David Winter

The Structure of Fields

Springer-Verlag New York · Heidelberg · Berlin
World Publishing Corporation, Beijing, China

David Winter

Professor of Mathematics
University of Michigan
Ann Arbor, Michigan 48104

AMS Subject Classifications (1970)
12C05, 12E05, 12Fxx, 12H05

Library of Congress Cataloging in Publication Data

Winter, David J.
Structure of fields.

(Graduate texts in mathematics, v. 16)
1. Fields, Algebraic. 2. Galois theory.
I. Title. II. Series.
QA247.W55 512'.32 73-21824
ISBN 0-387-90074-4

ISBN 0-387-90074-8 Springer-Verlag New York Heidelberg Berlin
ISBN 3-540-90074-8 Springer-Verlag Berlin Heidelberg New York
ISBN 7-5062-0046-5 World Publishing Corporation China

Preface

The theory of fields is one of the oldest and most beautiful subjects in algebra. It is a natural starting point for those interested in learning algebra, since the algebra needed for the theory of fields arises naturally in the theory's development and a wide selection of important algebraic methods are used. At the same time, the theory of fields is an area in which intensive work on basic questions is still being done.

This book was written with the objective of exposing the reader to a thorough treatment of the classical theory of fields and classical Galois theory, to more modern approaches to the theory of fields and to one approach to a current problem in the theory of fields, the problem of determining the structure of radical field extensions.

I have written the book in the form of a text book, and assume that the reader is familar with the elementary properties of vector spaces and linear transformations. The other basic algebra needed for the book is developed in Chapter 0, although a reader with very little background in algebra should also consult other sources. Exercises varying from quite easy to very difficult are included at the end of each chapter. Some of these exercises supplement the text and are referred to at points where readers may want to see further discussion. Others are used to cover in outline form important material peripheral to the main themes in the book.

Chapters 1–4 give a comprehensive treatment of the more classical side of the theory of fields and Galois theory. Chapter 1 and 2 are concerned with the general structure of polynomials and extension fields. Galois theory is developed extensively in Chapter 3. Chapter 4 covers the fundamental theorems on algebraic function fields and relates algebraic function fields and affine algebraic varieties.

In Chapter 5, I discuss three modern versions of Galois theory, in which the Galois group of an extension is replaced by a ring, a Lie ring and a biring respectively. In Chapter 6, I describe the structure of radical extensions and their associated birings in terms of tori.

In Appendix S, I introduce the language of sets and describe the set theory needed for the book. Witt vectors are needed in 3.10, and their properties are developed in Appendix W. Tensor products are used quite often in Chapters 5 and 6, and are discussed in Appendix T.

In order to put the material of Chapters 5 and 6 in the proper formal framework, I have included a fairly thorough treatment of algebras, coalgebras and bialgebras in the appendices. In Appendix A, the structure of finite dimensional commutative algebras is determined. In Appendix C, I discuss coalgebras and develop the structure theory of cocommutative coalgebras.

In Appendix B, I develop a theory of K/k-bialgebras which generalizes the usual theory of k-bialgebras.

To those already familiar with the theory of fields, some further remarks may be of interest. In Chapter 2, the proof that the set k_{sep} of separable elements of a finite dimensional field extension of k is a simple field extension of k is simplified by a theorem on conjugates (see 2.2.10). At the beginning of Chapter 3, a generalization of the Dedekind Independence Theorem is proved (see 3.1.1). This is used to prove a theorem on Galois descent (see 3.2.5) which is then used to prove the Galois Correspondence Theorem (see 3.3.3). In 3.4, the proof of the Normal Basis Theorem is simplified by a theorem on conjugates (see 3.4.1). In Chapter 4, I prove that a p-basis of an arbitrary separable extension K/k is algebraically independent (see 4.3.17), which greatly simplifies the proofs of theorems on separating transcendency bases. In Chapter 5, I give a new treatment of the Jacobson-Bourbaki Correspondence Theorem (see 5.1.7) and an accompanying descent theorem (see 5.1.10), and of the Jacobson Differential Correspondence Theorem (see 5.2.6) and its accompanying descent theorem (see 5.2.9), inspired by work of Pierre Cartier and Gerhard Hochschild. In 5.3, I develop a Galois theory of normal extensions based on the biring $H(K/k)$ of an extension K/k. The structure of K/k is related to the structure of $H(K/k)$ (see 5.3.20), a Biring Correspondence Theorem is proved (see 5.3.12) and a radical splitting theorem for $H(K/k)$ is proved for finite dimensional normal extensions (see 5.3.21). This theory is parallel in some respects to a powerful Galois theory of normal extensions based on the universal cosplit measuring k-bialgebra of an extension K/k, developed by Moss Sweedler [20], but has the advantage that the biring $H(K/k)$ consists of linear transformations of K/k and is therefore more easily studied. In Chapter 6, I discuss in detail the structure of finite dimensional radical extensions K/k and their birings $H(K/k)$, in terms of tori. Tori are then used in proving a fairly deep generalization of a theorem of Jacobson on finite dimensional Lie rings of derivations of K (see 6.4.2). In Appendix B, I develop a formal theory of K/k-bialgebras, which reduces to the usual theory of k-bialgebras when $K = k$. I then define and discuss the K-measuring K/k-bialgebras and their k-forms, and determine the structure of the finite dimensional conormal K-measuring K/k-bialgebras and their cosplit k-forms. The theory thus developed places the material of Chapters 5 and 6 in a formal framework within which the structure of $H(K/k)$ can be more effectively studied.

Other approaches to the theory of radical extensions are outlined in E.5 and E.6 in the form of exercises. An outline of the proof of a theorem of Murray Gerstenhaber on subspaces of Der K closed under pth powers is given (see E.5.8). Higher derivations are introduced, and a sketch of the proof of Moss Sweedler's theorem characterizing in terms of higher derivations those finite dimensional radical extensions which are internal tensor products of simple extensions is given (see E.6.11, E.6.14). Moss Sweedler's universal cosplit measuring k-bialgebra is introduced and discussed in E.6.21 and E.6.22. The Pickert invariants of a radical extension are discussed in E.6.24 and E.6.25.

