n^* \simeq \prod \mathbb{Z}_{r_i}^*$$

19. Assume $p \neq 2$ is prime. Let $n = p^e$.
    i) Show that $|\mathbb{Z}_n^*| = p^{e-1}(p-1)$.
    ii) Show that $\mathbb{Z}_n^*$ has an element of order $p-1$.
    iii) Show that $1+p \in \mathbb{Z}_n^*$ has order p^{e-1}.
    iv) Show that $\mathbb{Z}_n^*$ is cyclic.
    v) If $n = 2^e$ then $\mathbb{Z}_n^*$ is cyclic if and only if $e = 1$ or 2.
    vi) Show that $\mathbb{Z}_n^*$ is cyclic if and only if $n = p^e$, $2p^e$ or 4.
20. If $n > 1$ then there exists an irreducible polynomial of degree n over $\mathbb{Q}$ whose Galois group is isomorphic to $\mathbb{Z}_n$.
21. Find an integer n and a field E such that $\mathbb{Q} < E < \mathbb{Q}(\omega_n)$ with $G_{\mathbb{Q}}(E) = \mathbb{Z}_8$. Here ω_n is a primitive n-th root of unity over $\mathbb{Q}$.
22. Calculate the Galois group of the polynomial $f(x) = x^5 - 4x + 2$.

More on Constructions

The following exercises show that not all regular n-gons can be constructed in the plane using only a straight edge and compass. The reader may refer to the exercises of Chapter 2 for the relevant definitions.

Definition A complex number z is **constructible** if its real and imaginary parts are both constructible. □

C1. Prove that the set of all constructible complex numbers forms a subfield of the complex numbers $\mathbb{C}$.
C2. Prove that a complex number $z = re^{i\theta}$ is constructible if and only if the real number r and the angle θ (that is, the real number $\cos\theta$) are constructible.
C3. Prove that if z is constructible, then both square roots of z are constructible. *Hint*: use the previous exercise.
C4. Prove that a complex number z is constructible if and only if there exists a tower of fields $\mathbb{Q} < F_1 < \cdots < F_n$, each one a quadratic extension of the previous one, such that $z \in F_n$.
C5. Prove that if z is constructible, then $[\mathbb{Q}(z):\mathbb{Q}]$ must be a power of 2.
C6. Show that the constructibility of a regular n-gon is equivalent to the constructibility of a primitive n-th root of unity ω_n. Since the

cyclotomic polynomial $Q_n(x)$ is irreducible over the rationals, we have $[\mathbb{Q}(\omega_n):\mathbb{Q}] = deg\ Q_n(x) = \phi(n)$.

C7. Prove that $\phi(n)$ is a power of 2 if and only if n has the form

$$n = 2^k p_1 \cdots p_m$$

where p_m are distinct *Fermat primes*, that is, primes of the form

$$2^{2^s} + 1$$

for some nonnegative integer s. *Hint*: if $2^j + 1$ is prime then j must be a power of 2. Conclude that if n does not have this form, then a regular n-gon is not constructible. For instance, we cannot construct a regular n-gon for n = 7, 11 or 90. [Gauss proved that if n has the above form, then a regular n-gon can be constructed. See Hadlock (1978).]

Chapter 11
Cyclic Extensions

Continuing our discussion of binomials begun in the previous chapter, we will show that if α is a root of $x^n - u$ and if ω is a primitive n-th root of unity over F, then $F(\omega,\alpha)$ is a splitting field for $x^n - u$ over F. Moreover, in the tower

$$F < F(\omega) < F(\omega,\alpha)$$

the first step is a cyclotomic extension, which as we have seen, is abelian and may be cyclic. The second step is cyclic of degree $d \mid n$. Nevertheless, as we will see in Chapter 13, the Galois group $G_F(F(\omega,\alpha))$ need not even be abelian. In studying the second step in this tower, we will actually characterize finite cyclic extensions, when the base field contains appropriate roots of unity.

Before beginning, we remark that if F is a field of characteristic $p \neq 0$ and if $p \mid n$, then F cannot contain a primitive n-th root of unity. For if $n = pm$ and $\omega^n - 1 = 0$ then

$$0 = \omega^n - 1 = \omega^{pm} - 1 = (\omega^m - 1)^p$$

and so $\omega^m = 1$, whence ω is an m-th root of unity, for $m < n$. Thus, saying that a field F contains a *primitive* n-th root of unity tacitly implies that $(n,\text{expchar}(F)) = 1$. (Such an implication is not made by saying that F contains the n-th roots of unity.)

11.1 Cyclic Extensions

Let F be a field with expchar(F) = p, let $u \in F$ and let S be the splitting field for the binomial $x^n - u$ over F. *We will assume throughout that* (n,p) = 1 and so $x^n - u$ has n distinct roots in S.

If α is a root of $x^n - u$ in S and ω is a primitive n-th root of unity over F then the roots of $x^n - u$ are

$$\alpha, \omega\alpha, \ldots, \omega^{n-1}\alpha \tag{11.1.1}$$

and so $S = F(\omega,\alpha)$. In words, all n-th roots of u can be obtained by first adjoining the n-th roots of unity and then adjoining any single n-th root of u.

The extension $F < S$ can thus be decomposed into a tower

$$F < F(\omega) < F(\omega,\alpha) = S$$

The first step is cyclotomic. We turn to a study of the second step.

It will simplify the notation to assume that $\omega \in F$. Thus $S = F(\alpha)$ is a splitting field for $x^n - u$ and so $F < F(\alpha)$ is a Galois extension. Each $\sigma \in G = G_F(S)$ is uniquely determined by its value on α and

$$\sigma\alpha = \omega^{k(\sigma)}\alpha$$

for some $k(\sigma) \in \mathbb{Z}_n$. Since $\omega \in F$, we have for $\sigma, \tau \in G$

$$(\sigma\tau)\alpha = \sigma(\omega^{k(\tau)}\alpha) = \omega^{k(\tau)}\sigma\alpha = \omega^{k(\tau)}\omega^{k(\sigma)}\alpha$$

Hence, the map $\sigma \mapsto \omega^{k(\sigma)}$ is a group monomorphism from G into U_n and therefore G is isomorphic to a subgroup of U_n. It follows that G is cyclic and if $|G| = [F(\alpha):F] = d$ then $d \mid n$. As the next theorem shows, this actually characterizes cyclic extensions when the base field contains a primitive n-th root of unity.

Theorem 11.1.1 Let F be a field containing a primitive n-th root of unity. The following are equivalent.

1) $F < E$ is cyclic of degree $d \mid n$.
2) $E = F(\alpha)$ where $min(\alpha,F) = x^d - v$, for $v \in F$ and $d \mid n$.
3) E is a splitting field for an irreducible binomial $x^d - v$, where $v \in F$ and $d \mid n$.
4) $E = F(\alpha)$ where α is a root of a binomial $x^n - u$, for $u \in F$.
5) E is a splitting field for a binomial $x^n - u$, for $u \in F$.

Proof. Let us first show that 2) through 5) are equivalent. Since F

contains a primitive d-th root of unity for any $d \mid n$, it is clear that 2) and 3) are equivalent, as are 4) and 5). If 2) holds then since $\alpha^d = v \in F$ and $x^d - \alpha^d$ divides $x^n - \alpha^n$, it follows that α is a root of $x^n - u$ where $u = \alpha^n \in F$. Hence 4) holds. Suppose now that 4) holds. The roots of $x^n - u$ are given by (11.1.1) and since the d roots of $p(x) = min(\alpha,F)$ are among the list (11.1.1), their product, which lies in F, has the form $\omega^e\alpha^d$. Hence $\alpha^d \in F$ and $p(x) = x^d - \alpha^d$. Thus, 2) holds.

We have already shown that 4) implies 1) so it remains to prove that 1) implies 2). Suppose that $F < E$ is cyclic of degree $d \mid n$, with Galois group

$$G = \langle\sigma\rangle = \{\iota,\sigma,\ldots,\sigma^{d-1}\}$$

Note that F contains a primitive d-th root of unity $\xi = \omega_n^{n/d}$. Now, $\alpha^d \in F = F(G)$ if and only if $\sigma\alpha^d = \alpha^d$, which is equivalent to $(\sigma\alpha)^d = \alpha^d$, or

$$\left(\frac{\alpha}{\sigma\alpha}\right)^d = 1 \tag{11.1.2}$$

If we can find an $\alpha \in E$ for which $\alpha/\sigma\alpha = \xi$, then (11.1.2) will hold, we will have $\alpha^d \in F$, whence $x^d - \alpha^d \in F[x]$ and if $p(x) = min(\alpha,F)$ then $p(x) \mid x^d - \alpha^d$. But the roots of p(x) are

$$\alpha,\ \sigma\alpha,\ldots,\sigma^{d-1}\alpha \tag{11.1.3}$$

and since $\sigma\alpha = \xi^{-1}\alpha$, we have $\sigma^k\alpha = \xi^{-k}\alpha$, which implies that the elements (11.1.3) are distinct. Hence, $deg\ p(x) = d$ and so $p(x) = x^d - \alpha^d$ and $E = F(\alpha)$, as desired.

Thus, we are left with finding an $\alpha \in E$ for which $\alpha/\sigma\alpha = \xi$. Since $\xi \in F$, its norm satisfies

$$N_{E/F}(\xi) = \xi^{[E:F]} = \xi^d = 1$$

The proof is then completed by taking $\beta = \xi$ in the following theorem. ∎

Theorem 11.1.2 (Hilbert's Theorem 90) Let $F < E$ be a finite cyclic extension with Galois group $G = \langle\sigma\rangle$. An element $\beta \in E$ has the form

$$\beta = \frac{\alpha}{\sigma\alpha}$$

for some $\alpha \in E^*$ if and only if its norm $N_{E/F}(\beta)$ is equal to 1.

Proof. Let $[E:F] = d$. Suppose that $N_{E/F}(\beta) = 1$. We desire an $\alpha \in E$ for which $\beta(\sigma\alpha) = \alpha$. Consider the maps

$$\tau_0 = \iota, \quad \tau_k = \beta(\sigma\beta)(\sigma^2\beta)\cdots(\sigma^{k-1}\beta)\sigma^k, \quad \text{for } 0 < k \leq d$$

Then

$$\tau_{k+1} = \beta(\sigma\tau_k), \quad \text{for } 0 \leq k \leq d-1$$

Since $\tau_d = N_{E/F}(\beta)\sigma^d = \iota = \tau_0$, the map

$$\tau = \sum_{k=0}^{d-1} \tau_k$$

which is nonzero by the Dedekind Independence Theorem, satisfies $\beta(\sigma\tau) = \tau$. Since $\tau \neq 0$, there exists a nonzero $\gamma \in E$ for which $\tau\gamma \neq 0$ and so $(\beta\sigma)(\tau\gamma) = \tau\gamma$, that is, $\beta = \tau\gamma/\sigma(\tau\gamma)$, whence $\alpha = \tau\gamma$ is the desired element. We leave proof of the converse to the reader. ∎

11.2 Extensions of Degree Char(F)

There is an "additive" version of Theorem 11.1.1 which deals with cyclic extensions of degree equal to $p = \text{char}(F) > 0$, where the role of the binomial $x^n - u$ is played by the polynomial $x^p - x - u$.

Suppose that F is a field of characteristic $p \neq 0$. Let $F < E$ and suppose that $\alpha \in E$ is a root of the polynomial

$$f(x) = x^p - x - u$$

for $u \in F$. Since the prime subfield of F is $\mathbb{Z}_p$, and since $k^p = k$ for any $k \in \mathbb{Z}_p$, the p distinct elements

$$\alpha, \alpha + 1, \ldots, \alpha + p - 1$$

are the roots of f(x). Unlike the previous case, we need no special conditions on F to insure that if an extension of F contains one root of f(x), it contains all the roots of f(x). Hence, $F(\alpha)$ is a splitting field of f(x).

We have two cases to consider. If $\alpha \in F$ then f(x) splits in F. Now suppose that $\alpha \notin F$. Then $p(x) = min(\alpha,F)$ has degree $d > 1$, with roots

$$\alpha, \alpha + e_1, \ldots, \alpha + e_{d-1}$$

where $0 \leq e_i \leq p - 1$. The sum of these roots is $d\alpha + k$, for some integer k, and since this number lies in F but $\alpha \notin F$, we must have $d = p$, whence $f(x) = min(\alpha,F)$ is irreducible. In short, f(x) either splits in F or is irreducible over F with splitting field $F(\alpha)$, for any root α of f(x).

Since $F(\alpha)$ is a splitting field for the separable polynomial $f(x) =$

$x^p - x - u$, we deduce that $F < F(\alpha)$ is Galois. If $f(x)$ is irreducible over F and $G = G_F(F(\alpha))$, there exists a $\sigma \in G$ for which $\sigma\alpha = \alpha + 1$. Since $\sigma^i\alpha = \alpha + i$, it follows that $G = \langle\sigma\rangle = \{\iota,\sigma,\ldots,\sigma^{p-1}\}$ is the cyclic group generated by σ.

Theorem 11.2.1 (Artin–Schreier) Let $\mathrm{char}(F) = p \neq 0$. The polynomial $f(x) = x^p - x - u$ either splits in F or is irreducible over F. Moreover, the following are equivalent.

1) $F < E$ is cyclic of degree p.
2) $E = F(\alpha)$ where $min(\alpha,F) = x^p - x - u$, for $u \in F$.
3) E is a splitting field for the irreducible polynomial $x^p - x - u$, where $u \in F$.

Proof. It is clear that 2) and 3) are equivalent and we have seen that 2) implies 1). To prove that 1) implies 2), suppose that $F < E$ is cyclic of degree p, with Galois group $G = \langle\sigma\rangle = \{\iota,\sigma,\ldots,\sigma^{p-1}\}$. Then $\alpha^p - \alpha \in F$ if and only if

$$\sigma(\alpha^p - \alpha) = \alpha^p - \alpha$$

or, equivalently,

$$(\sigma\alpha - \alpha)^p = \sigma\alpha - \alpha$$

Hence, if we find an $\alpha \in E$ for which $\sigma\alpha - \alpha = 1$ then $\alpha^p - \alpha \in F$. Moreover, $\sigma\alpha = \alpha + 1$ and so $\sigma^i\alpha = \alpha + i$, which implies that the roots of $min(\alpha,F)$ are the distinct values

$$\alpha,\ \alpha + 1,\ldots,\alpha + p - 1$$

It follows that

$$min(\alpha,F) = x^p - x - (\alpha^p - \alpha)$$

and hence that $[F(\alpha):F] = [E:F]$ and $E = F(\alpha)$. Since $\mathrm{Tr}_{E/F}(-1) = 0$, the proof is completed by taking $\beta = -1$ in the additive version of Hilbert's Theorem 90 given below. ∎

Theorem 11.2.2 (Hilbert's Theorem 90, Additive Version) Let $F < E$ be a finite cyclic extension with Galois group $G = \langle\sigma\rangle$. An element $\beta \in E$ has the form $\beta = \alpha - \sigma\alpha$ for some $\alpha \in E$ if and only if $\mathrm{Tr}_{E/F}(\beta) = 0$.

Proof. Let $[E:F] = n$ and consider the map

$$\tau = \beta\sigma + [\beta+(\sigma\beta)]\sigma^2 + \cdots + [\beta+(\sigma\beta)+\cdots+(\sigma^{n-2}\beta)]\sigma^{n-1}$$

It is easy to verify that $\tau - \sigma\tau = \beta(\iota + \sigma + \cdots + \sigma^{n-1})$ and so if

$Tr_{E/F}(\gamma) = 1$ for some $\gamma \in E$ (such a γ must exists since $F < E$ is finite and separable and so the trace map is not the zero map) then

$$\tau\gamma - \sigma\tau\gamma = \beta Tr_{E/F}(\gamma) = \beta$$

Thus, $\alpha = \tau\gamma$ is the desired element. ∎

In this section and the previous one, we have discussed cyclic extensions of degree n where (n,expchar(F)) = 1 or $n = p = char(F) \neq 0$. A discussion of cyclic extensions of degree $n = p^k$ for $k > 1$ is quite a bit more involved (requiring a discussion of so-called *Witt vectors*) and thus falls beyond the intended scope of this book. The interested reader may wish to consult the books by Karpilovsky (1989) or Lang (1993).

Exercises

1. Let $F < E$ be cyclic of degree n, with Galois group $G = \langle\sigma\rangle$. If $\beta \in E$ has the form $\beta = \alpha/\sigma\alpha$ for some $0 \neq \alpha \in E$, show that $N_{E/F}(\beta) = 1$.
2. Let $F < E$ be cyclic of degree p^n where p is a prime. Let $F < K < E$ with $F < K$ cyclic of degree p^d where $d < n$. Let $F < L < E$ and suppose that $E = KL$. Show that $E = L$.
3. Let $char(F) = p \neq 0$ and let $F(\alpha_1) = F(\alpha_2)$ be cyclic of degree p over F, where $min(\alpha_i,F) = x^p - x - u_i$. Show that $\alpha_2 = n\alpha_1 + b$ where $b \in F$ and $0 < n \leq p-1$.
4. Let F be a field and let E be the extension of F generated by the n-th roots of unity, for *all* $n \geq 1$. Show that $F < E$ is abelian.
5. Let E be a field and let σ be an automorphism of E of order d. Suppose that $\beta \in E$ has the property that $\sigma\beta = \beta$ and $\beta^d = 1$. Prove that there exists an $\alpha \in E$ such that $\sigma\alpha = \alpha\beta$.
6. Let E be a field and let σ be an automorphism of E of order $d > 1$. Show that there exists an $\alpha \in E$ such that $\sigma\alpha = \alpha + 1$.
7. Let $F < E$ be finite and abelian. Show that $E = F_1 \cdots F_m$ is the composite of fields F_i such that $F < F_i$ is cyclic of prime power degree. Thus, the study of finite abelian extensions reduces to the study of cyclic extensions of prime power degree.
8. Let F be a field containing the n-th roots of unity. Let $\overline{F}$ be an algebraic closure of F. Show that if $\alpha \in \overline{F}$ is separable over F and if α is a root of the binomial $x^n - u$ with $u \in F$, then $F < F(\alpha)$ is cyclic of degree $d \mid n$.