Reflected in this book are the ideas of many people who ave influenced me directly and through their work in my thinking about ields. I would particularly like to mention George Seligman, with whom I first studied fields, Nathan Jacobson, whose work on fields is the basis fo a large part of this book and Moss Sweedler, whose work on coalgebras, bia ebras and field theory is reflected in the last part of this book. Since a refie ion is not real substitute for an original idea, readers are urged to explore the books and papers listed in the reference section, especially [2], [5], [9], 10], [11], [12], [18], [19], [20].

Much of this book is based on a course on bialgebras and courses on field theory given at the University of Michigan in 1969, 1971 and 1972. Most of the material of Chapters 5 and 6 and of Appendix B is the outgrowth of preliminary research described at the 1971 Conference on Lie Algebras and Related Topics at Ohio State University.

I would like to take this opportunity to express my thanks to my friend and former student, Pedro Sanchez, whose lecture notes to my courses made easier the writing of parts of this book, and to Hershey Kisilevsky, who showed me the irreducible polynomial used in proving 3.12.2. I also wish to thank the National Science Foundation for their support of research described h re, and to express my appreciation to the California Institute of Technology, whose generous support during the academic year 1972–3 enabled the remaining research to be completed at this early date. Finally, I would like to express my thanks to Catherine Rader and Frances Williams, whose superb typing made as painless as possible the job of preparing the manuscript.

Ann Arbor, Michigan and
Pasadena, California, March 1, 1973 David J. Winter

TABLE OF CONTENTS

0 Introduction

In this chapter, we give a brief but fairly self-contained introduction to abstract algebra, in order to develop the language, conventions and basic algebra used throughout the remainder of the book. Our notation for sets of objects and for operations on sets is given in Appendix S.

We begin with basic material on groups, rings and fields. We then briefly discuss transformation groups. Finally, we discuss the Krull Closure in a group in anticipation of its role in Chapter 3.

0.1 Basic algebra

A *product* on a set S is a mapping from $S \times S$ to S, which we may denote $(x, y) \mapsto x \circ y$. A subset T of a set S with product $x \circ y$ is *closed* (or *closed under* $x \circ y$) if $x \circ y \in T$ for all $x, y \in T$. A product $x \circ y$ on S is *associative* if $(x \circ y) \circ z = x \circ (y \circ z)$ for $x, y, z \in S$. An element e of a set S with product $x \circ y$ is an *identity* of S if $e \circ x = x \circ e = x$ for $x \in S$. One shows easily that S has at most one such e (see E.0.1). If such an e exists, S is said to *have an identity*.

A *monoid* (or *semigroup with identity*) is a set S with an associative product $x \circ y$ such that S has an identity. A *submonoid* of a monoid S is a closed subset T of S containing the identity of S. Such a T together with the product $x \circ y$ $(x, y \in T)$ is a monoid. For any element x of a monoid S, we let x^0 be the identity element of S and $x^n = x \circ x \circ \cdots \circ x$ (n times) for any positive integer n. In particular, $x^1 = x$ for $x \in S$. For $x \in S$, the set T consisting of $x^0, x^1, \ldots$ is a submonoid of S and $x^{m+n} = x^m \circ x^n$, $(x^m)^n = x^{mn}$ for all nonnegative integers m, n (see E.0.4). In a monoid S, an *inverse* of an element $x \in S$ is an element $y \in S$ such that $x \circ y = y \circ x = e$, e being the identity element of S. For each $x \in S$, x has at most one inverse y (see E.0.2). If $x \in S$ has an inverse, then we say that x is a *unit* or an *invertible element* of S, and we denote the inverse of x by x^-. The set S^* of units of S is a submonoid of S and $(x \circ y)^- = y^- \circ x^-$, $(x^-)^- = x$ for $x, y \in S^*$ (see E.0.3). For $x \in S^*$, we define $x^{(-n)} = (x^-)^n$ for any positive integer n. In particular, $x^{-1} = x^-$ for $x \in S^*$. We call x^n the nth *power* of x with respect to the product $\circ$. For $x \in S^*$, the set consisting of $x^0, x^{-1}, x^1, x^{-2}, x^2, \ldots$ is a submonoid of S and $x^{m+n} = x^m \circ x^n$, $(x^m)^n = x^{mn}$ for all integers m, n (see E.0.4). Elements x, y of monoid S *commute* if $x \circ y = y \circ x$. A monoid S is *Abelian* (or *commutative*) if $x \circ y = y \circ x$ for $x, y \in S$. If S is an Abelian monoid containing elements $x_1, \ldots, x_m$, we let $\prod_1^m x_i$ denote $x_1 \circ \cdots \circ x_m$ and then have $(\prod_1^m x_i)^n = \prod_1^m (x_i)^n$ for any nonnegative integer n (see E.0.5).

A *group* is a monoid S every element of which is a unit. Thus, a group is a monoid S such that $S = S^*$. For any monoid S, S^* is a group called the *group of units* of S. A *subgroup* of a group S is a submonoid T of S such that

$x^- \in T$ for all $x \in T$. A subgroup T of a group S with product $x \circ y$ $(x, y \in S)$ is a group with product $x \circ y$ $(x, y \in T)$. A group S is *Abelian* if it is Abelian as a monoid. If $x_1, \ldots, x_m$ are elements of an Abelian group S, then $(\prod_1^m x_i)^- = \prod_1^m (x_i)^-$ and $(\prod_1^m x_i)^n = \prod_1^m (x_i)^n$ for any integer n (see E.0.5).

A *ring* is a set A with two products $x + y$ and xy, called *addition* and *multiplication* respectively, such that A with addition is an Abelian group, A with multiplication is a monoid and $x(y + z) = xy + xz$, $(x + y)z = xz + yz$ for $x, y, z \in A$. A *subring* of a ring A is a subset B of A which is a subgroup of A with addition and a submonoid of A with multiplication. A subring B of a ring A together with the addition $x + y$ and multiplication xy $(x, y \in B)$ is a ring. The identities of a ring A with respect to addition and multiplication are denoted 0 and e respectively. The element e is the *identity* of the ring A. For $x \in A$, x^n is the nth power of x with respect to multiplication. We let $-x$ be the additive inverse of x in A, so that $x + (-x) = 0$, and we let $y - x = y + (-x)$ for $x, y \in A$. We then define $0 \cdot x = 0$, $n \cdot x = x + \cdots + x$ (n times) and $(-n) \cdot x = n \cdot (-x)$ for any positive integer n, so that $n \cdot x$ is the nth power of x with respect to addition. In particular, $1 \cdot x = x$ for $x \in A$. One easily proves the basic equations $x0 = 0x = 0$, $(-x)y = -(xy) = x(-y)$ for $x, y \in A$ and the basic equations $(m + n) \cdot x = m \cdot x + n \cdot x$, $m \cdot (n \cdot x) = (mn) \cdot x$, $m \cdot (x + y) = m \cdot x + m \cdot y$ for $x, y \in A$ and any integers m and n (see E.0.4).

A ring A is *commutative* if the monoid A with multiplication is commutative, that is, if $xy = yx$ for $x, y \in A$. An element x of A is a *unit* of the ring A if x is a unit in the monoid A with multiplication. The group of units of A is denoted A^*.

A ring A is an *integral domain* if A is commutative and $A - \{0\}$ is nonempty and closed under multiplication xy. In an integral domain, $e \neq 0$ (see E.0.7). A *field* is an integral domain K such that the group of units K^* is $K - \{0\}$, that is, such that each nonzero element is a unit. Every subring of a field is an integral domain. A *subfield* of a field K is a subring k of K such that $x \in k - \{0\} \Rightarrow x^{-1} \in k - \{0\}$. A subfield of a field K is a field. Every integral domain A is a subring of some field K such that $K = \{xy^{-1} | x \in A, y \in A - \{0\}\}$, and such a field K is a *field of quotients* of A (see E.0.10). Any two fields of quotients of A are essentially the same (see E.0.11).

A *homomorphism/isomorphism* from a monoid or group S with product $x \circ y$ and identity e to a monoid or group S' with product $x' \circ' y'$ and identity e' is a mapping/bijective mapping f from S to S' such that $f(x \circ y) = f(x) \circ' f(y)$ and $f(e) = e'$. If an *isomorphism* from S to S' exists, S and S' are *isomorphic*. An *automorphism* of S is an isomorphism from S to S.

A *homomorphism/isomorphism* from a ring or field A to a ring or field A' is a mapping/bijective mapping f from A to A' such that f is a homomorphism/isomorphism of monoids from A with addition to A' with addition and from A with multiplication to A' with multiplication. If an isomorphism from A to A' exists, A and A' are *isomorphic*. An *automorphism* of A is an isomorphism from A to A.

An *ideal* of a ring A is a nonempty subset I of A closed under addition such

that $xy \in I$ for $x \in A$, $y \in I$ and for $x \in I$, $y \in A$. The sets $\{0\}$ and A are ideals of A. In a commutative ring A, the set $xA = \{xa \mid a \in A\}$ $(x \in A)$ is an ideal of A called the *principle ideal* generated by x. If A is an integral domain and every ideal of A is principal, A is a *principle ideal domain.*

Suppose that S is an Abelian group with product $x + y$ and that T is a subgroup of S. We let $x + T = \{x + y \mid y \in T\}$ for $x \in S$. Then $x \in x + T$ and $x + T$ is the *coset* of T in S containing x. Two cosets $x + T$ and $x' + T$ are equal if and only if $x - x' \in T$. If $x - x' \notin T$, $x + T$ and $x' + T$ are disjoint (see E.0.17). Thus, an element x is contained in precisely one coset, namely $x + T$. We let S/T be the set $\{x + T \mid x \in S\}$ of cosets of T in S. We can define a product $(x + T) + (y + T) = (x + y) + T$ in T, and S/T with this product is an Abelian group (see E.0.17).

Next, let A be a ring and I an ideal of A. We can also define a product $(x + I)(y + I) = xy + I$, and A/I with the so defined additive and multiplicative products is a ring (see E.0.18). The mapping $f(x) = x + I$ $(x \in A)$ is a homomorphism from A to A/I. The ring A/I is the *quotient ring* of A by I, f the *quotient homomorphism.*

If $f: A \to B$ is a homomorphism from a ring A to a ring B, then the set Kernel $f = \{a \in A \mid f(a) = 0\}$ is an ideal of A called the *kernel* of f. The set Image $f = \{f(a) \mid a \in A\}$ is a subring of B called the *image* of f. There is an isomorphism from $A/\text{Kernel } f$ to Image f which sends a $+\text{Kernel } f$ to $f(a)$ for $a \in A$ (see E.0.19). In particular, f is injective if and only if Kernel $f = \{0\}$.

Now suppose that A is a commutative ring and let I be an ideal of A. Then I is *maximal* if $I \neq A$ and the only ideals of A containing I are I and A. One shows easily that A is maximal if and only if A/I is a field (see E.0.23). If A/I is an integral domain, then I is a prime ideal. Equivalently, I is a *prime* ideal if $I \neq A$ and $xy \notin I$ for $x \notin I$, and $y \notin I$. The kernel of any homomorphism f from A into an integral domain is prime.

We now let K and L denote fields and let 1 denote the identity of K. Then K has no ideals other than $\{0\}$ and K, since $K/\{0\}$ is a field.

0.1.1 Proposition. Every homomorphism f from K to L is injective.

Proof. Kernel f is an ideal of K. Since $f(1) \neq 0$, *Kernel* $f \neq K$. Thus, Kernel $f = \{0\}$ and f is injective. □

For $a_0, \ldots, a_n \in K$, we let $\sum_0^n a_i X^i = a_0 X^0 + \ldots + a_n X^n$ denote the infinity-tple $(a_0, \ldots, a_n, 0, \ldots)$ (all entries are 0 after the $(n + 1)$-st). This is called the *polynomial with coefficients* $a_0, \ldots, a_n$. The polynomials $aX^0 (a \in K)$ are the *constant* polynomials, or the polynomials of *degree* 0. The *degree* of a nonconstant polynomial $\sum_0^n a_i X^i$, denoted Deg $\sum_0^n a_i X^i$, is the integer d such that $a_d \neq 0$ and $a_i = 0$ for $i > d$. The *leading coefficient* of $\sum_0^n a_i X^i$ is a_d where $d = \text{Deg} \sum_0^n a_i X^i$. If the leading coefficient of $\sum_0^n a_i X^i$ is 1, we say that $\sum_0^n a_i X^i$ is *monic.* One shows easily that two polynomials $\sum_0^n a_i X^i$ and $\sum_0^n b_i X^i$ are equal if and only if $a_i = b_i$ for $1 \leq i \leq n$. The set of polynomials with coefficients in K is denoted $K[X]$. We let