Chapter 12
Solvable Extensions

We now turn to the question of when an arbitrary polynomial equation $p(x) = 0$ is *solvable by radicals.* Loosely speaking, this means (for $\text{char}(F) = 0$) that we can reach the roots of $p(x)$ by a finite process of adjoining n-th roots of existing elements, that is, by a finite process of passing from a field K to a field $K(\alpha)$, where α is a root of a binomial $x^n - u$, with $u \in K$. We begin with some basic facts about solvable groups.

12.1 Solvable Groups

Definition A **normal series** in a group G is a tower of subgroups

$$\{\epsilon\} = G_0 < G_1 < G_2 < \cdots < G_n = G$$

where $G_i \triangleleft G_{i+1}$. A normal series is **abelian** if each factor group G_{i+1}/G_i is abelian, and **cyclic** if each factor group is cyclic. □

Definition A group is **solvable** (or **soluble**) if it has an abelian normal series. □

Theorem 12.1.1 The following are equivalent for a nontrivial finite group G.

1) G has an abelian normal series.
2) G has a cyclic normal series.

3) G has a normal series in which each factor group G_{i+1}/G_i is cyclic of prime order.

Proof. It is clear that 3)⇒2)⇒1). Thus, we need only prove that 1)⇒3). Let $\{G_i\}$ be an abelian normal series. We wish to refine this series by inserting subgroups until all quotients have prime order. The Correspondence Theorem (Theorem 0.2.15) says that the natural projection $\pi: G_{i+1} \to G_{i+1}/G_i$ is a normality-preserving bijection from the subgroups of G_{i+1} containing G_i to the subgroups of G_{i+1}/G_i. Hence, by Cauchy's Theorem, if a prime p divides $o(G_{i+1}/G_i)$ then G_{i+1}/G_i has a subgroup of order p, which must have the form H_i/G_i for $G_i < H_i < G_{i+1}$.

Since G_{i+1}/G_i is abelian, $H_i/G_i \lhd G_{i+1}/G_i$, whence $H_i \lhd G_{i+1}$. Since $G_i \lhd G_{i+1}$, we also have $G_i \lhd H_i$. Thus, $G_i \lhd H_i \lhd G_{i+1}$. Note also that H_i/G_i is abelian and, by the Third Isomorphism Theorem,

$$G_{i+1}/H_i \simeq \frac{G_{i+1}/G_i}{H_i/G_i}$$

is the quotient of an abelian group and is therefore also abelian.

Thus, we have refined the original abelian normal series by introducing H_i, where H_i/G_i has prime order. Since G is a finite group, we may continue the refinement process until we have an abelian normal series, each of whose quotient groups has prime order. ∎

The next theorem gives some basic properties of solvable groups. The proofs of all but statement 2) can be found in standard texts on group theory.

Theorem 12.1.2

1) Any finitely generated abelian group is solvable.
2) (Feit-Thompson) Any finite group of odd order is solvable.
3) Any subgroup of a solvable group is solvable.
4) If $H \lhd G$ then G is solvable if and only if H and G/H are solvable.
5) Any homomorphic image of a solvable group is solvable.
6) The direct product of a finite number of solvable groups is solvable.
7) The symmetric group S_n is solvable if and only if $n \leq 4$. □

12.2 Solvable Extensions

Although the upcoming results can be proved in the context of arbitrary finite extensions, we shall restrict our attention to separable

extensions. As the reader knows, this produces no loss of generality for fields of characteristic 0 or finite fields.

Definition A finite separable extension $F < E$ is **solvable** if there exists a field S for which $F < E < S$, where $F < S$ is Galois and has a solvable Galois group $G_F(S)$. □

Theorem 12.2.1

1) If $F < E$ is solvable, then there exists a field S such that $F < E < S$ where $F < S$ is finite, Galois and solvable.
2) A finite Galois extension $F < E$ is solvable if and only if the Galois group $G_F(E)$ is solvable.
3) If $F < E$ is solvable and E^{nc} is the normal closure of E over F then $F < E^{nc}$ is solvable.

Proof. Let $F < E$ be solvable and let S be the field mentioned in the definition. Since $F < S$ is normal, we have $F < E < E^{nc} < S$. By Theorem 4.5.2, the separability of $F < E$ implies that $F < E^{nc}$ is Galois. Moreover,

$$G_F(E^{nc}) \simeq \frac{G_F(S)}{G_{E^{nc}}(S)}$$

is solvable and so $F < E^{nc}$. This proves part 3). Theorem 2.9.6 implies that if $F < E$ is finite then so is $F < E^{nc}$ and so part 1) is proved. Finally, if $F < E$ is finite, Galois and solvable then $E^{nc} = E$ and part 3) implies part 2). The converse is obvious. ∎

In view of part 1) of the previous theorem, we may always assume that the field S in the definition of solvable is a finite extension of F.

Theorem 12.2.2 The class of solvable extensions is distinguished.

Proof. Suppose first that $F < E$ is solvable and $F < K$ is arbitrary. Then there exists a field S such that $F < E < S$ with $F < S$ finite, Galois and $G_F(S)$ solvable. Hence, $K < SK$ is finite and Galois. Since $G_K(SK)$ is isomorphic to $G_{K \cap S}(S)$, which is a subgroup of $G_F(S)$, it too is solvable. Hence $K < EK$ is solvable.

Suppose now that $F < E$ is solvable and $F < K < E$. Hence, there exists an S such that $F < K < E < S$ where $F < S$ is finite and Galois and $G_F(S)$ is solvable. It follows that $K < S$ is Galois and since $G_K(S)$ is a subgroup of $G_F(S)$, the former is solvable, whence $K < E$ is solvable. It is evident that $F < K$ is solvable.

Suppose now that $F < K < E$ with $F < K$ and $K < E$ solvable and consider Figure 12.2.1.

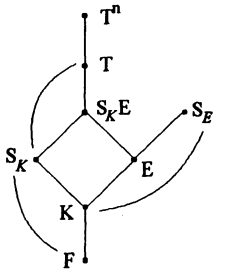

Figure 12.2.1

Since $F < K$ is solvable there exists S_K such that $F < K < S_K$ where $F < S_K$ is finite, Galois and $G_F(S_K)$ is solvable. Similarly, since $K < E$ is solvable, there exists a field S_E such that $K < E < S_E$ where $K < S_E$ is finite, Galois and $G_K(S_E)$ is solvable. Since $K < E$ is solvable, the lifting $S_K < S_K E$ is solvable and so there exists a field T such that $S_K < S_K E < T$ where $S_K < T$ is finite, Galois and

$$G_{S_K}(T)$$

is solvable.

If $F < T$ was normal, our problems would be quickly solvable, but it need not be. Thus, we turn to the normal closure T^{nc} of T over F. Since $F < T$ is finite and separable, it follows that $F < T^{nc}$ is finite and Galois. Recall that $T^{nc} = \vee \sigma T$, for all $\sigma \in Hom_F(T,\overline{T})$ and since

$$| \operatorname{Hom}_F(T,\overline{T}) | = [T:F]_s$$

is finite, this composite is a finite one. For each $\sigma \in Hom_F(T,\overline{T})$, the map $\sigma: T \to \sigma T$ is an F-automorphism. The normality of $F < S_K$ implies that $\sigma S_K = S_K$ and since $S_K < T$ is Galois and $G_{S_K}(T)$ solvable, it follows that $S_K < \sigma T$ is Galois and $G_{S_K}(\sigma T)$ is solvable.

According to Theorem 5.5.3, the extension $S_K < T^{nc}$ is Galois and $G_{S_K}(T^{nc})$ is isomorphic to a subgroup of the product $\prod G_{S_K}(\sigma T)$ and since this is a finite product, it is solvable. Finally, since

$$G_F(S_K) \simeq \frac{G_F(T^{nc})}{G_{S_K}(T^{nc})}$$

and both $G_F(S_K)$ and $G_{S_K}(T^{nc})$ are solvable, so is $G_F(T^{nc})$, whence $F < E$ is solvable. ∎

12.3 Solvability by Radicals

Loosely speaking, when $\text{char}(F) = 0$, an extension $F < E$ is *solvable by radicals* if it is possible to reach E from F by adjoining a finite sequence of n-th roots of existing elements. More specifically, we have the following definitions, which also deal with the case where $\text{char}(F) \neq 0$.

Definition Let $\text{expchar}(F) = p$ and let $F < R$. A **radical series** for $F < R$ is a tower of fields

$$F = R_0 < R_1 < \cdots < R_n = R$$

such that each step $R_i < R_{i+1}$ is one of the following types:

Type 1: $R_{i+1} = R_i(\beta_i)$ where β_i is an r_i-th root of unity.

Type 2: $R_{i+1} = R_i(\alpha_i)$ where α_i is a root of $x^{r_i} - u_i$, with $1 \neq u_i \in R_i$ and $(r_i,p) = 1$.

Type 3: (For $p > 1$ only) $R_{i+1} = R_i(\alpha_i)$ where α_i is a root of $x^p - x - u_i$, with $u_i \in R_i$.

For steps of types 1 and 2, the number r_i is the **exponent** of the step. The **exponent** of a type 3 step is p. □

Note that if $\text{expchar}(F) = p \neq 1$ and β is an r-th root of unity where $r = mp^e$ and $(m,p) = 1$ then β is also an m-th root of unity. Hence, we may assume that in a type 1 extension, the exponent r_i is relatively prime to the characteristic p.

Note also that lifting a radical series gives another radical series with the same type steps, for if $R_{i+1} = R_i(\alpha)$, where α is a root of $f(x) \in R_i[x]$, then

$$KR_{i+1} = (KR_i)(\alpha)$$

where α is a root of $f(x) \in (KR_i)[x]$.

Definition A **radical extension** is a finite separable extension $F < R$ that has a radical series. A finite separable extension $F < E$ is **solvable by radicals** if there exists a radical extension $F < R$ containing E, that is, $F < E < R$. □

Theorem 12.3.1 The class of extensions that are solvable by radicals is distinguished. If $F < E$ is solvable by radicals then so is $F < E^{nc}$ where E^{nc} is the normal closure of E over F.

Proof. Let $F < E$ be solvable by radicals, with associated radical series $\{R_i\}$. Thus, $F < E < R$. Let $F < K$ be any extension. Lifting the series by K gives a radical series $\{KR_i\}$ from K to KR containing KE, whence $K < KE$ is solvable by radicals.

Now let $F < K < E$ with $F < K$ and $K < E$ solvable by radicals. Let $\{R_i\}$ be the radical series for $F < R$ containing K and let $\{S_i\}$ be a radical series for $K < S$ containing E. We lift the series $\{S_i\}$ by R to get a radical series $\{RS_i\}$ for $RK < RS$ containing RE. Since $RK = K$, the series $\{R_i\}$, followed by the series $\{RS_i\}$, is a radical series for $F < RS$ containing EK. Thus, $F < EK$ is solvable by radicals.

If $F < K < E$ and $F < E$ is solvable by radicals then *a fortiori* $F < K$ is solvable by radicals. If $\{R_i\}$ is a radical series for $F < R$ containing E then $\{KR_i\}$ is a radical series for $K < KR$ containing $KE = E$, whence $K < E$ is solvable by radicals.

For the last statement, let $F < E < R$ where $F < R$ is radical. Let $\sigma \in \mathrm{Hom}_F(E,\overline{E})$. Since $E < R$ is algebraic, we may extend σ to $\overline{\sigma} \in \mathrm{Hom}_F(R,\overline{E})$. Since $\overline{\sigma}:R \to \overline{\sigma}(R)$ is an F-isomorphism if $\{R_i\}$ is a radical series for $F < R$ then $\{\overline{\sigma}R_i\}$ is a radical series for $F < \overline{\sigma}R$ containing σE. Hence, $F < \sigma E$ is also solvable by radicals. Since $E^{nc} = \vee \sigma E$ is a finite composite, it follows that $F < E^{nc}$ is solvable by radicals. ∎

Now we come to the key result that links the concepts of solvable extension and solvability by radicals.

Theorem 12.3.2 A finite separable extension $F < E$ is solvable by radicals if and only if it is solvable.

Proof. Suppose first that $F < E$ is solvable. Let S be a field for which $F < E < S$ where $F < S$ is finite, Galois and $G = G_F(S)$ is solvable. Thus, there is a normal series decomposition

$$\{\epsilon\} = G_0 < G_1 < G_2 < \cdots < G_n = G \tag{12.3.1}$$

where $G_i \triangleleft G_{i+1}$ and G_{i+1}/G_i is cyclic of prime order r_i dividing $|G|$. Taking fixed fields gives

$$F = F(G) < F(G_{n-1}) < \cdots < F(G_0) < F(\{\epsilon\}) = S \tag{12.3.2}$$

Unfortunately, since the appropriate roots of unity may not lie in these fields, we cannot apply the relevant theorems (11.1.1 and 11.2.1) of the previous chapter to conclude that this is a radical series. Hence, we first adjoin the necessary r_i-th roots of unity.

If $G_i < G_{i+1}$ is a step in the series (12.3.1) then the corresponding step in (12.3.2) has prime degree

$$r_i = [F(G_i):F(G_{i+1})]$$

dividing [S:F]. So let

$$[S:F] = n = mp^e$$

where $p = \text{expchar}(F)$ and $(m,p) = 1$ and let ω be a primitive m-th root of unity. If we show that $F(\omega) < S(\omega)$ is solvable by radicals then since $F < F(\omega)$ is a type 1 extension, it follows that $F < S(\omega)$ is solvable by radicals and therefore so is $F < S$. Since $F(\omega) < S(\omega)$ is a lifting of the finite, solvable Galois extension $F < S$ by $F(\omega)$, it is also finite, solvable and Galois. Note also that $[S(\omega):F(\omega)] \mid [S:F]$ and so if $r \neq p$ is any prime dividing $[S(\omega):F(\omega)]$, then $r \mid m$ and so $F(\omega)$ contains a primitive r-th root of unity.

Thus, the extension $F(\omega) < S(\omega)$ is finite, Galois and solvable and $F(\omega)$ contains a primitive r-th root of unity for any prime $r \neq p$ that divides $[S(\omega):F(\omega)]$. We need to show that $F(\omega) < S(\omega)$ is solvable by radicals. In view of this, we may as well assume to begin with that F contains a primitive r-th root of unity for any prime $r \neq p$ dividing [S:F].

Referring to Equation (12.3.2), consider the Galois correspondence on the finite Galois extension $F(G_{i+1}) < S$. Since $F(G_i)$ is an intermediate field and $G_i \lhd G_{i+1}$, Theorem 5.4.1 implies that $F(G_{i+1}) < F(G_i)$ is Galois and

$$G_{F(G_{i+1})}(F(G_i)) \simeq G_{i+1}/G_i$$

which is cyclic of prime order r_i dividing [S:F]. To simplify the notation, let

$$F(G_{i+1}) = L, \quad F(G_i) = M \quad \text{and} \quad r_i = r$$

Then $G_L(M)$ is cyclic of prime order r dividing mp^e.

If $r = p$, Theorem 11.2.1 implies that there exists an $\alpha \in M$ for which $M = L(\alpha)$, where α is a root of $x^p - x - u$ for some $u \in L$. Thus, $L < M$ is an extension of type 3. If $r \neq p$ then $r \mid m$ and so L contains a primitive r-th root of unity. Theorem 11.1.1 then implies that $M = L(\alpha)$, where α is a root of $x^r - u$ for some $u \in L$. Hence, $L < M$ is an extension of type 2. Thus, each step in the tower (12.3.2) is of type 2 or type 3 and we conclude that $F < S$ is solvable by radicals, as desired.

For the converse, suppose that $F < E$ is solvable by radicals. Then $F < E^{nc}$ is Galois and solvable by radicals. Let

$$F = R_0 < R_1 < \cdots < R_n = R$$

be a radical series for $F < R$ containing E^{nc}. We wish to adjoin appropriate roots of unity, lifting the series to one in which each step is cyclic. Then, by tacking on a front end, we get a series with cyclic steps that begins with F and goes past E.

Let r be the least common multiple of all of the exponents in the series $\{R_i\}$ and let ω be a primitive r-th root of unity. If $R_i < R_i(\alpha_i)$ is a step of type 1, then α_i is an r_i-th root of unity where $r_i \mid r$ and so $R_i(\alpha_i,\omega) = R_i(\omega)$. Hence, lifting $\{R_i\}$ to $\{R_i(\omega)\}$ eliminates all steps of type 1. (We remove any trivial steps of degree 1.)