$$\sum_0^n a_i X^i + \sum_0^n b_i X^i = \sum_0^n (a_i + b_i) X^i$$

and

$$\left(\sum_0^m a_i X^i\right)\left(\sum_0^n b_j X_j\right) = \sum_0^{m+n} c_k X^k$$

where $c_k = \sum_{i+j=k} a_i b_j$, define addition and multiplication in $K[X]$. One easily shows that $K[X]$ with these products is a commutative ring. Note that $\mathrm{Deg}\,(f(X)g(X)) = \mathrm{Deg}\,f(X) + \mathrm{Deg}\,g(X)$ for nonzero $f(X)$, $g(X) \in K[X]$ (see E.0.24). It follows that $K[X]$ is an integral domain. It is convenient to "identify" a with aX^0 for $a \in K$ and 1 with X^0 (see E.0.9). Then K is the subset of constant polynomials and K is a subring of $K[X]$. The group of units of $K[X]$ is $K^* = K - \{0\}$ (see E.0.25).

0.1.2 Proposition. $K[X]$ is a principle ideal domain.

Proof. Let I be a nonzero ideal of $K[X]$. Take $f(X)$ to be a nonzero element of I of least degree, $g(X)$ a nonzero element of I. What we must show is that $g(X)$ is a multiple $f(X)h(X)$ of $f(X)$ (for some $h(X) \in K[X]$). Suppose not, and take the degree of $g(X)$ to be minimal such that $g(X) \in I - \{0\}$ and $g(X)$ is not a multiple of $f(X)$. Choose X^i such that $\mathrm{Deg}\,(f(X)X^i - (a_m/b_n)g(X)) < \mathrm{Deg}\,g(X)$ where a_m, b_n are the leading coefficients of $f(X)$, $g(X)$ respectively. By the minimality assumption, $f(X)X^i - (a_m/b_n)g(X)$ is a multiple of $f(X)$. But then $g(X)$ obviously is also a multiple of $f(X)$, a contradiction. Thus, every $g(X) \in I$ is a multiple of $f(X)$. □

The group of units of $K[X]$ is K^*. Elements $f(X)$, $g(X) \in K[X]$ are *associates* if $f(X) = cg(X)$ for some unit $c \in K^*$. Equivalently, $f(X)$ and $g(X)$ are associates if $f(X)$ divides $g(X)$ and $g(X)$ divides $f(X)$, where we say that $f(X)$ *divides* $g(X)$ if $g(X) = f(X)h(X)$ for some $h(X) \in K[X]$. If $f(X)$ is not a unit and if only units and associates of $f(X)$ divide $f(X)$, then $f(X)$ is *irreducible*.

0.1.3 Proposition. The following conditions are equivalent, for $f(X) \in K[X]$.

1. $f(X)$ is irreducible;
2. the ideal $f(X)K[X]$ is maximal;
3. the ideal $f(X)K[X]$ is prime.

Proof. Let $I = f(X)K[X]$. Suppose that $f(X)$ is irreducible and that J is an ideal of $K[X]$ containing I. Then the generator $g(X)$ of J divides $f(X)$ and is either a unit or an associate of $f(X)$, Thus, $J = A$ or $J = I$ is maximal. Suppose next that I is maximal. Then A/I is a field, so that I is prime. Finally, let I be prime and let $f(X) = g(X)h(X)$. Then $g(X) \in I$ or $h(X) \in I$. Thus, $f(X)$ divides $g(X)$ or $h(X)$. But $g(X)$ and $h(X)$ divide $f(X)$. Thus, $g(X)$ or $h(X)$ is an associate of $f(X)$ and $h(X)$ or $g(X)$ a unit. □

0.1.4 Proposition. Let $f(X)$ be irreducible and suppose that $f(X)$ divides $g(X)h(X)$. Then $f(X)$ divides $g(X)$ or $h(X)$.

Proof. Let $d(X)$ be the generator of the ideal $I = \{f(X)a(X) + g(X)b(X) \mid a(X), b(X) \in K[X]\}$ of $K[X]$. Then $d(X)$ divides each element of

I. Since $f(X), g(X) \in I$, $d(X)$ divides $f(X)$ and $g(X)$. Since $f(X)$ is irreducible, $d(X)$ is a unit c or $d(X)$ is an associate of $f(X)$. In the latter case, $f(X)$ divides $g(X)$ since $d(X)$ does. In the former case $c = f(X)a(X) + g(X)b(X)$ for some $a(X), b(X) \in K[X]$. Then $ch(X) = f(X)a(X)h(X) + g(X)h(X)b(X)$. Since $f(X)$ divides $g(X)h(X)$, $f(X)$ divides $ch(X)$, hence divides $h(X)$. □

0.1.5 Theorem. A nonconstant polynomial $f(X) \in K[X]$ can be factored into $f(X) = \prod_1^m g_i(X)$ where the $g_i(X)$ are monic irreducible elements of $K[X]$. Moreover, the factors $h_j(X)$ of any other such factorization $f(X) = \prod_1^n h_i(X)$ with $h_i(X) \in K[X]$ irreducible can be rearranged to $f(X) = \prod_1^n h_{i'}(X)$ so that $g_1(X) = h_{1'}(X) \ldots, g_m(X) = h_{n'}(X)$ (in particular, $m = n$).

Proof. The existence of the factorization is seen by a simple induction on $\mathrm{Deg}\, f(X)$. The uniqueness follows easily from 0.1.4 (see E.0.39). □

0.1.6 Proposition. Let R be a commutative ring containing x and containing the field k as subring. Then there is precisely one homomorphism $e: k[X] \to R$ such that $e(a) = a$ for $a \in k$ and $e(X) = x$.

Proof. Since each nonzero $f(X) \in k[X]$ has the form $\sum_0^n a_i X^i$ $(a_n \neq 0)$ where n and the a_i are uniquely determined by $f(X)$, we may define e by $e(\sum_0^n a_i X^i) = \sum_0^n a_i x^i$. We leave the remaining details to the reader. □

The homomorphism e described in 0.1.6 is the *evaluation homomorphism* from $k[X]$ to R at x. It is convenient to denote $e(f(X))$ by $f(x)$ for $f(X) \in k[X]$.