If $R_i < R_i(\alpha_i)$ is a step of type 2, then α_i is a root of $x^{r_i} - u_i$ and since $R_i(\omega)$ contains a primitive r_i-th root of unity, Theorem 11.1.1 implies that $R_i(\omega) < R_i(\omega,\alpha_i)$ is cyclic. Finally, Theorem 11.2.1 guarantees that if $R_i < R_{i+1}$ is of type 3, then $R_i(\omega) < R_{i+1}(\omega)$ is cyclic.

Thus, each step in the tower

$$F < F(\omega) = R_0(\omega) < \cdots < R_n(\omega) = R(\omega)$$

is abelian, all steps after the first one being cyclic. Taking Galois groups gives a series

(12.3.3)

$$\{\epsilon\} = G_{R(\omega)}(R(\omega)) < G_{R_n(\omega)}(R(\omega)) < \cdots < G_{R_0(\omega)}(R(\omega)) < G_F(R(\omega))$$

Since $R_i < R_{i+1}$ is normal, so is $R_i(\omega) < R_{i+1}(\omega)$ and so

$$G_{R_{i+1}(\omega)}(R(\omega)) \triangleleft G_{R_i(\omega)}(R(\omega))$$

and the quotient group is

$$\frac{G_{R_i(\omega)}(R(\omega))}{G_{R_{i+1}(\omega)}(R(\omega))} \simeq G_{R_i(\omega)}(R_{i+1}(\omega))$$

which is abelian. Thus, Equation (12.3.3) is an abelian normal series for $G_F(R(\omega))$ and so $F < R(\omega)$ is solvable. Hence, $F < R$ is solvable. ∎

12.4 Polynomial Equations

The initial motivating force behind Galois theory was the solution of polynomial equations $f(x) = 0$. Perhaps the crowning achievement of Galois theory is the statement, often phrased as follows: there is no

formula, similar to the quadratic formula, for solving polynomial equations of degree 5 or greater over $\mathbf{Q}$. However, this is not the whole story. The fact is that, for some polynomial equations, there is a formula and for others there is not and, moreover, we can tell by looking at the Galois group of the polynomial whether or not there is such a formula. In fact, there are even algorithms for solving polynomial equations when they are "solvable," but these algorithms are unfortunately not practical.

Let us restrict attention to fields of characteristic 0. We refer to the four basic arithmetic operations (addition, subtraction, multiplication and division) and the taking of n-th roots as the **five basic operations.**

Let C be a field. We will say that an element $\alpha \in \overline{C}$ is **obtainable by formula from C** if we can obtain α by applying a finite sequence of any of the five basic operations, to a finite set of elements from C.

Suppose we can obtain any element from the field K by formula from C. Applying any of the four basic arithmetic operations to the elements of K gets us nothing new. However, taking an n-th root of an element $\alpha \in K$ gives us access to *all* elements of $L = K(\sqrt[n]{\alpha})$, since any element of L is a polynomial in $\sqrt[n]{\alpha}$ over K. Hence, repeated use of the five basic operations allows us to obtain any element lying within any finite tower of the form

$$C = F_0 < F_1 < F_2 < \cdots < F_n \tag{12.4.1}$$

where $F_{i+1} = F_i(\alpha_i)$, with α_i a root of a binomial $x^{n_i} - u_i$ over F_i. Since we are assuming that char(F) = 0, the tower (12.4.1) is just a radical series for $C < F_n$. Hence, we can obtain by formula any element in any radical extension $C < R$ of C.

On the other hand, let $\alpha \in R$ where Equation (12.4.1) is a radical series for $C < R$. Then $\alpha \in F_i = F_{i-1}(\alpha_i)$, where $\alpha_i = \sqrt[n]{u_{i-1}}$, with $u_{i-1} \in F_{i-1}$. Since α is a polynomial in α_i over F_{i-1}, it follows that α can be obtained by formula from F_{i-1}. It is now clear that any element of R can be obtained by formula from C.

Theorem 12.4.1 Let C be a field of characteristic 0. An element $\alpha \in C$ can be obtained by formula from C if and only if α lies in a radical extension of C, that is, if and only if $C < C(\alpha)$ is solvable by radicals. □

Let us say that a root α of a polynomial $f(x) = a_0 + a_1x + \cdots + a_dx^d$ over F is **obtainable by formula** if we can obtain α by formula from $C = \mathbf{Q}(a_0, \ldots, a_d)$. Thus, a root α of f(x) is obtainable by formula if and only if $C < C(\alpha)$ is solvable by radicals. Theorems 12.3.1 and 12.3.2 now imply the following.

Theorem 12.4.2 Let $\text{char}(F) = 0$ and let $f(x) = a_0 + a_1x + \cdots + a_dx^d$ be a polynomial over F.

1) The roots of f(x) are obtainable by formula if and only if the extension $C < S$ is solvable, where $C = \mathbf{Q}(a_0, \ldots, a_d)$ and S is the splitting field for f(x) over C.
2) Let f(x) be irreducible over F. One root of f(x) is obtainable by formula if and only if all roots of f(x) are obtainable by formula. □

According to Theorem 10.5.7, for any prime number p, there exists a polynomial $f_p(x)$ of degree p over $\mathbf{Q}$ whose Galois group is isomorphic to S_p. Hence $f_p(x)$ is irreducible and since the group S_p is not solvable for $p \geq 5$, Theorem 12.4.2 implies that if $p \geq 5$, then *none* of the roots of $f_p(x)$ can be obtained by formula. Although it is much harder to show, this also holds for any positive integer n [see Hadlock, 1987]. Thus, we have the following.

Theorem 12.4.3 For any $n \geq 5$, there is an irreducible polynomial of degree n over $\mathbf{Q}$ none of whose roots are obtainable by formula. □

As a consequence, for any $n \geq 5$, there is no formula, similar to the quadratic formula, for the roots of any polynomial of degree n. More specifically, we have

Corollary 12.4.4 Let $n \geq 5$ and consider the generic polynomial $p(x) = y_0 + y_1x + \cdots + y_nx^n$, where $y_0, \ldots, y_n$ are algebraically independent over $\mathbf{Q}$. Then there is no algebraic formula, involving only the five basic operations, the elements of $\mathbf{Q}$ and the variables $y_0, \ldots, y_n$, with the property that, for any polynomial $f(x) = a_0 + a_1x + \cdots + a_nx^n$ of degree n over F, we can get a root of f(x) by replacing y_i in the formula by a_i, for all $i = 0, \ldots, n$. □

Exercises

1. Prove that if $H \triangleleft G$ then G is solvable if and only if H and G/H are solvable.
2. Prove that if $F < E$ is solvable by radicals and $\sigma \in \text{Hom}_F(E, \overline{E})$ then $F < \sigma E$ is also solvable by radicals.
3. Calculate the Galois group of the polynomial $f(x) = x^5 - 4x + 2$. Is there a formula for the roots?
4. Prove that if f(x) is a polynomial of degree n over F with Galois group isomorphic to S_n then f(x) is irreducible over F.
5. A finite separable extension $F < E$ of characteristic p is solvable by radicals if and only if there exists a finite extension $F < R$ with

$F < E < R$ and a radical series $\{R_i\}$ for $F < R$ in which each step $R_i < R_{i+1}$ is one of the following types: (1) $R_{i+1} = R_i(\omega_i)$ where ω_i is an r_i-th root of unity with r_i prime and $r_i \neq p$. (2) $R_{i+1} = R_i(\alpha_i)$ where α_i is a root of $x^r - u$, with $u \in R_i$, r prime and $r \neq p$. (3) (If $p > 0$ only) $R_{i+1} = R_i(\beta_i)$ where β_i is a root of the irreducible polynomial $x^p - x - u$, with $u \in R_i$.

6. Prove Theorem 12.4.2. *Hint*: for part 2), consider the normal closure of $C(\alpha)$, where α is an obtainable root of $f(x)$.
7. Let $f(x)$ be an irreducible cubic over $\mathbb{Q}$ with three real roots. Show that no root of $f(x)$ can be obtained by formula if we allow only *real* n-th roots. (That is, no root of $f(x)$ is contained in a radical series whose fields are subfields of $\mathbb{R}$.) *Hint*: Use the fact that the splitting field for $f(x)$ over $\mathbb{Q}$ is given by $\mathbb{Q}(\sqrt{\Delta}, r)$, where r is a root of $f(x)$ and Δ is the discriminant.

Chapter 13
Binomials

We continue our study of binomials by determining conditions that characterize irreducibility and describing the Galois group of a binomial $x^n - u$ in terms of 2×2 matrices over $\mathbb{Z}_n$. We then consider an application of binomials to determining the irrationality of linear combinations of radicals. Specifically, we prove that if $p_1, \ldots, p_m$ are distinct prime numbers, then the degree of

$$\mathbb{Q}(\sqrt[n]{p_1}, \ldots, \sqrt[n]{p_m})$$

over $\mathbb{Q}$ is as large as possible, namely, n^m. This implies that the set of all products of the form

$$\sqrt[n]{p_1^{e(1)}}\ \sqrt[n]{p_2^{e(2)}} \cdots \sqrt[n]{p_m^{e(m)}}$$

where $0 \leq e(i) \leq n-1$, is linearly independent over $\mathbb{Q}$. For instance, the numbers

$$1, \quad \sqrt[4]{3} = \sqrt[60]{3^{15}}, \quad \sqrt[5]{4} = \sqrt[60]{2^{24}} \quad \text{and} \quad \sqrt[6]{72} = \sqrt[60]{2^{30}3^{20}}$$

are of this form, where $p_1 = 2$, $p_2 = 3$. Hence, any expression of the form

$$a_1\sqrt[4]{3} + a_2\sqrt[5]{4} + a_3\sqrt[6]{72}$$

where $a_i \in \mathbb{Q}$, must be irrational, unless $a_i = 0$ for all i.

First, a bit of notation. If $u \in F$, then $u^{1/n}$ stands for a particular (fixed) root of $x^n - u$. The set of primitive n-th roots of unity is denoted

by Ω_n and ω_k always denotes a primitive k-th root of unity.

13.1 Irreducibility

Let us first recall a few facts about the norm. Let $F < E$ be finite with $\alpha \in E$. If the minimal polynomial of α

$$min(\alpha,F) = x^d + a_{d-1}x^{d-1} + \cdots + a_0$$

has roots $r_1,\ldots,r_d$ then

$$N(\alpha) = \prod_{i=1}^{d} r_i = (-1)^d a_0$$

where $N = N_{F(\alpha)/F}$. Note that $N(\alpha) \in F$. Also, for all $\beta \in F(\alpha)$ and $a \in F$, we have

1) $N(\beta^n) = N(\beta)^n$, n a positive integer,

2) $N(a\beta) = a^d N(\beta)$,

3) $N(a) = a^d$.

We begin with Lemma 4.7.6, restated here for convenience.

Lemma 13.1.1 If $\mathrm{char}(F) = p \neq 0$ and $u \in F$, $u \notin F^p$ then $x^{p^k} - u$ is irreducible for every $k \geq 1$.

Proof. If β is a root of $f(x) = x^{p^k} - u$ then, in a splitting field,

$$f(x) = (x - \beta)^{p^k}$$

Since $p(x) = min(\beta,F)$ divides $f(x)$, we have $p(x) = (x - \beta)^{p^d}$ for some $d \leq k$. Since the constant term β^{p^d} of $p(x)$ lies in F, if $d \leq k - 1$ we get

$$u = \beta^{p^k} = (\beta^{p^{k-1}})^p \in F^p$$

contrary to assumption. Hence $d = k$ and $f(x) = p(x)$ is irreducible. ∎

We turn next to primes different from $\mathrm{char}(F)$.

Lemma 13.1.2 Let p be a prime different from $\mathrm{char}(F)$. If $u \in F$, $u \notin F^p$ then $x^p - u$ is irreducible over F. Thus, $x^p - u$ is irreducible over F if and only if it has no roots in F.

Proof. Assume that $u \notin F^p$ and let α be a root of $x^p - u$ with

$[F(\alpha):F] = d \leq p$. Since $\alpha^p = u$, applying the norm $N = N_{F(\alpha)/F}$ gives

$$[N(\alpha)]^p = N(\alpha^p) = N(u) = u^d$$

Letting $N(\alpha) = v \in F$ gives $v^p = u^d$. If $p < d$ then $(d,p) = 1$ and there exist integers a and b for which $ad + bp = 1$. Hence

$$u = u^{ad+bp} = u^{ad}u^{bp} = v^{ap}u^{bp} = (v^a u^b)^p \in F^p$$

a contradiction. Thus $p = d$ and $x^p - u = \mathit{min}(\alpha,F)$ is irreducible. The second statement follows from the first. ∎

For $p \neq 2$, the previous result (and its proof) extends more or less directly to prime powers p^k, that is, if $u \notin F^p$ then

$$x^{p^k} - u$$

is irreducible over F. However, the case $p = 2$ is not quite as simple. Since for any nonzero $b \in \mathbb{Q}$, we have $-4b^4 \notin \mathbb{Q}^2$ but

$$x^{4m} + 4b^4 = (x^{2m} + 2bx^m + 2b^2)(x^{2m} - 2bx^m + 2b^2)$$

is reducible for all $m \geq 1$, we must at least include the restriction (for $4 \mid p^k$) that u cannot have the form $-4b^4$ for any $b \in F$, that is, $u \notin -4F^4$. It turns out that no further restrictions are needed.

Lemma 13.1.3 Let p be a prime, k a positive integer and $u \in F$. If $u \notin F^p$ and if $u \notin -4F^4$ when $4 \mid p^k$, then

$$f(x) = x^{p^k} - u$$

is irreducible over F.

Proof. If $p = \text{char}(F)$, the result follows from Lemma 13.1.1, so assume that $p \neq \text{char}(F)$. We proceed by induction on k. Lemma 13.1.2 shows that the result is true for $k = 1$ and hence that $x^p - u$ is irreducible over F. Assume the result is true for any positive integer less than $k \geq 2$. Let β be a root of f(x). In a splitting field, we have

$$x^p - u = (x - \alpha_1)(x - \alpha_2)\cdots(x - \alpha_p)$$

Hence

$$f(x) = x^{p^k} - u = (x^{p^{k-1}} - \alpha_1)(x^{p^{k-1}} - \alpha_2)\cdots(x^{p^{k-1}} - \alpha_p)$$

Thus β is a root of one of the binomial factors, say

$$g(x) = x^{p^{k-1}} - \alpha$$

where $\alpha = \alpha_i$ for some i. Since $\alpha = \beta^{p^{k-1}}$, we have the tower

$$F < F(\alpha) < F(\beta)$$

where $[F(\alpha):F] = p$. If g(x) is irreducible over $F(\alpha)$, it will follow that $[F(\beta):F(\alpha)] = p^{k-1}$ and so $[F(\beta):F] = p^k$, whence $f(x) = min(\beta,F)$, which is irreducible. We must now consider a few cases.

Case 1: $p \neq 2$. To show that g(x) is irreducible over $F(\alpha)$, we verify that $\alpha \notin F(\alpha)^p$. Suppose to the contrary that $\alpha = \gamma^p \in F(\alpha)^p$ for some $\gamma \in F(\alpha)$. Since $min(\alpha,F) = x^p - u$, applying the norm $N = N_{F(\alpha)/F}$ gives

$$-u = (-1)^p N(\alpha) = (-1)^p N(\gamma^p) = (-1)^p [N(\gamma)]^p$$

Since p is odd, we get $u = [N(\gamma)]^p \in F^p$, contrary to assumption. Hence $\alpha \notin F(\alpha)^p$, g(x) is irreducible over $F(\alpha)$ and f(x) is irreducible over F.

Case 2: $p = 2$. If $\alpha \notin F(\alpha)^2$ and $\alpha \notin -4F(\alpha)^4$, then the induction hypothesis shows that g(x) is irreducible over $F(\alpha)$, so we need to consider two subcases.

Case 2a: $p = 2$, $\alpha = \gamma^2 \in F(\alpha)^2$ for some $\gamma \in F(\alpha)$.

We show directly that f(x) is irreducible over F. If $N = N_{F(\alpha)/F}$ then since $min(\alpha,F) = x^2 - u$, the usual norm computation gives

$$-u = (-1)^2 N(\alpha) = N(\gamma^2) = [N(\gamma)]^2$$

Setting $N(\gamma) = b \in F$ gives $-u = b^2 \in F^2$. Since $u \notin F^2$, we get $-1 \notin F^2$. In other words, $i \notin F$, where i is a root of $x^2 + 1$. Over $F(i)$, we have the factorization

$$f(x) = x^{2^k} - u = x^{2^k} + b^2 = (x^{2^{k-1}} + ib)(x^{2^{k-1}} - ib) \tag{13.1.1}$$

If both of the factors on the right side are irreducible over $F(i)$, then f(x) cannot factor nontrivially over F. For if $f(x) = \prod a_i(x)$ is a nontrivial factorization, where the $a_i(x)$ are irreducible over F, then one of the factors has degree at most 2^{k-1}, and is not one of the factors in (13.1.1). Factoring each $a_i(x)$ into irreducibles over $F(i)$ would then produce a prime factorization over $F(i)$ distinct from (13.1.1), which is not possible since F[x] is a unique factorization domain.

Now, if one of the factors in (13.1.1) is reducible, the induction hypothesis implies that one of ib or $-ib$ lies in $F(i)^2$ or $-4F(i)^4 = [2iF(i)^2]^2$. In either case, one of ib or $-ib$ is in $F(i)^2$, say

$$\pm ib = (c + di)^2 = c^2 + 2cdi - d^2$$

Thus, $c^2 = d^2$ and $b^2 = 4c^2d^2 = 4c^4$. It follows that $u = -b^2 = -4c^4$, a contradiction to the hypothesis of the lemma. Thus, $f(x)$ is irreducible over F.

Case 2b: $p = 2$, $\alpha \notin F(\alpha)^2$ but $\alpha = -4\gamma^4$, for some $\gamma \in F(\alpha)$.

Since α has degree 2 over F, taking norms gives

$$-u = N(\alpha) = N(-4\gamma^4) = 16[N(\gamma)]^4$$

and so $-u \in F^2$. Hence, $-u = a^2$ for $a \in F$ and so $-1 = a^2/u = a^2/\alpha^2 \in F(\alpha)^2$, say $-1 = i^2$, with $i \in F(\alpha)$. Then

$$\alpha = -4\gamma^4 = (2i\gamma^2)^2 \in F(\alpha)^2$$

a contradiction. Hence, this case cannot occur. ∎

Now we can prove the main result of this section.

Theorem 13.1.5 Let $n \geq 2$ be an integer and let $u \in F$. The following are equivalent.

1) $f(x) = x^n - u$ is irreducible over F.
2) $u \notin F^p$ for all primes $p \mid n$ and $u \notin -4F^4$ when $4 \mid n$.

In particular, if $4 \nmid n$, then $x^n - u$ is irreducible over F if and only if $x^p - u$ is irreducible over F, for all primes $p \mid n$.

Proof. The last statement follows from Lemma 13.1.2. Proof of 1)⇒2) is left to the reader. For the converse, we have seen that this result holds if $n = p^k$ is a prime power. Suppose that $n = p^k m$ where $(p,m) = 1$ and $k \geq 1$. We may assume that p is odd, for if 2 is the only prime divisor of n then $n = 2^k$ is a prime power. We proceed by induction on n. Let β be a root of $x^n - u$. In a splitting field, we have

$$x^m - u = (x - \alpha_1)(x - \alpha_2)\cdots(x - \alpha_m)$$

Thus

$$f(x) = x^n - u = x^{mp^k} - u = (x^{p^k} - \alpha_1)(x^{p^k} - \alpha_2)\cdots(x^{p^k} - \alpha_m)$$

Suppose that β is a root of

$$g(x) = x^{p^k} - \alpha$$

where $\alpha = \alpha_i$ for some i. By induction, $x^m - u$ is irreducible over F and

so the first step in the tower

$$F < F(\alpha) < F(\beta)$$

has degree m. If g(x) is irreducible over $F(\alpha)$, then the second step will have degree p^k, whence $[F(\beta):F] = mp^k = n$ and $f(x) = min(\beta,F)$, which is irreducible.

We apply the inductive hypothesis to show that g(x) is irreducible. Since p is odd, we need only show that $\alpha \notin F(\alpha)^p$. If $\alpha = \gamma^p$ for some $\gamma \in F(\alpha)$ then taking norms $N = N_{F(\alpha)/F}$ gives

$$-u = (-1)^m N(\alpha) = (-1)^m N(\gamma^p) = (-1)^m [N(\gamma)]^p$$

If m is odd, we get $u = [N(\gamma)]^p \in F^p$, a contradiction. If m is even then since p is odd, we have $u = [-N(\gamma)]^p \in F^p$, again a contradiction. Hence, $\alpha \notin F(\alpha)^p$, g(x) is irreducible over $F(\alpha)$ and f(x) is irreducible over F. ∎

13.2 The Galois Group of a Binomial

Let us now examine the Galois group of a binomial $x^n - u$ over F, for $u \neq 0$ and n relatively prime to expchar(F). If α is a root of $x^n - u$ and $\omega \in \Omega_n$, then the roots of $x^n - u$ are $\alpha, \omega\alpha, \ldots, \omega^{n-1}\alpha$ and so $S = F(\omega,\alpha)$ is a splitting field for $x^n - u$ over F. Moreover, in the tower

$$F < F(\omega) < F(\omega,\alpha) = S \tag{13.2.1}$$

the first step is a cyclotomic extension, which is abelian since its Galois group is isomorphic to a subgroup of $\mathbb{Z}_n^*$. The second step is cyclic of degree $d \mid n$ with $min(\alpha,F(\omega)) = x^d - \alpha^d$. Nevertheless, the Galois group $G_F(S)$ need not be abelian.

The fact that α and ω both satisfy simple polynomials *over F* is the key to describing the Galois group $G_F(S)$. Since any $\sigma \in G_F(S)$ must permute the roots of $x^n - u$, there exists an integer $k(\sigma) \in \mathbb{Z}_n$ for which

$$\sigma\alpha = \omega^{k(\sigma)}\alpha$$

Moreover, since $F(\omega)$ is a normal extension of F, the restriction of σ to $F(\omega)$ is in $G_F(F(\omega))$ and therefore σ sends ω to another primitive n-th root of unity, that is,

$$\sigma\omega = \omega^{j(\sigma)}$$

where $j(\sigma) \in \mathbb{Z}_n^*$.

Multiplication in $G_F(S)$ has the following form. For $\sigma, \tau \in G_F(S)$,

$$\sigma\tau\alpha = \sigma(\omega^{k(\tau)}\alpha) = \omega^{j(\sigma)k(\tau)}\omega^{k(\sigma)}\alpha = \omega^{j(\sigma)k(\tau)+k(\sigma)}\alpha$$

and

$$\sigma\tau\omega = \sigma\omega^{j(\tau)} = \omega^{j(\sigma)j(\tau)}$$

There is something reminiscent of matrix multiplication in this. Indeed, let $\mathcal{M}_n$ be the set of all matrices of the form

$$\mathcal{M}_n = \left\{ \begin{bmatrix} 1 & 0 \\ k & j \end{bmatrix} : k \in \mathbb{Z}_n, j \in \mathbb{Z}_n^* \right\}$$

Since

$$\begin{bmatrix} 1 & 0 \\ k & j \end{bmatrix} \begin{bmatrix} 1 & 0 \\ k' & j' \end{bmatrix} = \begin{bmatrix} 1 & 0 \\ k+jk' & jj' \end{bmatrix}$$

we see that $\mathcal{M}_n$ is a subgroup of the general linear group $GL_2(\mathbb{Z}_n)$ of all nonsingular 2×2 matrices over $\mathbb{Z}_n$. (All entries are taken modulo n.) Comparing this product with the action of the product $\sigma\tau$ shows that the map $\psi: G_F(S) \to \mathcal{M}_n$ defined by

$$\psi:\sigma \mapsto \begin{bmatrix} 1 & 0 \\ k(\sigma) & j(\sigma) \end{bmatrix}$$

satisfies

$$\psi(\sigma\tau) = \psi(\sigma)\psi(\tau)$$

and is, in fact, a monomorphism from $G_F(S)$ into $\mathcal{M}_n$.

Since $|\mathcal{M}_n| = n\phi(n)$, where ϕ is the Euler phi-function, the map ψ is surjective if and only if

$$[S:F] = |G_F(S)| = n\phi(n)$$

But in the tower

$$F < F(\omega) < F(\omega,\alpha) = S$$

we always have $[F(\omega):F] \leq \phi(n)$ and $[F(\omega,\alpha):F(\omega)] \leq n$. (See Figure 13.2.1.) Hence ψ is surjective (and an isomorphism) if and only if equality holds in these two inequalities.

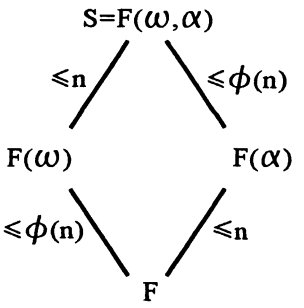

Figure 13.2.1

Theorem 13.2.1 Let n be a positive integer relatively prime to expchar(F). Let S be the splitting field for $x^n - u$ over F, where $u \in F$, $u \neq 0$. Let α be a root of $x^n - u$ and $\omega \in \Omega_n$. Then $G_F(S)$ is isomorphic to a subgroup of the group $\mathcal{M}_n$ described above, via the monomorphism

$$\psi:\sigma \mapsto \begin{bmatrix} 1 & 0 \\ k(\sigma) & j(\sigma) \end{bmatrix}$$

where $\sigma\alpha = \omega^{k(\sigma)}\alpha$ and $\sigma\omega = \omega^{j(\sigma)}$. In addition, ψ is an isomorphism and $G_F(S) \simeq \mathcal{M}_n$ if and only if both steps in the tower (13.2.1) have maximum degree, that is, if and only if both of the following hold

1) $[F(\omega):F] = \phi(n)$,

2) $[F(\omega,\alpha):F(\omega)] = n$, that is, $x^n - u$ is irreducible over $F(\omega)$. □

Statement 2) is phrased in terms of $F(\omega)$ and we would prefer a statement involving only the base field F. For n prime, this is easy.

Lemma 13.2.2 Let p be a prime and let $\omega \in \Omega_p$. Then $x^p - u$ is irreducible over $F(\omega)$ if and only if it is irreducible over F. Equivalently, $x^p - u$ has a root in $F(\omega)$ if and only if it has a root in F.

Proof. Certainly, if $x^n - u$ is irreducible over $F(\omega)$, it is also irreducible over F. For the converse, consider the tower

$$F < F(\omega) < F(\omega,\alpha)$$

Since $x^p - u$ is irreducible over F, we have

$$p = [F(\alpha):F] \leq [F(\omega,\alpha):F]$$

On the other hand, the first step in the tower has degree at most $\phi(p) = p - 1$ and the second step is cyclic of degree $d \mid p$, whence $d = 1$ or p. Hence $[F(\omega,\alpha):F(\omega)] = p$, which implies that $x^p - u = min(\alpha,F(\omega))$ is irreducible over $F(\omega)$. ∎

In order to extend this result to arbitrary n (and for its own interest), we want to say more about when the Galois group $G_F(S)$ is abelian. Of course, since both steps in the tower

$$F < F(\omega) < F(\omega,\alpha) = S$$

are abelian, if either step is trivial, then $G_F(S)$ is abelian. Thus, if $\omega \in F$ or if $\alpha \in F(\omega)$ then $G_F(S)$ is abelian. The converse is also true when n is prime.

Lemma 13.2.3 Let p be a prime and let $\omega \in \Omega_p$. Then the Galois group $G_F(S)$ is abelian if and only if at least one step in the tower (13.2.1) is trivial, that is, if and only if either $\omega \in F$ or $x^p - u$ has a root in $F(\omega)$ [or, equivalently, a root in F].

Proof. One direction has already been discussed so we need only show that if $\omega \notin F$ and $x^p - u$ is irreducible over $F(\omega)$ then $G_F(S)$ is not abelian. Since $\omega \notin F$, it has a conjugate $\omega^j \neq \omega$ that is also not in F. Let $\tau \in G_F(F(\omega))$ be defined by $\tau\omega = \omega^j$. Since $x^p - u$ is irreducible over $F(\omega)$, for each $i \in \mathbb{Z}_p$, the map τ may be extended to a $\sigma_i \in G_F(S)$ defined by

$$\sigma_i\omega = \omega^j, \quad \sigma_i\alpha = \omega^i\alpha$$

Taking $i = 1$ and $i' = 0$ gives

$$\sigma_1\sigma_0\alpha = \sigma_1\alpha = \omega\alpha$$

and

$$\sigma_0\sigma_1\alpha = \sigma_0(\omega\alpha) = \omega^j\alpha$$

and these are distinct since $\omega \neq \omega^j$. Hence, σ_1 and σ_0 do not commute and $G_F(S)$ is not abelian. ∎

We can now strengthen the statement of Theorem 13.2.1 by showing that, in certain cases, when n is odd and $[F(\omega):F] = \phi(n)$, then $x^n - u$ is

irreducible over $F(\omega)$ if and only if it is irreducible over F. The idea of the proof is this. Suppose that p(x) is an irreducible polynomial over F, with splitting field S. Suppose also that E is a normal extension of F. Then p(x) has a root in E if and only if it splits in E, that is, if and only if $F < S < E$. Now, if $F < E$ is an abelian extension, that is, if $G_F(E)$ is abelian, then so is any quotient group of $G_F(E)$, in particular, so is

$$G_F(S) \simeq \frac{G_F(E)}{G_S(E)}$$

Thus, if $G_F(S)$ is not abelian, we can conclude that p(x) does not have a root in E.

Part of the hypotheses of the next theorem is that the base field F does not contain any n-th roots of unity, other than 1. Note that this is equivalent to saying that F does not contain any primitive p-th roots of unity for any prime $p \mid n$.

Theorem 13.2.4 Let n be an odd positive integer relatively prime to expchar(F). Let ω be a primitive n-th root of unity over F and suppose that F does not contain a primitive p-th root of unity for any prime $p \mid n$. Let $F < A$ be any abelian extension. Then $x^n - u$ is irreducible over F if and only if it is irreducible over A.

Proof. Clearly, if $x^n - u$ is irreducible over A, it is also irreducible over the smaller field F. Suppose that $x^n - u$ is irreducible over F, but not over A. Since $4 \nmid n$, Theorem 13.1.5 and Lemma 13.1.2 imply that there exists a prime $p \mid n$ for which no roots of $x^p - u$ lie in F, but some root α of $x^p - u$ lies in A. Hence, Lemma 13.2.3 implies that if ξ is a primitive p-th root of unity, then the Galois group $G_F(F(\xi,\alpha))$ is not abelian.

On the other hand, since $F < A$ is normal and A contains one root of the irreducible polynomial $x^p - u$, it contains all roots of $x^p - u$. Thus,

$$F < F(\xi,\alpha) < A$$

But $F < A$ is abelian and therefore so is the quotient

$$G_F(F(\xi,\alpha)) \simeq \frac{G_F(A)}{G_{F(\xi,\alpha)}(A)}$$

This contradiction implies that $x^n - u$ is irreducible over A. ∎

According to Theorem 10.2.9, if $[F(\omega):F] = \phi(n)$, then F cannot contain any primitive p-th roots of unity for any $p \mid n$ and we may

apply Theorem 13.2.4 to get the following strengthening of Theorem 13.2.1.

Corollary 13.2.5 Referring to Theorem 13.2.1, if n is an odd positive integer relatively prime to expchar(F) then $G_F(S) \simeq \mathcal{M}_n$ if and only if $[F(\omega):F] = \phi(n)$ and $x^n - u$ is irreducible over F. □

Since $[\mathbb{Q}(\omega):\mathbb{Q}] = \phi(n)$, we have

Corollary 13.2.6 Referring to Theorem 13.2.1, if $F = \mathbb{Q}$ and n is an odd positive integer then $G_{\mathbb{Q}}(S) \simeq \mathcal{M}_n$ if and only if $x^n - u$ is irreducible over $\mathbb{Q}$. □

Thus, when $F < F(\omega)$ has the largest possible degree $\phi(n)$ (which includes the important case $F = \mathbb{Q}$), we see that $G_F(S) \simeq \mathcal{M}_n$ if and only if $x^n - u$ is irreducible over F. In some sence, $\mathcal{M}_n$ is the "most nonabelian" subgroup of $\mathcal{M}_n$. At the opposite extreme, we can show, again when $[F(\omega):F] = \phi(n)$, that $G_F(S)$ is abelian if and only if $x^n - u$ actually has a root in F.

Theorem 13.2.7 Let n be an odd positive integer relatively prime to expchar(F). Let S be the splitting field for $x^n - u$ over F, where $u \in F$, $u \neq 0$. Suppose that $[F(\omega):F] = \phi(n)$ where $\omega \in \Omega_n$. Then the following are equivalent.

1) $G_F(S)$ is abelian
2) $x^n - u$ has a root in F
3) $x^n - u$ has a root in $F(\omega)$ [and therefore splits in $F(\omega)$]

Proof. Clearly, 2)⇒3)⇒1). Suppose that $G_F(S)$ is abelian and let k be the largest divisor of n for which $u \in F^k$, that is, $u = f^k$ for some $f \in F$. The proof will be complete if we show that $k = n$. If $k < n$, let p be a prime number dividing n/k. Consider the tower

$$F < F(\omega_p) < F(\omega_p, f^{1/p}) \tag{13.2.2}$$

Note that $x^p - f$ is irreducible over F, for if not, then $f = g^p \in F^p$ for some $g \in F$, whence $u = f^k = g^{pk} \in F^{pk}$, in contradiction to the definition of k. Hence $[F(f^{1/p}):F] = p$ and

$$[F(\omega_p, f^{1/p}):F] \geq p$$

Theorem 10.2.9 implies that $[F(\omega_p):F] = p - 1$ and since $F(\omega_p) < F(\omega_p, f^{1/p})$ is cyclic of degree dividing the prime p, neither step in the tower (13.2.2) is trivial. Hence, Lemma 13.2.3 implies that the Galois group $H = G_F(F(\omega_p, f^{1/p}))$ is not abelian.

We will now produce a contradiction by showing that $G_F(S)$ abelian implies H is abelian. Since each root of $x^p - f$ is a root of $x^{pk} - u$ we have

$$F < F(\omega_p, f^{1/p}) < F(\omega_{pk}, u^{1/pk})$$

Since $(u^{1/n})^{n/pk}$ is a root of $x^{pk} - u$, at least one root of $x^{pk} - u$ is in $F(\omega, u^{1/n})$. But $\omega^{n/pk} = \omega_{pk}$ and so all roots of $x^{pk} - u$ are in $F(\omega, u^{1/p})$. Hence,

$$F < F(\omega_p, f^{1/p}) < F(\omega_{pk}, u^{1/pk}) < F(\omega, u^{1/n})$$

Since $F < F(\omega, u^{1/n})$ is assumed to be abelian, so is the subextension $F < F(\omega_p, f^{1/p})$, that is, H is abelian. This contradiction completes the proof that 1) implies 2). ∎

In the exercises, we ask the reader to provide a simple example to show that Theorems 13.2.4 and 13.2.7 fail to hold when n is even.