Commutative rings isomorphic to $k[X]$ also have the properties described for $k[X]$ in the last few paragraphs. Such rings are used often in this book and are referred to as follows.

0.1.7 Definition. Let R be a commutative ring containing x and containing the field k as subring. Suppose that the evaluation homomorphism $f(X) \mapsto f(x)$ from $k[X]$ to R is an isomorphism. Then we say that x is an *indeterminant* over k and R is a polynomial ring over k in the indeterminant x, and we denote R by $k[x]$.

We now consider a polynomial ring $k[x]$ over k in an indeterminant x and its field of quotients $k(x)$. The elements of $k[x]$ are of the form $f(x) = \sum_0^n a_i x^i$ $(a_i \in k$ for all $i)$ and the elements of $k(x)$ are of the form $u(x)/v(x)$ where $u(x) \in k[x]$ and $v(x) \in k[x] - \{0\}$. Let $k(x)[X]$ be the polynomial ring over the field $k(x)$ in an indeterminant X, and let $k[x][X]$ be the subring of $k(x)[X]$ consisting of the polynomials in X of the form $\sum_0^n a_i(x)X^i$ where the $a_i(x)$ are elements of $k[x]$ for $1 \leq i \leq n$.

0.1.8 Definition. An element $f(X) = \sum_0^n a_i(x)X^i$ of $k[x][X]$ is *primitive* if no irreducible element of $k[x]$ divides $a_i(x)$ for all i.

For any $f(X) \in k(x)[X]$, one can write $f(X) = a(x)f^*(X)$ where $f^*(X)$ is a primitive element of $k[x][X]$ and $a(x) \in k(x)$.

0.1.9 Proposition. Let $a(x)f^*(X) = b(x)g^*(X)$ where $f^*(X), g^*(X)$ are primitive elements of $k[x][X]$ and $a(x), b(x) \in k(x) - \{0\}$. Then $f^*(X) = dg^*(X)$ for some $d \in k$.

Proof. Let $a(x) = s(x)/t(x)$ and $b(x) = u(x)/v(x)$ where $s(x)$, $t(x)$, $u(x)$, $v(x) \in k[x]$. Then $s(x)v(x)f^*(X) = t(x)u(x)g^*(X)$. By 0.1.5, the coefficients in $k[x]$ of the left hand side $s(x)v(x)f^*(X)$ have a common divisor $m(x)$ of greatest degree, which is unique up to a constant multiple. Since $f^*(X)$ is primitive, $s(x)v(x)$ is such a common divisor, so that $s(x)v(x)$ is a constant multiple of $m(x)$. The same argument applies to the right hand side of the equation. Consequently, $s(x)v(x)d = t(x)u(x)$ for some $d \in k$. It follows that $s(x)v(x)f^*(X) = s(x)v(x)dg^*(X)$ and $f^*(X) = dg^*(X)$. □

0.1.10 Proposition. Let $f^*(X)$ and $g^*(X)$ be primitive elements of $k[x][X]$. Then $f^*(X)g^*(X)$ is a primitive element of $k[x][X]$.

Proof. Let $f^*(X) = \sum_0^m a_i(x)X^i$ and $g^*(X) = \sum_0^n b_j(x)X^j$. Let $c(x)$ be an irreducible element of $k[x]$, and let $a_i(x)$ and $b_j(x)$ be the first coefficients of $f^*(X)$ and $g^*(X)$ respectively which are not divisible by $c(x)$. Then the $(i+j)$th coefficient of $f^*(X)g^*(X)$ is $a_i(x)b_j(x) + \sum_{r=1}^{i} a_{i-r}(x)b_{j+r}(x) + \sum_{s=1}^{j} a_{i+s}(x)b_{j-s}(x)$, which is not divisible by $c(x)$ since the latter two sums are divisible by $c(x)$ and $a_i(x)b_j(x)$ is not divisible by $c(x)$ (see 0.1.4). □

0.1.11 Theorem. Let $f(X)$, $g(X)$, $h(X) \in k(x)[X]$ and let $f(X) = a(x)f^*(X)$, $g(X) = b(x)g^*(X)$, $h(X) = c(x)h^*(X)$ where $f^*(X)$, $g^*(X)$, $h^*(X)$ are primitive elements of $k[x][X]$. Then if $f(X)g(X) = h(X)$, we have $f^*(X)g^*(X) = dh^*(X)$, for some $d \in k$.

Proof. Let $f(X)g(X) = h(X)$. Then we have $a(x)b(x)f^*(X)g^*(X) = c(x)h^*(X)$. Since $f^*(X)g^*(X)$ and $h^*(X)$ are primitive, it follows that $f^*(X)g^*(X) = dh^*(X)$ for some $d \in k$, by 0.1.9. □

The observations that we have just made show that $k[x][X]$ has a unique factorization property analogous to the unique factorization property of $k(x)[X]$ described in 0.1.5. More generally, the integral domain $k[X_1, \ldots, X_n] = (\ldots((k[X_1])[X_2])\ldots[X_n])$ (constructed by iterating the construction of $k[x][X]$ and called the *polynomial ring* over k in the n indeterminants $X_1, \ldots, X_n$) has such a unique factorization property. (see E.0.49).

0.2 Groups

We now let G be a group with identity element e. It is often convenient to denote e by 1 and the subgroup $\{e\}$ by **1**. *If* **S** is a collection of subgroups of G, then $\bigcap_{H \in \mathbf{S}} H$ is a subgroup of G. If $S \subset G$ and **S** is the collection of subgroups of G containing S, then $\langle S \rangle = \bigcap_{H \in \mathbf{S}} H$ is the subgroup of G *generated* by S. If $S = \{s_1, \ldots, s_n\}$, we denote $\langle S \rangle$ by $\langle s_1, \ldots, s_n \rangle$. In particular, $\langle g \rangle$ is the subgroup of G generated by g. If $G = \langle g \rangle$, then G is *cyclic* with *generator* g. The *order* of G is the cardinality (number of elements) of G and is denoted $|G|$. The *order* of an element of g of G is the order of $\langle g \rangle$ and is denoted $|g|$. The mapping $\alpha : \mathbb{Z} \to \langle g \rangle$ defined by $\alpha(m) = g^m$ for $m \in \mathbb{Z}$ is a homomorphism from $\mathbb{Z}$ as additive group onto $\langle g \rangle$. (See E.0.4). The kernel of α is an ideal I of $\mathbb{Z}$, so that $I = \{0\}$ or $I = \mathbb{Z}n$ (set of multiples of n) for some positive integer n (see E.0.30). Thus, $\langle g \rangle$ is isomorphic to $\mathbb{Z}$ or to the additive group