We conclude this section by generalizing the previous theorem, in order to characterize precisely (for n odd) when $G_F(S)$ is abelian. The proof follows lines similar to the proof of Theorem 13.2.7, but is a bit more intricate and since it involves no new insights, the reader may wish to skip it on first reading. However, the result is of interest since it shows how the relationship between the n-th roots of unity and the ground field F play a role in the commutativity of $G_F(S)$. We first need a result that is of interest in its own right. The proof is left as an exercise.

Theorem 13.2.8 Let $x^n - a$ and $x^n - b$ be irreducible over F and suppose that F contains a primitive n-th root of unity. Then $x^n - a$ and $x^n - b$ have the same splitting field over F if and only if $b = c^n a^r$ for some $c \in F$ and r relatively prime to n. □

Theorem 13.2.9 Let n be an odd positive integer relatively prime to expchar(F). Let U_n be the group of n-th roots of unity over F and let $U_m = U_n \cap F^*$. If S is the splitting field for $x^n - u$ ($u \in F$, $u \neq 0$), then $G_F(S)$ is abelian if and only if $u^m \in F^n$.

Proof. Note first that $m \mid n$ since U_m is a subgroup of U_n. Moreover, since $U_m = \langle \omega_m \rangle$ is cyclic, $\omega_i \in F$ if and only if $i \mid m$. Suppose first that $u^m = f^n$ for some $f \in F$. Then

$$u^{1/n} = \omega_{mn}^k f^{1/m}$$

for some integer k. (More precisely, given any n-th root $u^{1/n}$ of n and

any m-th root $f^{1/m}$ of f, there exists a k such that this equation holds.) The field $F(f^{1/m})$ is cyclic over F, since the latter contains a primitive m-th root of unity ω_m. Therefore, since $F < F(\omega_{mn})$ and $F < F(f^{1/m})$ are both abelian, so is the extension

$$F < F(\omega_{mn})F(f^{1/m}) = F(\omega_{mn},f^{1/m}) = F(\omega_{mn},u^{1/n})$$

Finally, since $F < S < F(\omega_{mn},u^{1/n})$, we deduce from Theorem 5.5.5 that $F < S$ is abelian.

For the converse, assume that $G_F(S)$ is abelian. Let k be the largest positive integer such that $m \mid k$, $k \mid n$ and $u^m \in F^k$, say $u^m = f^k$ for $f \in F$. (There is such an integer since $k = m$ satisfies these conditions.) We need to show that $k = n$. Suppose to the contrary that $k < n$ and let p be a prime number dividing n/k. Let p^s be the largest power of p such that $p^s \mid m$. (The hypothesis that n is odd and $[F(\omega):F] = \phi(n)$ in Theorem 13.2.7 implies that $m = 1$, whence $s = 0$.)

The first step is to show that the extension

$$F < F(\omega_{p^{s+1}},f^{1/p^{s+1}})$$

is abelian. It is clear that the notation is a bit unwieldy, so let us set $q = p^{s+1}$ and note that $q \mid n$ since $p^s \mid m \mid k$ and $p \mid (n/k)$. To see that this extension is abelian, we embed it in an abelian extension. Since

$$(f^{1/q})^{kq} = f^k = u^m = (u^{m/kq})^{kq}$$

we have $f^{1/q} = \omega_{kq}^j u^{m/kq}$ for some j and so

$$F(\omega_q,f^{1/q}) < F(\omega_{kq},f^{1/q}) = F(\omega_{kq},u^{m/kq})$$

If we set

$$v = (u^{1/n})^{nm/kq}$$

then v is a root of $x^{kq/m} - u$ and $v \in F(\omega_{kq},u^{1/n})$. Hence, all roots of $x^{kq/m} - u$ are contained in $F(\omega_{kq},u^{1/n})$, that is,

$$F(\omega_{kq},u^{m/kq}) < F(\omega_{kq},u^{1/n})$$

Putting the pieces together gives

$$F < F(\omega_q,f^{1/q}) < F(\omega_{kq},u^{m/kq}) < F(\omega_{kq},u^{1/n}) < F(\omega_{qk})F(\omega_n,u^{1/n})$$

Since $F < F(\omega_{qk})$ and $F < F(\omega_n,u^{1/n})$ are abelian (the latter by assumption), the composite

$$F < F(\omega_{qk})F(\omega_n, u^{1/n})$$

is abelian and therefore so is

$$F < F(\omega_q, f^{1/q})$$

We now propose to arrive at a contradiction by considering the tower

$$F < F(\omega_q) < F(\omega_q, f^{1/q})$$

Note that $x^p - f$ is irreducible over F, since otherwise $f = g^p \in F^p$ for some $g \in F$, whence $u = f^k = g^{pk} \in F^{pk}$, in contradiction to the definition of k.

We first take the case $s = 0$, whence $q = p$. Since $x^p - f$ is irreducible over F, we have $[F(f^{1/p}):F] = p$ and

$$[F(\omega_p, f^{1/p}):F] \geq p$$

Since $p \nmid m$, it follows that $\omega_p \notin F$ and so the extension $F < F(\omega_p)$ is not trivial. Since $[F(\omega_p):F] \leq p - 1$ and $F(\omega_p) < F(\omega_p, f^{1/p})$ is cyclic of degree dividing the prime p, the latter extension is also not trivial. Hence, Lemma 13.2.3 implies that the Galois group $H = G_F(F(\omega_p, f^{1/p}))$ is not abelian, the desired contradiction.

Now assume that $s > 0$. With regard to the first step in the tower, letting $r = p^s \geq p$, we have $r \mid m$ and $q \nmid m$, hence $\omega_r \in F$ but $\omega_q \notin U_m$. Since $s > 0$, we also get $\omega_p \in F$. Hence $x^p - \omega_r$ is either irreducible or splits in F. But ω_q is a root not in F and so $x^p - \omega_r$ is irreducible over F. (Note that for $s > 0$, the first step in the tower has degree p, rather than a number dividing $p - 1$, hence we cannot use the same strategy as when $s = 0$.) Since the roots of $x^p - \omega_r$ are

$$\omega_q, \omega_r\omega_q, \ldots, \omega_r^{p-1}\omega_q$$

for each $j \in \mathbb{Z}_p$, there is a $\sigma_j \in G_F(F(\omega_q))$ for which $\sigma_j\omega_q = \omega_r^j\omega_q$. To show that $G_F(F(\omega_q, f^{1/q}))$ is not abelian, we shall need only $\sigma_0:\omega_q \mapsto \omega_q$ and $\sigma_1:\omega_q \mapsto \omega_r\omega_q$.

There are two possibilities for the second step in the tower. If $x^q - f$ is irreducible over $F(\omega_q)$ then we can extend σ_0 and σ_1 to elements of $G_F(F(\omega_q, f^{1/q}))$ by defining

$$\sigma_{0,1}:\omega_q \mapsto \omega_q, \quad \sigma_{0,1}:f^{1/q} \mapsto \omega_q f^{1/q}$$

and

$$\sigma_{1,0}:\omega_q \mapsto \omega_r\omega_q, \quad \sigma_{1,0}:f^{1/q} \mapsto f^{1/q}$$

Then

$$\sigma_{0,1}\sigma_{1,0}f^{1/q} = \sigma_{0,1}f^{1/q} = \omega_q f^{1/q}$$

and

$$\sigma_{1,0}\sigma_{0,1}f^{1/q} = \sigma_{1,0}(\omega_q f^{1/q}) = \omega_r\omega_q f^{1/q}$$

which are distinct since $\omega_r \neq 1$. Hence, $G_F(F(\omega_q, f^{1/q}))$ is not abelian, a contradiction.

If $x^q - f$ is reducible over $F(\omega_q)$ then $f \in F(\omega_q)^p$. Thus $f = \beta^p$ for some $\beta \in F(\omega_q)$ and so $F(\beta) < F(\omega_q)$. Since $x^p - \omega_r$ and $x^p - f$ are both irreducible over F, it follows that $[F(\omega_q):F] = p$ and $[F(\beta):F] = p$, whence $F(\omega_q) = F(\beta)$. Thus, $x^p - f$ and $x^p - \omega_r$ have the same splitting field over F and Theorem 13.2.8 implies that

$$f = \omega_r^j v^p$$

for some $v \in F$. Taking k-th powers gives, since $r \mid k$,

$$u^m = f^k = \omega_r^{kj} v^{kp} = v^{kp}$$

for $v \in F$, which contradicts the definition of k. Thus, $k = n$ and the theorem is proved. ∎

*13.3 The Independence of Irrational Numbers

A familiar argument (at least for $p = 2$) shows that if p is a prime number then $\sqrt{p} \notin \mathbb{Q}$ and so $[\mathbb{Q}(\sqrt{p}):\mathbb{Q}] = 2$. Our plan in this section is to extend this result to more than one prime p and to n-th roots for $n \geq 2$. Since the case when n is even involves some rather intricate details which give no further insight into the issues involved, we will confine our attention to n odd. (The case $n = 2$ is straightforward and we invite the reader to supply a proof of Theorem 13.3.2 for this case.) If $\alpha > 0$ is rational, the notations $\sqrt[n]{\alpha}$ and $\alpha^{1/n}$ will denote the *real positive* n-th root of α. The results of this section were first proved by Bescovitch [1940] but the method of proof we employ follows more closely that of Richards [1974].

Lemma 13.3.1 Let $u = a/b$ be a positive rational number, expressed in lowest terms, that is, where $(a,b) = 1$. If $n \geq 2$ is an integer then

$\sqrt[n]{\frac{a}{b}} \in \mathbb{Q}$ if and only if $a = c^n$ and $b = d^n$ for some integers c and d

In particular, if p is a prime, then $\sqrt[n]{p} \notin \mathbb{Q}$.

Proof. One direction is quite obvious. Suppose then that

$$(\frac{c}{d})^n = \frac{a}{b}$$

where c and d are positive integers and (c,d) = 1. Then $ad^n = bc^n$ and since (a,b) = 1, it follows that $a \mid c^n$. Thus $c^n = \alpha a$ for some integer α. Substituting this into $ad^n = bc^n$ gives $ad^n = \alpha ab$ or $d^n = \alpha b$. But since (c,d) = 1, we also have $(c^n,d^n) = 1$, that is, $(\alpha a,\alpha b) = 1$. Hence $\alpha = 1$ and so $a = c^n$ and $b = d^n$. ∎

Suppose now that n is odd. Since $p \notin \mathbb{Q}^r$ for any prime $r \mid n$, Theorem 13.1.5 implies that $x^n - p$ is irreducible over $\mathbb{Q}$ and so $[\mathbb{Q}(\sqrt[n]{p}):\mathbb{Q}] = n$. Let us generalize this to more than one prime.

Theorem 13.3.2 Let $n \geq 2$ be an integer and let $p_1,\ldots,p_m$ be distinct primes. Then

$$[\mathbb{Q}(\sqrt[n]{p_1},\ldots,\sqrt[n]{p_m}):\mathbb{Q}] = n^m$$

Proof. As mentioned earlier, we confine our proof to the case where $n \geq 3$ is odd. Let $\omega \in \Omega_n$. Since

$$[\mathbb{Q}(\omega)(\sqrt[n]{p_1},\ldots,\sqrt[n]{p_m}):\mathbb{Q}(\omega)] \leq [\mathbb{Q}(\sqrt[n]{p_1},\ldots,\sqrt[n]{p_m}):\mathbb{Q}] \leq n^m$$

it is sufficient to show that

$$[\mathbb{Q}(\omega)(\sqrt[n]{p_1},\ldots,\sqrt[n]{p_m}):\mathbb{Q}(\omega)] = n^m$$

which we shall do by induction on m.

Let p be a prime. Since $x^n - p$ is irreducible over $\mathbb{Q}$ and $\mathbb{Q}$ contains no primitive r-th roots of unity for any prime $r \mid n$, Theorem 13.2.4 implies that $x^n - p$ is also irreducible over $\mathbb{Q}(\omega)$. Hence,

$$[\mathbb{Q}(\omega,\sqrt[n]{p}):\mathbb{Q}(\omega)] = n$$

and the theorem holds for m = 1.

Now let us suppose that the theorem is true for the integer m and let p be a prime distinct from the distinct primes $p_1,\ldots,p_m$. Let

$$F = \mathbb{Q}(\omega) \quad \text{and} \quad E = \mathbb{Q}(\omega)(\sqrt[n]{p_1},\ldots,\sqrt[n]{p_m})$$

If $x^n - p$ is not irreducible over E then there exists a prime $r \mid n$ such that $p^{1/r} \in E$. Thus, $p^{1/r}$ is a linear combination, over $\mathbb{Q}(\omega)$, of terms of

the form

$$\sqrt[n]{p_1^{e(1)}}\ \sqrt[n]{p_2^{e(2)}} \cdots \sqrt[n]{p_m^{e(m)}}$$

where $0 \leq e(i) \leq n-1$. There are two cases to consider.

Case 1: If the linear combination involves only one term, then

$$\sqrt[r]{p} = c\sqrt[n]{p_1^{e(1)}}\ \sqrt[n]{p_2^{e(2)}} \cdots \sqrt[n]{p_m^{e(m)}}$$

where $c \in \mathbb{Q}(\omega)$ and not all $e(i)$ are 0. If $n = rd$, this can be written in the form

$$\sqrt[n]{\frac{p^d}{p_1^{e(1)} \cdots p_m^{e(m)}}} \in \mathbb{Q}(\omega)$$

This says that the radicand q is a positive rational number and the polynomial $x^n - q$ has a root in $\mathbb{Q}(\omega)$. According to Theorem 13.2.7, $x^n - q$ must also have a root in $\mathbb{Q}$, which is not possible since q does not have the form a^n/b^n, for integers a, b. Hence, this case cannot occur.

Case 2: At least two terms in the linear combination are nonzero. It follows that one of the primes p_i, which we may assume for convenience is p_m, appears to different powers in at least two distinct terms. Collecting terms that involve like powers of p_m gives

$$(13.3.1) \qquad p^{1/r} = A_0 + A_1 p_m^{1/n} + A_2 p_m^{2/n} + \cdots + A_{n-1} p_m^{(n-1)/n}$$

where $A_i \in \mathbb{Q}(\omega)(\sqrt[n]{p_1}, \ldots, \sqrt[n]{p_{m-1}})$ and where at least two of the A_i's are nonzero. Now, since

$$\mathbb{Q}(\omega) < \mathbb{Q}(\omega)(\sqrt[n]{p_1}, \ldots, \sqrt[n]{p_m})$$

is a Galois extension (this is why we adjoined ω in the first place), the inductive hypothesis implies that its Galois group G has size n^m. Since any $\sigma \in G$ must send roots of $x^n - p_i$ to other roots, it must send $\sqrt[n]{p_i}$ to $\omega^j \sqrt[n]{p_i}$ for some $j = 0, \ldots, n-1$. Since there are n^m such choices, all of these choices must occur.

Thus, there is a $\sigma \in G$ for which

$$\sigma p_m^{1/n} = \omega p_m^{1/n}, \quad \sigma p_i^{1/n} = p_i^{1/n} \ \text{(for all } i < m)$$

Since $\sigma p^{d/n} = \omega^k p^{d/n}$ for some $0 \leq k \leq n-1$, applying σ to (13.3.1) gives

$$\omega^k p^{d/n} = A_0 + A_1 \omega p_m^{1/n} + A_2 \omega^2 p_m^{2/n} + \cdots + A_{n-1} \omega^{n-1} p_m^{(n-1)/n}$$

We now multiply (13.3.1) by ω^k and subtract the previous equation to get

$$0 = (\omega^k - 1)A_0 + (\omega^k - \omega)A_1 p_m^{1/n} + \cdots + (\omega^k - \omega^{n-1})p_m^{(n-1)/n}$$

where at least one of the coefficients $(\omega^k - \omega^i)A_i$ is nonzero. This is a contradiction to the inductive hypothesis. We have therefore established that $x^n - p$ is irreducible over E and the proof is complete. ∎

Exercises

1. Let n be relatively prime to char(F). Show that the Galois group of $x^n - u$ is isomorphic to a subgroup of the group generated by σ, τ where $\sigma^n = \tau^{\phi(n)} = 1$, $\sigma\tau\sigma^{-1} = \tau^r$. What is r?
2. (Van der Waerden) Let n be relatively prime to char(F). Show that the Galois group of $x^n - u$ is isomorphic to the group of linear substitutions modulo n: $x \to cx + d$ where $d \in \mathbb{Z}_n$, $c \in \mathbb{Z}_n^*$.
3. Let $x^n - u \in GF(q)[x]$. Show that the following are equivalent: (i) $r \mid n$, r prime implies $u \notin GF(q)^r$ and (ii) $r \mid n$, r prime implies $r \mid o(u)$ but $r \nmid (q-1)/o(u)$ where $o(u)$ is the multiplicative order of u in $GF(q)$.
4. Prove Lemma 13.1.2 by factoring $x^p - u$ in a splitting field and then considering $min(\alpha, F)$.
5. Prove the following without using any of the results of Section 13.1. If $u \in F$ and $(m,n) = 1$ then $x^{mn} - u$ is irreducible over F if and only if $x^m - u$ and $x^n - u$ are irreducible over F.
6. Let $\text{char}(F) = p \neq 0$ and let $F < E$ be cyclic of degree p^k, with Galois group $G = \langle\sigma\rangle$. If there exists a $\beta \in E$ with $\text{Tr}_{E/F}(\beta) = 1$ show that there exists an $\alpha \in E$ for which the polynomial $f(x) = x^p - x - \alpha$ is irreducible over E.
7. Let $\text{char}(F) = p > 0$ and let $n = p^e m$ where $(m,p) = 1$. Show that the Galois groups of
$$x^n - u \quad \text{and} \quad x^m - u^{p^{-e}}$$
are the same.
8. Let n be a positive integer relatively prime to expchar(F) and let ω be a primitive n-th root of unity over F. Let $S = F(\omega, u^{1/n})$ be the splitting field for $f(x) = x^n - u$ over F, where $u \in F$, $u \neq 0$. If $4 \mid n$ and if $u^{1/2} \notin F$ then $G_F(S)$ is not abelian.
9. Show that Theorem 13.2.4 and Theorem 13.2.7 fail to hold when n is even. *Hint*: $\sqrt{2} \in \mathbb{Q}(\omega)$, where ω is a primitive 8-th root of unity.
10. Prove the following: Let f(x) be a monic irreducible polynomial of degree m over F, with constant term $-a_0$. Let $n \geq 2$ be an integer with the following properties (i) $(m,n) = 1$, (ii) $4 \nmid n$ (iii) $a_0 \notin F^r$

for all primes $r \mid n$. Then the polynomial $f(x^n)$ is also irreducible over F.

11. Let ω be a primitive n-th root of unity over F, n odd, and let α be a root of $x^n - u$ over F. Then $S = F(\omega,\alpha)$ is the splitting field for $x^n - u$. Assume that $G_F(S) \simeq \mathcal{M}_n$. (See Theorem 13.2.1.) In this exercise, we determine the largest abelian subextension F^{ab} of S.
    a) If G is a group, the subgroup G′ generated by all **commutators** $\alpha\beta\alpha^{-1}\beta^{-1}$, for α, $\beta \in G$, is called the **commutator subgroup**. Show that G′ is the smallest subgroup of G for which G/G′ is abelian.
    b) If the commutator subgroup $G_F(E)'$ of a Galois group $G_F(E)$ is closed, that is, if $G_F(E)' = G_K(E)$ for some $F < K < E$, then K is the largest abelian extension of F contained in E.
    c) The commutator subgroup of $\mathcal{M}_n$ is

$$\mathcal{M}_n' = \left\{ \begin{bmatrix} 1 & 0 \\ k & 1 \end{bmatrix} : k \in \mathbb{Z}_n \right\}$$

and

$$\psi(G_{F(\omega)}(S)) = \psi(G_F(S)) \cap \mathcal{M}_n' = \left\{ \begin{bmatrix} 1 & 0 \\ i\frac{n}{d} & 1 \end{bmatrix} : i \in \mathbb{Z}_d \right\}$$

where $d = [F(\omega,\alpha):F(\omega)]$.
    d) $G_F(S)' = G_{F(\omega)}(S)$, and so $F(\omega)$ is the largest abelian extension of F contained in $F(\omega,\alpha)$.

12. Prove that if $p_1,\ldots,p_m$ are distinct primes then

$$[\mathbb{Q}(\sqrt{p_1},\ldots,\sqrt{p_m}):\mathbb{Q}] = 2^m \tag{1}$$

by induction on m.

13. Show that $\sqrt{60} \notin \mathbb{Q}(\sqrt{42},\sqrt{10})$.

14. Let n be a positive integer relatively prime to expchar(F) and let ω be a primitive n-th root of unity over F. Let $S = F(\omega,u^{1/n})$ be the splitting field for $f(x) = x^n - u$ over F, where $u \in F$, $u \neq 0$. If for some prime $p \mid n$, we have $\omega_p \notin F$ and $u^{1/p} \notin F$, where ω_p is a primitive p-th root of unity over F, then the Galois group $G_F(S)$ is not abelian.

15. Let $x^n - a$ and $x^n - b$ be irreducible over F and suppose that F contains a primitive n-th root of unity. Then $x^n - a$ and $x^n - b$ have the same splitting field over F if and only if $b = c^n a^r$ for some $c \in F$ and r relatively prime to n. *Hint*: if the splitting fields are the same, consider how the common Galois group acts on a root of each binomial.

16. Let $F < E$ be a finite Galois extension and let α, $\beta \in E$ have degrees m and n over F, respectively. Suppose that $[F(\alpha,\beta):F] = mn$.
    1) Show that if α_i is a conjugate of α and β_j is a conjugate of β then there is a $\sigma \in G_F(E)$ such that $\sigma\alpha = \alpha_i$ and $\sigma\beta = \beta_j$. Hence, the conjugates of $\alpha + \beta$ are $\alpha_i + \beta_j$.
    2) Show that if the difference of two conjugates of α is never equal to the difference of two conjugates of β then $F(\alpha,\beta) = F(\alpha + \beta)$.
17. Let r be a prime different from char(F). Let $f(x) = x^r - u$ and $g(x) = x^r - v$ be irreducible over F, with roots α and β, respectively. Use the previous problem to show that if $[F(\alpha,\beta):F] = r^2$ then $F(\alpha,\beta) = F(\alpha + \beta)$.

Chapter 14
Families of Binomials

In this chapter, we look briefly at families of binomials and their splitting fields and Galois groups. We have seen that when the base field F contains a primitive n-th root of unity, cyclic extensions of degree $d \mid n$ correspond to splitting fields of a single binomial $x^n - u$. More generally, we will see that abelian extensions of exponent n correspond to splitting fields of families of binomials. We will also address the issue of when two families of binomials have the same splitting field.

14.1 The Splitting Field

Let F be a field containing a primitive n-th root of unity and consider a family $\mathfrak{F}$ of binomials given by

$$\mathfrak{F} = \{x^n - u \mid u \in U\}$$

where $U \subseteq F$ is the set of constant terms. We will refer to n as the **exponent** of the family $\mathfrak{F}$.

If S_u is the splitting field for $x^n - u$, then $S = \vee\{S_u \mid u \in U\}$ is the splitting field for the family $\mathfrak{F}$. Since each extension $F < S_u$ is Galois, so is $F < S$ and Theorem 5.5.3 implies that $G_F(S)$ is isomorphic to a subgroup of the product

$$H = \prod_{u \in U} G_F(S_u)$$

Since each $F < S_u$ is cyclic of degree dividing n, the group H is the direct product of cyclic groups of order dividing n and is therefore abelian with exponent n. (Recall that a group G has *exponent* n if $\alpha^n = 1$ for all $\alpha \in G$.) Hence, $G_F(S)$ is abelian with exponent n. An abelian extension $F < S$ whose Galois group $G_F(S)$ has exponent n will be referred to as an abelian extension with **exponent n.**

Thus, if F contains a primitive n-th root of unity, the splitting field of any family of binomials over F of exponent n is an abelian extension of F with exponent n. Happily, the converse is also true.

Suppose that $F < E$ is an abelian extension with exponent n. Let K be any field for which $F < K < E$ where $F < K$ is finite. Since $F < E$ is abelian, so is $F < K$. In addition, $G_F(K)$ is finite and has exponent n. Since a finite abelian group is a direct product of cyclic subgroups, we have

$$G_F(K) \simeq G_1 \times \cdots \times G_m$$

where each G_i is cyclic with exponent n and hence order $n_i \mid n$. Corollary 5.5.4 implies that K is a composite $K = K_1 \cdots K_m$ where $G_F(K_i) \simeq G_i$ is cyclic of order $n_i \mid n$. Since F contains the n_i-th roots of unity and $F < K_i$ is cyclic, Theorem 11.1.1 implies that $K_i = F(\alpha_i)$ is the splitting field for

$$min(\alpha_i, F) = x^{n_i} - \alpha_i^{n_i}$$

where $\alpha_i \in E$. Hence $K = F(\alpha_1, \ldots, \alpha_m)$ is the splitting field over F for the family

$$\mathcal{F}_K = \{x^{n_i} - \alpha_i \mid i = 1, \ldots, m\}$$

It follows that E is the splitting field for the union $\bigcup \mathcal{F}_K$, taken over all finite intermediate fields K.

Theorem 14.1.1 Let F be a field containing a primitive n-th root of unity. An extension $F < E$ is abelian with exponent n if and only if E is the splitting field for a family of binomials over F of exponent n. □

Definition Let F be a field containing a primitive n-th root of unity. An extension $F < E$ is a **Kummer extension** of exponent n if $F < E$ is abelian and has exponent n. □

Thus, according to Theorem 14.1.1, the Kummer extensions of F of exponent n are precisely the splitting fields over F of families of binomials of exponent n.

14.2 Kummer Theory

While each family of binomials gives rise to a unique Kummer extension, different families may produce the same extension, that is, different families may have the same splitting field. We seek a collection of families of binomials such that there is a one-to-one correspondence between families in the collection and Kummer extensions.

Let us phrase the problem a little differently, for which we require some notation. Recall that if $u \in F$, then by $u^{1/n}$ we mean a particular (fixed) root of $x^n - u$. If $A \subseteq F$, we let $A^{1/n}$ denote the set of *all* n-th roots of all elements of A. Also, if $A \subseteq F$ and n is a nonnegative integer then $A^n = \{a^n \mid a \in A\}$.

Let F be a field containing a primitive n-th root of unity. Of course, we may identify a family $\mathfrak{F} = \{x^n - b \mid b \in U\}$ of binomials of (fixed) exponent n with the set $U \subseteq F^*$ of constant terms (since binomials with zero constant term are not very interesting, we exclude such binomials). Moreover, the splitting field for $\mathfrak{F}$ is $S = F(U^{1/n})$.

In seeking a bijective correspondence between subsets $U \subseteq F^*$ and splitting fields $S = F(U^{1/n})$, it is natural to restrict attention to maximal sets $U \subseteq F^*$ that generate the given splitting field. As we now show, if $S = F(U^{1/n})$ for some $U \subseteq F^*$, then

$$S = F(\langle U, F^{*n}\rangle^{1/n})$$

where $\langle U, F^{*n}\rangle$ is the subgroup of F^* generated by U and F^{*n}. To see this, note that if $u_1, \ldots, u_k \in U$ and $f \in F^*$ then for some integer j, we have

$$(f^n u_1^{e_1} \cdots u_k^{e_k})^{1/n} = \omega_n^j f(u_1^{1/n})^{e_1} \cdots (u_k^{1/n})^{e_k} \in F(U^{1/n})$$

and so we get nothing new in $F(U^{1/n})$ by adjoining any element of

$$\langle U, F^{*n}\rangle = \{f^n u_1^{e_1} \cdots u_k^{e_k} \mid f \in F^*, u_i \in U\}$$

That is to say,

$$F(\langle U, F^{*n}\rangle^{1/n}) = F(U^{1/n})$$

It follows that, as far as splitting fields for families of binomials of exponent n are concerned, we may restrict attention to sets of constant terms that are subgroups of F^* containing F^{*n}. Indeed, we will show that if $\mathfrak{U}_n$ is the class of all subgroups U of F^* containing F^{*n} then the association $U \mapsto F(U^{1/n})$ is a bijection onto the class $\mathfrak{K}_n$ of all Kummer extensions E of F with exponent n. We will also obtain a description of

the Galois group G of $F < E$ in terms of U.

Let $F < F(U^{1/n})$ be a Kummer extension with Galois group G, and let $\sigma \in G$ and $u \in U$. If α is a root of $x^n - u$ then $\sigma\alpha$ is also a root of $x^n - u$ and so

$$\sigma\alpha = \omega_{\sigma,\alpha}\alpha$$

for some n-th root of unity $\omega_{\sigma,\alpha}$. If β is another root of $x^n - u$, then $\beta = \omega^i\alpha$ where $\omega \in \Omega_n$ and so $\sigma(\beta/\alpha) = \sigma(\omega^i) = \omega^i = \beta/\alpha$. It follows that

$$\omega_{\sigma,\beta} = \frac{\sigma\beta}{\beta} = \frac{\sigma\alpha}{\alpha} = \omega_{\sigma,\alpha}$$

Hence, $\omega_\sigma = \omega_{\sigma,\alpha}$ depends only on σ.

It follows that the map $\langle , \rangle : G \times U \to U_n$ defined by

$$\langle \sigma, u \rangle = \omega_\sigma = \frac{\sigma\alpha}{\alpha}, \text{ for any } \alpha \text{ with } \alpha^n = u$$

is well-defined (does not depend on α) and we may write

$$\langle \sigma, u \rangle = \frac{\sigma u^{1/n}}{u^{1/n}} \tag{14.2.1}$$

without ambiguity. Moreover, if $\alpha^n = u$ and $b^n = v$ then for $\sigma, \tau \in G$,

$$\langle \sigma\tau, u \rangle = \frac{\sigma\tau\alpha}{\alpha} = \frac{\omega_\tau\omega_\sigma\alpha}{\alpha} = \omega_\tau\omega_\sigma = \frac{\sigma\alpha}{\alpha}\frac{\tau\alpha}{\alpha} = \langle \sigma, u \rangle \langle \tau, u \rangle$$

and

$$\langle \sigma, uv \rangle = \frac{\sigma(\alpha\beta)}{\alpha\beta} = \frac{\sigma\alpha}{\alpha}\frac{\sigma\beta}{\beta} = \langle \sigma, u \rangle \langle \sigma, v \rangle$$

Thus, for each $\sigma \in G$, the map $\psi_\sigma : U \to U_n$ defined by $\psi_\sigma u = \langle \sigma, u \rangle$ is a group homomorphism and for each $u \in U$, the map $\theta_u : G \to U_n$ defined by $\theta_u\sigma = \langle \sigma, u \rangle$ is also a group homomorphism. This prompts a discussion of the following notions.

Dual Groups and Pairings

If A and B are groups, we denote by Hom(A,B) the set of all group homomorphisms from A to B. Note that Hom(A,B) is a group under the product

$$(\psi\theta)(\alpha) = (\psi\alpha)(\theta\alpha)$$

with identity being the constant map $\psi\alpha = 1$ for all $\alpha \in A$. Using this notation, we can state with regard to the pairing (14.2.1), that $\psi_\sigma \in$

$\mathrm{Hom}(U,U_n)$, for all $\sigma \in G$ and $\theta_u \in \mathrm{Hom}(G,U_n)$, for all $u \in U$.

Lemma 14.2.1

1) If A, B and C are abelian groups then

$$\mathrm{Hom}(A \times B,C) \simeq \mathrm{Hom}(A,C) \times \mathrm{Hom}(B,C)$$

2) If A is a finite abelian group of exponent n, then $\mathrm{Hom}(A,U_n) \simeq A$. Hence, $|\mathrm{Hom}(A,U_n)| = |A|$.

Proof. We leave it as an exercise to show that the map

$$\mathfrak{P}:\mathrm{Hom}(A,C) \times \mathrm{Hom}(B,C) \to \mathrm{Hom}(A \times B,C)$$

defined by

$$\mathfrak{P}(\psi,\theta)(\alpha,\beta) = \psi(\alpha)\theta(\beta)$$

is an isomorphism, proving part 1). For part 2), since A can be written as the product of finite cyclic groups, part 1) implies that we need only show that $\mathrm{Hom}(A,U_n) \simeq A$ when $A = \langle\alpha\rangle$ is cyclic. If A has order $m \mid n$, then $\psi \in \mathrm{Hom}(A,U_n)$ maps A into U_m, since for any $\alpha \in A$ we have

$$(\psi\alpha)^m = \psi(\alpha^m) = \psi 1 = 1$$

Suppose that $U_m = \langle\omega\rangle$ and let $\psi \in \mathrm{Hom}(A,U_n)$ be defined by $\psi(\alpha) = \omega$. Then

$$\langle\psi\rangle = \{\iota,\psi, \psi^2,\ldots,\psi^{m-1}\}$$

is a cyclic subgroup of $\mathrm{Hom}(A,U_n)$ of order $m = |U_m|$. Since every element of $\mathrm{Hom}(A,U_n)$ is uniquely determined by its value on α, we deduce that $\mathrm{Hom}(A,U_n) = \langle\psi\rangle$ is cyclic of order m, whence $\mathrm{Hom}(A,U_n) \simeq A$. ∎

Definition If A, B and C are abelian groups, a **pairing** of $A \times B$ into C is a map $\langle,\rangle:A \times B \to C$ that is a "bihomomorphism", that is,

1) For each $\alpha \in A$, the map $\psi_\alpha:B \to C$ defined by $\psi_\alpha(\beta) = \langle\alpha,\beta\rangle$ is a group homomorphism.
2) For each $\beta \in B$, the map $\theta_\beta:A \to C$ defined by $\theta_\beta(\alpha) = \langle\alpha,\beta\rangle$ is a group homomorphism. □

A pairing is the analog of a bilinear map between vector spaces. Note that $\langle 1,\beta\rangle = \langle\alpha,1\rangle = 1$ for all $\alpha \in A$ and $\beta \in B$ and that $\langle\alpha,\beta\rangle^{-1} = \langle\alpha^{-1},\beta\rangle = \langle\alpha,\beta^{-1}\rangle$. If $S \subseteq A$ and $T \subseteq B$, we set

$$\langle S,T\rangle = \{\langle s,t\rangle \mid s \in S,\ t \in T\}$$

(We will write $\langle\{\alpha\},T\rangle$ as $\langle\alpha,T\rangle$ and $\langle S,\{\beta\}\rangle$ as $\langle S,\beta\rangle$.) The **left kernel** of a pairing is the set

$$K_L = \{\alpha \in A \mid \langle\alpha,B\rangle = \{1\}\}$$

and the **right kernel** is defined similarly

$$K_R = \{\beta \in B \mid \langle A,\beta\rangle = \{1\}\}$$

It is easy to see that these kernels are subgroups of their respective parent groups.