$\{\bar{0}, \bar{1}, \ldots, \overline{n-1}\}$ of integers modulo n. (See E.0.38). It follows that if $|g|$ is infinite, then $\langle g\rangle = \{g^m | m = 0, \pm 1, \pm 2, \ldots\}$ and the powers $g^m (m \in \mathbb{Z})$ are distinct. And if $|g|$ is finite, then $\langle g\rangle = \langle g^0, g^1, \ldots, g^{n-1}\rangle$ where $|g| = n$ and where n is the least positive integer such that $g^n = e$. Moreover, $g^m = e$ if and only if n divides m.

Let H be a subgroup of a group G and let $x \in G$. We let xH denote the set $\{xh | h \in H\}$ and call xH the *left coset* of H in G defined by x. The set of left cosets of H in G is denoted G/H. Left cosets xH and yH are equal if and only if $x^{-1}y \in H$. If $x^{-1}y \notin H$, the xH and yH are disjoint (see E.0.68). Thus, each element x of G is contained in precisely one left coset of H in G, namely xH. The *index* of H in G is the cardinality (number of elements) $|G/H|$ of G/H and is denoted $G:H$. The index $G:\mathbf{1}$ of $\mathbf{1}$ in G is the order of G. Since the cardinality of xH is $H:\mathbf{1}$ for all $x \in G$, we have the following theorem.

0.2.1 Theorem. Let G be a group, H a subgroup of G. Then $G:\mathbf{1} = (G:H)(H:\mathbf{1})$. In particular, the order $H:\mathbf{1}$ of any subgroup H and the order $|g|$ of any element g of a finite group G divide the order $G:\mathbf{1}$ of G. □

If $G_1, \ldots, G_n$ are groups, the set $G_1 \times \ldots \times G_n$ together with the product $(g_1, \ldots, g_n)(h_1, \ldots, h_n) = (g_1h_1, \ldots, g_nh_n)$ is a group called the *outer direct product* of $G_1, \ldots, G_n$ and denoted $\prod_1^n G_i$ (outer direct product). If G is a group and if $G_1, \ldots, G_n$ are subgroups of G such that the mapping $f: \prod_1^n G_i$ (outer direct product) $\to G$ defined by $f(g_1, \ldots, g_n) = g_1 \ldots g_n$ is an isomorphism, then we say that G is the *inner direct product* of $G_1, \ldots, G_n$ and write $G = \prod_1^n G_i$ (inner direct product). Note that $|\prod_1^n G_i| = \prod_1^n |G_i|$ for any inner or outer direct product $\prod_1^n G_i$.

Suppose that G is a finite Abelian group. For any prime number p, the set $G_p = \{g \in G \mid g^{p^f} = e \text{ for some } f\}$ is a subgroup of G. The order of G_p is a power of p, as we now show by induction on the order of G_p. If $|G_p| = 1$, the assertion is trivial. Otherwise, let g be an element of $G_p - \{e\}$ and let $H = \langle g\rangle$. Since G is Abelian, we may pass from the group G_p to the group G_p/H. By induction, its order $G_p:H$ is a power of p. Since the order of $H = \langle g\rangle$ is a power of p, the order $G_p:\mathbf{1} = (G_p:H)(H:\mathbf{1})$ is a power of p.

We claim that $G = \prod_1^n G_{p_i}$ (internal direct product) where $|G| = \prod_1^n p_i^{f_i}$. To see this, consider the homomorphism $f: \prod_1^n G_{p_i}$ (outer direct product) $\to G$ defined by $f(g_1, \ldots, g_n) = g_1, \ldots, g_n$. We must show that Kernel $f = \mathbf{1}$ and Image $f = G$. Let p be a prime and let $(g_1, \ldots, g_n)$ be an element of $\prod_1^n G_{p_i}$ (outer direct product) of order p. Then $g_j^p = e$ for all j. Since $g_j \in G_{p_j}$, we have $g_j = e$ for $p \neq p_j$. But then $p = p_i$ and $f(g_1, \ldots, g_n) = g_i$ has order p for some i, so that $(g_1, \ldots, g_n) \notin$ Kernel f. If Kernel $f \neq \mathbf{1}$, then one sees easily that Kernel f would contain an element $(g_1, \ldots, g_n)$ of prime order, which we have just seen to be impossible. Thus, Kernel $f = \mathbf{1}$. Next, let $g \in G$ and note that the order of g is of the form $|g| = \prod_1^n p_i^{e_i}$, by 0.2.1. Since the integers $|g|/p_1^{e_1}, \ldots, |g|/p_n^{e_n}$ have greatest common divisor 1, we can express 1 as a linear combination $1 = m_1(|g|/p_1^{e_1}) + \cdots + m_n(|g|/p_n^{e_n})$ where $m_1, \ldots, m_n \in \mathbb{Z}$ (see E.0.41). Letting $g_i = g^{d_i}$ where $d_i = m_i(|g|/p_i^{e_i})$, we have $g = g^1 = g^{\sum_1^n d_i} = \prod_1^n g_j$ and $g_i^{p_i^{e_i}} = e$ for

$1 \leq i \leq n$. Thus, $g = f(g_1, \ldots, g_n)$ and $g \in \text{Image } f$. We have now shown that $G = \text{Image } f$ and $\mathbf{1} = \text{Kernel } f$, so that $G = \prod_1^n G_{p_i}$ (inner direct product).

The assumption in the preceding paragraph that G be a finite Abelian group can be replaced by the much weaker assumption that G be a finite *nilpotent* group, that is, that the subset $G_p = \{g \in G \mid g^{p^f} = e \text{ for some } f\}$ be a subgroup of G for every prime p. For then each G_p is a subgroup of G whose order is a power of p (see 0.3.2). And one sees easily that for any two distinct prime numbers p and q, the elements of G_p commute with the elements of G_q (see E.0.70), so that f is a homomorphism. The remainder of the discussion goes through as in the Abelian case, and again we have $G = \prod_1^n G_{p_i}$ (inner direct product). We state this for future reference.