Note that $\langle\alpha_1,\beta\rangle = \langle\alpha_2,\beta\rangle$ for all $\beta \in B$ if and only if $\langle\alpha_1\alpha_2^{-1},B\rangle = \{1\}$, that is, if and only if $\alpha_1\alpha_2^{-1} \in K_L$, or equivalently, $\alpha_1 K_L = \alpha_2 K_L$. Similar statements holds for the right kernel. Thus, we may define a pairing from $A/K_L \times B/K_R$ to C by

$$\langle\alpha K_L,\beta K_R\rangle = \langle\alpha,\beta\rangle$$

and this pairing is **nonsingular**, that is, both the left and right kernels are trivial.

Theorem 14.2.2 Let $\langle,\rangle: A \times B \to U_n$ be a nonsingular pairing from abelian groups A and B into U_n. Then A and B both have exponent n. Moreover, A is finite if and only if B is finite, in which case

1) $A \simeq \mathrm{Hom}(B,U_n)$ and $B \simeq \mathrm{Hom}(A,U_n)$,
2) $|A| = |B|$.

Proof. First observe that if $\alpha \in A$ then $\langle\alpha^n,\beta\rangle = \langle\alpha,\beta\rangle^n = 1$ for all $\beta \in B$, and so $\alpha^n \in K_L$, whence $\alpha^n = 1$ and A has exponent n. A similar statement holds for B. Now consider the map $A \to \mathrm{Hom}(B,U_n)$ defined by $\alpha \mapsto \psi_\alpha$, where $\psi_\alpha: \beta \mapsto \langle\alpha,\beta\rangle$. Since

$$\psi_{\alpha\alpha'}(\beta) = \langle\alpha\alpha',\beta\rangle = \langle\alpha,\beta\rangle\langle\alpha',\beta\rangle = \psi_\alpha(\beta)\psi_{\alpha'}(\beta)$$

the map $\alpha \mapsto \psi_\alpha$ is a group homomorphism from A to $\mathrm{Hom}(B,U_n)$. If $\psi_\alpha = 1$ is the constant homomorphism then $\langle\alpha,\beta\rangle = 1$ for all $\beta \in B$, that is, $\alpha \in K_R$, whence $\alpha = 1$. Hence, the map $\alpha \mapsto \psi_\alpha$ is injective.

It follows from Lemma 14.2.1 that if B is finite, then

$$|A| \leq |\mathrm{Hom}(B,U_n)| = |B|$$

The dual argument shows that $|B| \leq |A|$ and so $|A| = |B|$. This also implies that the monomorphism $\alpha \mapsto \psi_\alpha$ is an isomorphism. ∎

Back to Binomials

We resume our study of the pairing $\langle , \rangle : G \times U \to U_n$ defined by

$$\langle \sigma, u \rangle = \frac{\sigma u^{1/n}}{u^{1/n}}$$

Since the identity is the only map in G that fixes every root of every binomial in the family, the left kernel of this pairing is

$$K_L = \{\sigma \in G \mid \sigma u^{1/n} = u^{1/n} \text{ for all } u \in U\} = \{\iota\}$$

An element $u \in U$ is in the right kernel if and only if

$$\sigma u^{1/n} = u^{1/n}$$

for all $\sigma \in G$, that is, if and only if $u^{1/n} \in F(G)^* = F^*$. Since $u^{1/n} \in F^*$ if and only if $u \in F^{*n}$, we have $K_R = F^{*n}$.

It follows that the pairing $\langle , \rangle : G \times (U/F^{*n}) \to U_n$ given by

$$\langle \sigma, uF^{*n} \rangle = \frac{\sigma u^{1/n}}{u^{1/n}}$$

is nonsingular. We may thus apply Theorem 14.2.2.

Theorem 14.2.3 Let F be a field containing a primitive n-th root of unity. If $E = F(U^{1/n})$ then the pairing

$$\langle , \rangle : G_F(E) \times U/F^{*n} \to U_n$$

given by

$$\langle \sigma, uF^{*n} \rangle = \frac{\sigma u^{1/n}}{u^{1/n}}$$

is nonsingular and so U/F^{*n} has exponent n and $|G_F(E)| = [E:F]$ is finite if and only if $(U:F^{*n})$ is finite, in which case

$$[E:F] = (U:F^{*n})$$

and

$$G_F(E) \simeq \mathrm{Hom}(U/F^{*n}, U_n)$$ □

Theorem 14.3.1 not only describes the Galois group of a Kummer extension, but allows us to show that the map $U \mapsto F(U^{1/n})$, from $\mathfrak{U}_n$ to $\mathfrak{K}_n$, is a bijection.

Theorem 14.2.4 Let F be a field containing a primitive n-th root of unity. Let $\mathfrak{K}_n$ be the class of all Kummer extensions $F < E$ of F with exponent n and let $\mathfrak{U}_n$ be the class of all subgroups U of F^* containing F^{*n}. Then the map $U \mapsto F(U^{1/n})$ is a bijection from $\mathfrak{U}_n$ onto $\mathfrak{K}_n$ with inverse given by $E \mapsto E^{*n} \cap F^*$

Proof. To show that the map in question is injective, suppose that $F(U^{1/n}) = F(V^{1/n})$, with $U, V \in \mathfrak{U}_n$. If $u \in U$, then $u^{1/n} \in F(V^{1/n})$ and so there exists a finite subset V_0 of V for which $u^{1/n} \in F(V_0^{1/n})$. Let $V_1 = \langle V_0, F^{*n} \rangle$ be the subgroup generated by V_0 and F^{*n}. Then

$$V_0^{1/n} \subseteq V_1^{1/n} \subseteq V^{1/n}$$

and

$$u^{1/n} \in F(V_0^{1/n}) \subseteq F(V_1^{1/n})$$

Note that $V_1 \in \mathfrak{U}_n$ is finitely generated (by V_0) over F^{*n} and hence $(V_1:F^{*n})$ is finite. Theorem 14.2.3 implies that

$$[F(V_1^{1/n}):F] = (V_1:F^{*n})$$

Let us now adjoin u. Let $V_2 = \langle u, V_1 \rangle$ be the subgroup generated by u and V_1. Then $V_2 \in \mathfrak{U}_n$ and

$$F(V_2^{1/n}) = F(\langle u, V_1 \rangle^{1/n}) = F(\langle \alpha, V_1^{1/n} \rangle) = F(V_1^{1/n})$$

Another application of Theorem 14.2.3 gives

$$(V_2:F^{*n}) = (V_1:F^{*n})$$

and since $V_1 \subseteq V_2$ we get $V_1 = V_2$. It follows that $u \in V_1 \subseteq V$ and since u was arbitrary, $U \subseteq V$. A symmetric argument gives $V \subseteq U$, whence $U = V$. This proves that the map $U \mapsto F(U^{1/n})$ is injective. We have seen that any Kummer extension $F < E$ in $\mathfrak{K}_n$ is a splitting field extension for a family $\mathfrak{F}$ of binomials with exponent n. If C is the set of constant terms and if U is the subgroup of F^* generated by C and F^{*n} then $E = F(U^{1/n})$ and so the map is surjective.

Let $F < E$ be a Kummer extension with exponent n and let $U = E^{*n} \cap F^*$. Then U is a subgroup of F^* containing F^{*n}, that is, $U \in \mathfrak{U}_n$. It is clear that $E \subseteq F(U^{1/n})$. For the reverse inclusion, let $\beta^n \in U$. Then $\beta^n = \alpha^n$ for some $\alpha \in E^*$, which implies that β is a root of $x^n - \alpha^n \in$

$F[x]$ and so $\beta = \omega^i\alpha \in E^*$. This shows that $U^{1/n} \subseteq E^*$ and so $E = F(U^{1/n})$. Hence, $E \mapsto U = E^{*n} \cap F^*$ is the inverse map. ∎

Exercises

1. Referring to Lemma 14.2.1, show that the map

$$\mathfrak{P}:\mathrm{Hom}(A,C) \times \mathrm{Hom}(B,C) \to \mathrm{Hom}(A \times B,C)$$

defined by

$$\mathfrak{P}(\psi,\theta)(\alpha,\beta) = \psi(\alpha)\theta(\beta)$$

is an isomorphism.

2. Let A be a finite group and let $\psi \in \mathrm{Hom}(G,U_n)$. Show that $\sum_{a \in A}\psi(a) = |A|$ if $\psi(a) = 1$ for all $a \in A$ and $\sum_{a \in A}\psi(a) = 0$ otherwise.
3. Let A be a finite abelian group with exponent n. If $\alpha \in A$ satisfies $\psi(\alpha) = 1$ for all $\psi \in \mathrm{Hom}(A,U_n)$ then $\alpha = 1$.
4. Let B be a proper subgroup of a finite abelian group A and let $\alpha \in A - B$. Then there exists $\psi \in \mathrm{Hom}(A,U_n)$ such that $\psi(B) = \{1\}$ but $\psi(\alpha) \neq 1$.
5. Let A be a finite abelian group and let B be a subgroup of A. Let $B^{\perp} = \{\psi \in \mathrm{Hom}(A,U_n) \mid \psi(B) = \{1\}\}$. Show that $\mathrm{Hom}(B,U_n) \simeq \mathrm{Hom}(A,U_n)/B^{\perp}$.
6. Let B be a subgroup of a finite abelian group A. Let $B^{\perp} = \{\psi \in \mathrm{Hom}(A,U_n) \mid \psi(B) = \{1\}\}$. Show that $\mathrm{Hom}(A/B,U_n) \simeq B^{\perp}$.
7. Let $\mathfrak{F} = \{f_i(x)\}$ be a family of binomials with *deg* $f_i(x) = n_i$. Suppose that $n_i \mid n$ for all i and let F contain a primitive n-th root of unity. Show that there is a family of binomials, each of which has degree n, with the same splitting field as $\mathfrak{F}$.
8. In this exercise, we develop the analogous theory for families of polynomials of the form $\mathfrak{F} = \{x^p - x - u_i\}$ where $p = \mathrm{char}(F) \neq 0$.
   1) Prove that $F < E$ is abelian with exponent p if and only if E is the splitting field of a family of the form $\mathfrak{F}$.
   2) Let $\mathfrak{P}:\overline{F} \to \overline{F}$ be the map $\mathfrak{P}\alpha = \alpha^p - \alpha$. Let $\mathfrak{P}^{-1}U = \{\alpha \in \overline{F}$ such that $\mathfrak{P}\alpha \in U\}$. Let $\mathfrak{U}$ be the class of all *additive* subgroups of F with $\mathfrak{P}^{-1}F \subseteq U$. Let $\mathfrak{E}_p$ be the class of all abelian extensions $F < E$ of F with exponent p. Prove the following theorem: The map $U \mapsto F(\mathfrak{P}^{-1}U)$ is a bijection between $\mathfrak{U}$ and $\mathfrak{E}_p$. If $F < E = F(\mathfrak{P}^{-1}U)$ is in $\mathfrak{E}_p$ has Galois group G then there is a well-defined pairing $\langle,\rangle:G \times U \to U_p$ given by $\langle\sigma,\alpha\rangle = \sigma\beta - \beta$ for any $\beta \in \mathfrak{P}^{-1}\alpha$. The left kernel is $\{1\}$ and the right kernel is $\mathfrak{P}F$. The extension $F < E$ is finite if and only if $(U:\mathfrak{P}F)$ is finite, in which case $[E:F] = (U:\mathfrak{P}F)$ and $G \simeq (U/\mathfrak{P}F)^{\wedge}$.

Appendix
Möbius Inversion

Möbius inversion is a method for inverting certain types of sums. The classical form of Möbius inversion was originally developed independently by P. Hall and L. Weisner in 1935. However, in 1964, Gian-Carlo Rota generalized the classical form to apply to a much wider range of situations. To describe the concept in its fullest generality, we require some facts about partially ordered sets.

PARTIALLY ORDERED SETS

Definition A **partial order** on a nonempty set P is a binary relation, denoted by $\leq$ and read "less than or equal to," with the following properties.

1) (**reflexivity**) For all $a \in P$,
$$a \leq a$$

2) (**antisymmetry**) For all $a,b \in P$,
$$a \leq b \text{ and } b \leq a \text{ implies } a = b$$

3) (**transitivity**) For all $a,b,c \in P$,
$$a \leq b \text{ and } b \leq c \text{ implies } a \leq c$$ □

Definition A **partially ordered set** is a nonempty set P, together with a partial order $\leq$ defined on P. The expression $a \leq b$ is read "a is less

than or equal to b." If $a,b \in P$, we denote the fact that a is *not* less than or equal to b by $a \not\leq b$. Also, we denote the fact that $a \leq b$, but $a \neq b$, by $a < b$.

If there exists an element $z \in P$ for which $z \leq x$ for all $x \in P$, we call z a **zero** element and denote it by 0. Similarly, if there exists an element $y \in P$ for which $x \leq y$ for all $x \in P$, then we call y a **one** and denote it by 1. □

As is customary, when the partial order $\leq$ is understood, we will use the phrase "let P be a partially ordered set."

Note that, in a partially ordered set, it is possible that not all elements are comparable. In other words, it is possible to have $x,y \in P$ with the property that $x \not\leq y$ and $y \not\leq x$. Thus, in general, $x \not\leq y$ is *not* equivalent to $y \leq x$. A partially ordered set in which every pair of elements is comparable is called a **totally ordered set** or a **linearly ordered set.**

Example A.2.1

1) The set $\mathbb{R}$ of real numbers, with the usual binary relation $\leq$, is a partially ordered set. It is also a totally ordered set.
2) The set $\mathbb{N}$ of natural numbers, together with the binary relation of divides, is a partially ordered set. It is customary to write $n \mid m$ (rather than $n \leq m$) to indicate that n divides m.
3) Let S be any set, and let $\mathcal{P}(S)$ be the power set of S, that is, the set of all subsets of S. Then $\mathcal{P}(S)$, together with the subset relation $\subseteq$, is a partially ordered set. □

Definition Let P be a partially ordered set. For $a,b \in P$, the **(closed) interval** [a,b] is the set

$$[a,b] = \{x \in P \mid a \leq x \leq b\}$$

We say that the partially ordered set P is **locally finite** if every closed interval is a finite set. □

Notice that, if P is locally finite and contains a zero element 0, then the set $\{x \in P \mid x \leq a\}$ is finite for all $a \in P$, for it is the same as the interval [0,a].

THE INCIDENCE ALGEBRA OF A PARTIALLY ORDERED SET

Now let P be a locally finite partially ordered set, and let F be a field. We set

$$\mathcal{A}(P) = \{f:P \times P \to F \mid f(x,y) = 0 \text{ if } x \not\leq y\}$$

Addition and scalar multiplication are defined on $\mathcal{A}(P)$ by

$$(f+g)(x,y) = f(x,y) + g(x,y)$$

and

$$(kf)(x,y) = k[f(x,y)]$$

We also define multiplication by

$$(f*g)(x,y) = \sum_{x \leq z \leq y} f(x,z)g(z,y)$$

the sum being finite, since P is assumed to be locally finite. Using these definitions, it is not hard to show that $\mathcal{A}(P)$ is an algebra, called the **incidence algebra** of P. The identity in this algebra is

$$\delta(x,y) = \begin{cases} 1 & \text{if } x = y \\ 0 & \text{if } x \neq y \end{cases}$$

The next theorem characterizes those elements of $\mathcal{A}(P)$ that have multiplicative inverses.

Theorem A.2.1 An element $f \in \mathcal{A}(P)$ is invertible if and only if $f(x,x) \neq 0$ for all $x \in P$.

Proof. An inverse g of f must satisfy

$$\sum_{x \leq z \leq y} f(x,z)g(z,y) = \delta(x,y) \tag{A.2.1}$$

In particular, for $x = y$, we get

$$f(x,x)g(x,x) = 1$$

This shows the necessity and also that g(x,x) must satisfy

$$g(x,x) = \frac{1}{f(x,x)} \tag{A.2.2}$$

Équation (A.2.2) defines g(x,y) when the interval [x,y] has cardinality 1, that is, when $x = y$. We can use (A.2.1) to define g(x,y) for intervals [x,y] of all cardinalities.

Suppose that g(x,y) has been defined for all intervals with cardinality at most n, and let [x,y] have cardinality n+1. Then, by (A.2.1), since $x \neq y$, we get

$$f(x,x)g(x,y) = -\sum_{x < z \leq y} f(x,z)g(z,y)$$

But g(z,y) is defined for $z > x$ since [z,y] has cardinality at most n, and so we can use this to define g(x,y). ∎

Definition The function $\zeta \in \mathcal{A}(P)$, defined by

$$\zeta(x,y) = \begin{cases} 1 & \text{if } x \leq y \\ 0 & \text{if } x \not\leq y \end{cases}$$

is called the **zeta function.** Its inverse $\mu(x,y)$ is called the **Möbius function.** □

The next result follows from the appropriate definitions.

Theorem A.2.2 The Möbius function is uniquely determined by any of the following conditions.

1) $\mu(x,x) = 1$ and, for $x < y$,

$$\sum_{x \leq z \leq y} \mu(z,y) = 0$$

2) $\mu(x,x) = 1$ and, for $x < y$,

$$\sum_{x \leq z \leq y} \mu(x,z) = 0$$

3) $\mu(x,x) = 1$ and, for $x < y$,

$$\mu(x,y) = -\sum_{x < z \leq y} \mu(z,y)$$

4) $\mu(x,x) = 1$ and, for $x < y$,

$$\mu(x,y) = -\sum_{x \leq z < y} \mu(x,z)$$ □

Now we come to the main result.

Theorem A.2.3 (Möbius Inversion) Let P be a locally finite partially ordered set with zero element 0. If f and g are functions from P to the field F, then

$$\text{(A.2.4)} \qquad g(x) = \sum_{y \leq x} f(y) \quad \Rightarrow \quad f(x) = \sum_{y \leq x} g(y)\mu(y,x)$$

If P is a locally finite partially ordered set with 1, then

$$\text{(A.2.5)} \qquad g(x) = \sum_{x \leq y} f(y) \quad \Rightarrow \quad f(x) = \sum_{x \leq y} \mu(x,y)g(y)$$

Proof. Since all sums are finite, we have, for any x,

$$\begin{aligned}\sum_{y \le x} g(y)\mu(y,x) &= \sum_{y \le x}\left[\sum_{z \le y} f(z)\right]\mu(y,x) \\ &= \sum_{z \le x}\ \sum_{z \le y \le x} f(z)\mu(y,x) \\ &= \sum_{z \le x} f(z) \sum_{z \le y \le x} \mu(y,x) \\ &= \sum_{z \le x} f(z)\delta(z,x) = f(x)\end{aligned}$$

The rest of the theorem is proved similarly. ∎

The formulas (A.2.4) and (A.2.5) are called **Möbius inversion formulas.**

Example A.2.2 (Subsets) Let $P = \mathcal{P}(S)$ be the set of all subsets of a finite set S, partially ordered by set inclusion. We will use the notation $\subseteq$ for subset and $\subset$ for *proper* subset. (In the text, we use $\subset$ for subset.) The zeta function is

$$\zeta(A,B) = \begin{cases} 1 & \text{if } A \subseteq B \\ 0 & \text{otherwise} \end{cases}$$

The Möbius function μ is computed as follows. From Theorem A.2.2, we have

$$\mu(A,A) = 1$$

and

$$\mu(A,B) = -\sum_{A \subseteq X \subset B} \mu(A,X)$$

So, for $x,y,z \notin A$, we have

$$\begin{aligned}\mu(A,A \cup \{x\}) &= -\mu(A,A) = -1 \\ \mu(A,A \cup \{x,y\}) &= -\mu(A,A) - \mu(A,A \cup \{x\}) - \mu(A,A \cup \{y\}) \\ &= -1+1+1 = 1 \\ \mu(A,A \cup \{x,y,z\}) &= -\mu(A,A) - \mu(A,A \cup \{x\}) - \mu(A,A \cup \{y\}) \\ &= -\mu(A,A \cup \{x,y\}) - \mu(A,A \cup \{x,z\}) - \mu(A,A \cup \{y,z\}) \\ &= -1+1+1+1-1-1-1 = -1\end{aligned}$$

It begins to appear that the values of μ alternate between $+1$ and -1 and that

$$\mu(A,B) = \begin{cases} (-1)^{|B-A|} & \text{if } A \subseteq B \\ 0 & \text{otherwise} \end{cases}$$

To verify this, we have $\mu(A,A) = 1$ and, for $A \subseteq B$,

$$\sum_{A \subseteq X \subseteq B} (-1)^{|B-A|} = \sum_{k=0}^{|B-A|} \binom{|B-A|}{k} (-1)^k = 0$$

Now let $P_1,\ldots,P_n$ be properties that the elements of a set S may or may not possess. For $K \subseteq \{1,\ldots,k\}$, let E(K) be the number of elements of S that have properties P_i for $i \in K$, *and no others.* Let F(K) be the number of elements of S that have *at least* properties P_i, for $i \in K$. Then

$$F(K) = \sum_{K \subseteq L} E(L)$$

Hence, by Möbius inversion,

$$E(K) = \sum_{K \subseteq L} (-1)^{|L-K|} F(L)$$

In particular, if $K = \emptyset$ is the empty set, then

$$E(\emptyset) = \sum_{L \subseteq S} (-1)^{|L|} F(L)$$

But $E(\emptyset)$ is the number of elements of S that have *none* of the properties, and so we get

$$\text{Number elements with no properties} = \sum_{k \geq 0} (-1)^k \sum_{i_1,\ldots,i_k} F(\{i_1,\ldots,i_k\})$$

This formula is the well known Principle of Inclusion-Exclusion, which we now see is just a special case of Möbius inversion. □

CLASSICAL MOBIUS INVERSION

Consider the partially ordered set $\mathbb{N}$ of natural numbers, ordered by division. That is, x is less than or equal to y if and only if x divides y, which we will denote by $x \mid y$. Notice that the natural number 1 (and *not* 0) is the zero element in this partially ordered set, since $1 \mid n$ for any natural number n.

In this case, the Möbius function $\mu(x,y)$ depends only on the ratio y/x, and is given by

$$\mu(x,y) = \mu(\tfrac{y}{x}) = \begin{cases} 1 & \text{if } \frac{y}{x} = 1 \\ (-1)^k & \text{if } \frac{y}{x} = p_1 p_2 \cdots p_k \text{ for } \textit{distinct} \text{ primes } p_i \\ 0 & \text{otherwise} \end{cases}$$

Notice that the "otherwise" case can occur if either $x \nmid y$ (x does not divide y) or if $p^2 \mid (y/x)$ for some prime p. Thus, the value of $\mu(x,y)$ depends on the nature of the prime decomposition of the ratio y/x.

To verify that this is indeed the Möbius function, we first observe that $\mu(x,x) = \mu(1) = 1$. Now let $x \mid y$, $x \neq y$ and

$$\frac{y}{x} = p_1^{e_1} p_2^{e_2} \cdots p_n^{e_n}$$

where the p_i are *distinct* primes. Then

$$\sum_{x \mid z \mid y} \mu(\tfrac{z}{x}) = \sum_{1 \mid \frac{z}{x} \mid \frac{y}{x}} \mu(\tfrac{z}{x}) = \sum_{1 \mid k \mid \frac{y}{x}} \mu(k) = \sum_{1 \leq j \leq n} \binom{n}{j} (-1)^j = 0$$

Now, in the present context, the Möbius inversion formula becomes

$$g(n) = \sum_{k \mid n} f(k) \quad \Rightarrow \quad f(n) = \sum_{k \mid n} g(k)\mu(\tfrac{n}{k})$$

This is the important classical formula, which often goes by the name Möbius inversion formula. □

MULTIPLICATIVE VERSION OF MOBIUS INVERSION

We now present a multiplicative version of the Möbius inversion formula.

Theorem A.2.4 Let P be a locally finite partially ordered set with zero element 0. If f and g are functions from P to F, then

$$g(x) = \prod_{y \leq x} f(y) \quad \Rightarrow \quad f(x) = \prod_{y \leq x} [g(y)]^{\mu(y,x)}$$

Proof. Since all products are finite, we have, for any x,

$$\prod_{y \leq x} [g(y)]^{\mu(y,x)} = \prod_{y \leq x} \left[\prod_{z \leq y} f(z) \right]^{\mu(y,x)}$$

$$= \prod_{z \leq x} \prod_{z \leq y \leq x} [f(z)]^{\mu(y,x)}$$

$$= \prod_{z \le x} f(z)^{\sum_{z \le y \le x} \mu(y,x)}$$

$$= \prod_{z \le x} f(z)^{\delta(z,x)} = f(x) \qquad \blacksquare$$

Example A.2.3 Let $P = \mathbb{N}$, and let F be the field of rational functions in x. Consider the formula

$$x^n - 1 = \prod_{k \mid n} Q_k(x)$$

Then, if we let $f(k) = Q_k(x)$ and $g(n) = x^n - 1$, Theorem A.2.4 gives

$$Q_n(x) = \prod_{k \mid n} (x^k - 1)^{\mu(n/k)} = \prod_{k \mid n} (x^{n/k} - 1)^{\mu(k)} \qquad \square$$

References

Adamson, I., *Introduction to Field Theory*, 2 ed., Cambridge University Press, 1982.

Artin, Emil, *Galois Theory*, 2 ed., Notre Dame Press, 1959.

Besicovitch, A.S., On the linear independence of fractional powers of integers, *J. London Math. Soc.*, 15 (1940) 3-6.

Brawley, J. and Schnibben, G., *Infinite Algebraic Extensions of Finite Fields*, AMS, 1989.

Edwards, Harold, *Galois Theory*, Springer-Verlag, 1984.

Ellis, Graham, *Rings and Fields*, Oxford University Press, 1993.

Fenrick, Maureen, *Introduction to the Galois Correspondence*, Birkhäuser, 1992.

Gaal, Lisl, *Classical Galois Theory*, 4 ed., Chelsea, 1988.

Garling, D.J.H., *Galois Theory*, Cambridge University Press, 1986.

Hadlock, Charles, *Field Theory and Its Classical Problems*, MAA, 1978.

Jacobson, Nathan, *Basic Algebra II*, Freeman, 1989.

Karpilovsky, G., *Topics in Field Theory*, Elsevier, 1989.

Kuga, M., *Galois' Dream*, Birkhauser, 1993.

Lang, Serge, *Algebra*, 3rd ed., Addison-Wesley, 1993.

Lidl, R. and Niederreiter, H., *Introduction to Finite Fields and Their Applications*, Cambridge University Press, 1986.

McCarthy, Paul, *Algebraic Extensions of Fields*, 2 ed., Dover, 1976.

Nagata, M., *Field Theory*, Marcel Dekker, 1977.

Richards, Ian, An application of Galois theory to elementary arithmetic, *Advances in Mathematics* 13 (1974) 268-273.

Roman, S., *Advanced Linear Algebra*, Springer-Verlag, 1992.

Roman, S., *Coding and Information Theory*, Springer-Verlag, 1992.

Rotman, Joseph, *Galois Theory*, Springer-Verlag, 1990.

Schinzel, A., Abelian binomials, power residues, and exponential congruences, *Acta. Arith.* 32 (1977) 245-274.

Stewart, Ian, *Galois Theory*, 2 ed., Chapman and Hall, 1989.

Winter, D., *The Structure of Fields*, Springer-Verlag, 1974.

Wójcik, J., Contributions to the theory of Kummer extensions, *Acta Arith.* 40 (1982) 155-174.

Note: An extensive bibliography of over 600 entries can be found in Karpilovsky, G., *Topics in Field Theory*, Elsevier, 1989.

Index of Symbols

Index

Graduate Texts in Mathematics

continued from page ii

65 WELLS. Differential Analysis on Complex Manifolds. 2nd ed.
66 WATERHOUSE. Introduction to Affine Group Schemes.
67 SERRE. Local Fields.
68 WEIDMANN. Linear Operators in Hilbert Spaces.
69 LANG. Cyclotomic Fields II.
70 MASSEY. Singular Homology Theory.
71 FARKAS/KRA. Riemann Surfaces. 2nd ed.
72 STILLWELL. Classical Topology and Combinatorial Group Theory. 2nd ed.
73 HUNGERFORD. Algebra.
74 DAVENPORT. Multiplicative Number Theory. 2nd ed.
75 HOCHSCHILD. Basic Theory of Algebraic Groups and Lie Algebras.
76 IITAKA. Algebraic Geometry.
77 HECKE. Lectures on the Theory of Algebraic Numbers.
78 BURRIS/SANKAPPANAVAR. A Course in Universal Algebra.
79 WALTERS. An Introduction to Ergodic Theory.
80 ROBINSON. A Course in the Theory of Groups.
81 FORSTER. Lectures on Riemann Surfaces.
82 BOTT/TU. Differential Forms in Algebraic Topology.
83 WASHINGTON. Introduction to Cyclotomic Fields.
84 IRELAND/ROSEN. A Classical Introduction to Modern Number Theory. 2nd ed.
85 EDWARDS. Fourier Series. Vol. II. 2nd ed.
86 VAN LINT. Introduction to Coding Theory. 2nd ed.
87 BROWN. Cohomology of Groups.
88 PIERCE. Associative Algebras.
89 LANG. Introduction to Algebraic and Abelian Functions. 2nd ed.
90 BRØNDSTED. An Introduction to Convex Polytopes.
91 BEARDON. On the Geometry of Discrete Groups.
92 DIESTEL. Sequences and Series in Banach Spaces.
93 DUBROVIN/FOMENKO/NOVIKOV. Modern Geometry—Methods and Applications. Part I. 2nd ed.
94 WARNER. Foundations of Differentiable Manifolds and Lie Groups.
95 SHIRYAYEV. Probability.
96 CONWAY. A Course in Functional Analysis. 2nd ed.
97 KOBLITZ. Introduction to Elliptic Curves and Modular Forms. 2nd ed.
98 BRÖCKER/TOM DIECK. Representations of Compact Lie Groups.
99 GROVE/BENSON. Finite Reflection Groups. 2nd ed.
100 BERG/CHRISTENSEN/RESSEL. Harmonic Analysis on Semigroups: Theory of Positive Definite and Related Functions.
101 EDWARDS. Galois Theory.
102 VARADARAJAN. Lie Groups, Lie Algebras and Their Representations.
103 LANG. Complex Analysis. 3rd ed.
104 DUBROVIN/FOMENKO/NOVIKOV. Modern Geometry—Methods and Applications. Part II.
105 LANG. $SL_2(\mathbf{R})$.
106 SILVERMAN. The Arithmetic of Elliptic Curves.
107 OLVER. Applications of Lie Groups to Differential Equations. 2nd ed.
108 RANGE. Holomorphic Functions and Integral Representations in Several Complex Variables.
109 LEHTO. Univalent Functions and Teichmüller Spaces.
110 LANG. Algebraic Number Theory.
111 HUSEMÖLLER. Elliptic Curves.
112 LANG. Elliptic Functions.
113 KARATZAS/SHREVE. Brownian Motion and Stochastic Calculus. 2nd ed.
114 KOBLITZ. A Course in Number Theory and Cryptography. 2nd ed.
115 BERGER/GOSTIAUX. Differential Geometry: Manifolds, Curves, and Surfaces.
116 KELLEY/SRINIVASAN. Measure and Integral. Vol. I.
117 SERRE. Algebraic Groups and Class Fields.
118 PEDERSEN. Analysis Now.
119 ROTMAN. An Introduction to Algebraic Topology.
120 ZIEMER. Weakly Differentiable Functions: Sobolev Spaces and Functions of Bounded Variation.

121 LANG. Cyclotomic Fields I and II. Combined 2nd ed.
122 REMMERT. Theory of Complex Functions. *Readings in Mathematics*
123 EBBINGHAUS/HERMES et al. Numbers. *Readings in Mathematics*
124 DUBROVIN/FOMENKO/NOVIKOV. Modern Geometry—Methods and Applications. Part III.
125 BERENSTEIN/GAY. Complex Variables: An Introduction.
126 BOREL. Linear Algebraic Groups.
127 MASSEY. A Basic Course in Algebraic Topology.
128 RAUCH. Partial Differential Equations.
129 FULTON/HARRIS. Representation Theory: A First Course. *Readings in Mathematics*
130 DODSON/POSTON. Tensor Geometry.
131 LAM. A First Course in Noncommutative Rings.
132 BEARDON. Iteration of Rational Functions.
133 HARRIS. Algebraic Geometry: A First Course.
134 ROMAN. Coding and Information Theory.
135 ROMAN. Advanced Linear Algebra.
136 ADKINS/WEINTRAUB. Algebra: An Approach via Module Theory.
137 AXLER/BOURDON/RAMEY. Harmonic Function Theory.
138 COHEN. A Course in Computational Algebraic Number Theory.
139 BREDON. Topology and Geometry.
140 AUBIN. Optima and Equilibria. An Introduction to Nonlinear Analysis.
141 BECKER/WEISPFENNING/KREDEL. Gröbner Bases. A Computational Approach to Commutative Algebra.
142 LANG. Real and Functional Analysis. 3rd ed.
143 DOOB. Measure Theory.
144 DENNIS/FARB. Noncommutative Algebra.
145 VICK. Homology Theory. An Introduction to Algebraic Topology. 2nd ed.
146 BRIDGES. Computability: A Mathematical Sketchbook.
147 ROSENBERG. Algebraic K-Theory and Its Applications.
148 ROTMAN. An Introduction to the Theory of Groups. 4th ed.
149 RATCLIFFE. Foundations of Hyperbolic Manifolds.
150 EISENBUD. Commutative Algebra with a View Toward Algebraic Geometry.
151 SILVERMAN. Advanced Topics in the Arithmetic of Elliptic Curves.
152 ZIEGLER. Lectures on Polytopes.
153 FULTON. Algebraic Topology: A First Course.
154 BROWN/PEARCY. An Introduction to Analysis.
155 KASSEL. Quantum Groups.
156 KECHRIS. Classical Descriptive Set Theory.
157 MALLIAVIN. Integration and Probability.
158 ROMAN. Field Theory.