0.2.2 Theorem. Let G be a finite nilpotent group. Then $G = \prod_1^n G_{p_i}$ (inner direct product) where $G:\mathbf{1} = \prod_1^n p_i^{e_i}$ is the prime decomposition of the order of G. □

A *basis* for a finite Abelian group G is a set of distinct nonidentity elements $g_1, \ldots, g_m$ of G such that $G = \langle g_1 \rangle \cdots \langle g_m \rangle$ (internal direct product). For distinct nonidentity elements $g_1, \ldots, g_m$ of G to be a basis for G, it is necessary and sufficient that $G = \langle g_1, \ldots, g_m \rangle$ and that $\prod_1^n g_i^{e_i} = e$ if and only if $g_i^{e_i} = e$ for $1 \leq i \leq m$, the e_i being integers for $1 \leq i \leq n$.

Every nontrivial finite Abelian group G has a basis. To prove this, we first note that since $G = \prod_1^n G_{p_i}$ (internal direct product) where $G:\mathbf{1} = \prod_1^n p_i^{e_i}$ is the prime decomposition of $G:\mathbf{1}$, it suffices to consider the case where $G = G_p$ and $G:\mathbf{1} = p^e$, p being a prime number. We now procede by induction on $G:\mathbf{1}$. If $G:\mathbf{1} = p$, then $G = \langle g \rangle$ for any $g \in G - \mathbf{1}$. Suppose that $G:\mathbf{1} = p^e > p$ and let $G^p = \{g^p \mid g \in G\}$. Then $G \supsetneq G^p$, as one easily verifies, and we may assume that $G^p = \mathbf{1}$ or G^p has a basis $g_1, \ldots, g_r$. In the former case, the argument is as for vector spaces—in fact, Abelian groups G such that $G^p = \mathbf{1}$ may be regarded as vector spaces over the field $\{\bar{0}, \bar{1}, \ldots, \overline{p-1}\}$ of p elements (see E.0.38). In the latter case, let $h_1, \ldots, h_r$ be elements of G such that $h_i^p = g_i$ for $1 \leq i \leq r$, and let $H = \langle h_1, \ldots, h_r \rangle$. Then $h_1, \ldots, h_r$ is a basis for H. For suppose that $\prod_1^r h_i^{e_i} = e$. We must show that $h_i^{e_i} = e$ for $1 \leq i \leq r$. Taking pth powers, we have $\prod_1^r g_i^{e_i} = e$, so that $g_i^{e_i} = e$ and $p | e_i$ for $1 \leq i \leq r$. Letting $e_i = pf_i$, we have $e = \prod_1^r h_i^{e_i} = \prod_1^r g_i^{f_i}$. Thus, $e = g_i^{f_i}$ and $e = h_i^{e_i}$ for $1 \leq i \leq r$. Note that there is nothing more to prove if $G = H$, so that we may assume $G \supsetneq H$. Letting $\bar{x}$ denote the coset xH for $x \in G$, we choose, by induction, a basis $\bar{x}_1, \ldots, \bar{x}_s$ for $\bar{G} = G/H$. Since $G^p = H^p$, there exist $u_1, \ldots, u_s \in H$ such that $x_j^p = u_j^p$ for $1 \leq j \leq s$. Letting $y_j = x_j u_j^{-1}$, we have $\bar{y}_j = \bar{x}_j$ and $y_j^p = e$ for $1 \leq j \leq s$. We claim that $h_1, \ldots, h_r, y_1, \ldots, y_s$ is a basis for G. It is clear that $G = \langle h_1, \ldots, h_r, y_1, \ldots, y_s \rangle$. Suppose that $e = \prod_1^r h_i^{e_i} \prod_1^s y_j^{f_j}$. Then $\bar{e} = \prod_1^s \bar{y}_j^{f_j}$, so that $\bar{e} = \bar{y}_j^{f_j}$ and $p | f_j$ for $1 \leq j \leq s$. But then $e = y_j^{f_j}$, since $e = y_j^p$, for $1 \leq j \leq s$. Thus, $e = \prod_1^s h_i^{e_i}$ and $e = h_i^{e_i}$ for $1 \leq i \leq r$. Thus, $h_1, \ldots, h_r, y_1, \ldots, y_s$ is a basis for G. We state this theorem for future reference.

0.2.3 Theorem. Every nontrivial Abelian group G has a basis. □

The *exponent* Exp G of a finite group G is the least integer m such that $g^m = e$ for all $g \in G$.

0.2.4 Theorem. Let G be a finite nilpotent group. Then G has an element of order Exp G.

Proof. We know that $G = \prod_1^n G_{p_i}$ (internal direct product) (see 0.2.2). Since the elements of G_{p_i} all have orders which are powers of p_i (see 0.3.2), G_{p_i} has an element g_i whose order is the exponent of G_{p_i}. Letting $|g_i| = p_i^{e_i}$, the element $g = \prod_1^n g_i$ has order $\prod_1^n p_i^{e_i}$, and one easily sees that $\prod_1^n p_i^{e_i}$ is the exponent of G. □

We now turn to an arbitrary group G. For $x \in G$, we let Int $x(g) = {}^x g = xgx^{-1}$ for $g \in G$. Then Int $x: G \to G$ is an automorphism of G, called the *inner automorphism* of G determined by x. Note that Int $e: G \to G$ is id_G and Int$(xy) =$ Int $x \circ$ Int y. Thus, Int is a homomorphism from G to the group of bijections from G to G (see E.0.82). We let Int $G = \{\text{Int } g \mid g \in G\}$ and $C(G) = \{x \in G \mid \text{Int } x = int\, e\} = \{x \in G \mid xg = gx \text{ for all } g \in G\}$. The subgroup $C(G)$ of G is called the *center* of G.

A subgroup H of a group G is *normal* in G if Int $x(H) = H$ for all $x \in G$. For a subgroup H of G to be normal, it is necessary and sufficient that $xH = Hx$ for all $x \in G$, where $Hx = \{hx \mid h \in H\}$. If H is a normal subgroup of G, then the product $(xH)(yH) = (xy)\,H\,(x, y \in G)$ is well defined and $G/H = \{xH \mid x \in G\}$ together with this product is a group, called the *quotient group* of G by H (see E.0.69). For any normal subgroup H of a group G, the mapping $f: G \to G/H$ defined by $f(x) = xH\,(x \in G)$ is a surjective homomorphism with Kernel H, and is called the *quotient homomorphism* from G to G/H.

If f is a homomorphism from a group G to a group G', then Kernel $f = \{x \in G \mid f(x) = e\}$ is a normal subgroup of G, Image $f = \{f(x) \mid x \in G\}$ is a subgroup of G' and there is an isomorphism from $G/$Kernel f to Image f mapping x Kernel f to $f(x)$ for all $x \in G$. In particular, f is injective if and only if Kernel $f = \mathbf{1}$.

If N and H are subgroups of a group G and if N is normal in G, then $NH = \{xy \mid x \in N, y \in H\}$ is a subgroup of G and N is a normal subgroup of NH. Furthermore, $N \cap H$ is a normal subgroup of H and there is an isomorphism from NH/N to $H/N \cap H$ mapping xN to $x(N \cap H)$ for all $x \in H$ (see E.0.71).

A *tower* in G is a chain $\mathbf{1} \subset G_1 \subset \cdots \subset G_n = G$ of subgroups of G. If G_i is normal in G_{i+1} and G_{i+1}/G_i is cyclic for $1 \leq i \leq n-1$, then this tower is *cyclic*. If G has a cyclic tower, G is *solvable*. If N is a normal subgroup of G, then G is solvable if and only if N and G/N are solvable (see E.0.76).

0.3 Transformation groups

Let G be a group, e the identity element of G. A *G-space* is a set X together with a product $\pi: G \times X \to X$, denoted $(g, x) \mapsto gx$ for $g \in G$, $x \in X$, such that $ex = x$ and $(gh)x = g(hx)$ for $g, h \in G$, $x \in X$. A G-space X determines a homomorphism from G into the group $F(X, X)^*$ of bijective functions from

the set X to itself (see E.0.82). The kernel of this homomorphism is $N = \{g \in G \mid gx = x \text{ for } x \in X\}$, and is called the *kernel* of G on X. If $N = \mathbf{1}$, then X is *faithful*.

A *G-morphism* from a G-space X to a G-space Y is a mapping f from X to Y such that $f(gx) = gf(x)$ for $g \in G$, $x \in X$. A *G-isomorphism* from X to Y is a bijective G-morphism from X to Y. A *G-automorphism* of X is a G-isomorphism from X to X. The set of G-morphisms from X to Y/G-isomorphisms from X to Y/G-automorphisms of X is denoted $\mathrm{Hom}_G(X, Y)/\mathrm{Isom}_G(X, Y)/\mathrm{Aut}_G X$.

A subset Y of a G-space X is *G-stable* (or *stable under G*) if $g(Y) = Y$ for $g \in G$. Such a Y together with $\pi|_{G \times Y}$ is a G-space called a *G-subspace* of X.

For $x \in X$, we let Gx denote $\{gx \mid g \in G\}$ and call Gx the *G-orbit* of x (or the *orbit* of x *under* G, or the *orbit* of G *containing* x). A subset Y of X is G-stable if and only if $Y = \bigcup_{y \in Y} Gy$. We let $X^G = \{x \in X \mid Gx = \{x\}\}$ and call X^G the *set of fixed points of* G in X.

We may regard G together with the group product $G \times G \to G$ as a G-space. More generally, G/H with the product $G \times G/H \to G/H$ given by $g(xH) = gxH$ $(g \in G, x \in G)$ is a G-space for any subgroup H of G.

We let $G_x = \{g \in G \mid gx = x\}$ and call G_x the *isotropy subgroup* of x. Then there is a G-isomorphism from G/G_x (as a G-space) to Gx (as G-space) mapping gG_x to gx for $g \in G$. In particular, $G{:}G_x = |Gx|$ (the cardinality of Gx) for $x \in G$. If $X = Gx$ for some (or every) $x \in X$, we say that G is *transitive* on X (or X is a *transitive* G-space). If $Gx = X$ and $G_x = \mathbf{1}$ for some (or every) $x \in X$, we say that G is *simply transitive* on X (or X is a *simply transitive* G-space). Thus, G is simply transitive on X if and only if the mapping $f_x\colon G \to X$ sending g to gx for $g \in C$ is a G-isomorphism for some (or every) $x \in X$. Also, G is simply transitive on X if and only if for any $x, y \in X$, there exists a unique $g \in G$ such that $gx = y$.

A *G-group* is a group H together with a product $G \times H \to H$ with respect to which H is a G-space such that $g(xy) = (gx)(gy)$ for $g \in G$, $x, y \in H$. For $g \in G$, the mapping $x \mapsto gx$ on a G-group H is an automorphism of H. Thus, products with respect to which a group H is a G-group correspond to homomorphisms from G to the group $\mathrm{Aut}\, H$ of automorphisms of H. We carry over to G-groups the terminology *kernel*, *faithful*, *G-morphism*, *G-isomorphism*, etc. which we introduced for G-spaces. Note that if H is a G-group, the set H^G of fixed points of G in H is a subgroup of H.

A very important instance of a G-group is the group G itself, together with the product $G \times G \to G$ defined by $(g, x) \mapsto {}^g x = g \times g^{-1}$ $(g \in G, x \in G)$. In this case, the orbit of $x \in G$ is ${}^G x = \{gxg^{-1} \mid g \in G\}$, and is called the *conjugacy class* of x in G. The elements of ${}^G x$ are the *conjugates* of x in G. For ${}^G x$ to consist of the single point x, it is necessary and sufficient that x be an element of the center $C(G)$ of G. For a finite group, we therefore have the decomposition $G = C(G) \cup {}^G x_1 \cup \cdots \cup {}^G x_m$ (disjoint union) where ${}^G x_1, \ldots, {}^G x_m$ are those distinct orbits of G having two or more elements. Since $|{}^G x| = G{:}G_x$ for $x \in G$, this yields the *class equation* $G{:}\mathbf{1} = C(G){:}\mathbf{1} + G{:}G_{x_1} + \cdots + G{:}G_{x_m}$ of G. The subgroup G_x occurring in the class equation