Graduate Texts in Mathematics

Nathan Jacobson

Lectures in Abstract Algebra

III. Theory of Fields and Galois Theory

抽象代数讲义

第3卷

Springer-Verlag
世界图书出版公司

Nathan Jacobson

Lectures in Abstract Algebra

III. Theory of Fields and Galois Theory

Springer-Verlag New York Heidelberg Berlin

Nathan Jacobson
Yale University
Department of Mathematics
New Haven, Connecticut 06520

Managing Editor

P. R. Halmos
Indiana University
Department of Mathematics
Swain Hall East
Bloomington, Indiana 47401

Editors

F. W. Gehring
University of Michigan
Department of Mathematics
Ann Arbor, Michigan 48104

C. C. Moore
University of California at Berkeley
Department of Mathematics
Berkeley, California 94720

AMS Subject Classification
12-01

Library of Congress Cataloging in Publication Data

Jacobson, Nathan, 1910–
Lectures in abstract algebra.
(Graduate texts in mathematics; v. 32)
Reprint of the 1951–1964 ed. published by Van Nostrand, New York in The University series in higher mathematics.
Bibliography: v. 3, p.
Includes indexes.
CONTENTS: 2. Linear algebra. 3. Theory of fields and Galois theory. 1. Algebra, Abstract. I. Title. II. Series.
QA162.J3 1975 512'.02 75–15564

Third corrected printing, 1980.

All rights reserved

No part of this book may be translated or reproduced in any form without written permission from Springer-Verlag.

© 1964 by Nathan Jacobson

This reprint has been authorized by Springer-Verlag (Berlin/Heidelberg/New York) for sale in the People's Republic of China only and not for export therefrom.
Reprinted in China by Beijing World Publishing Corporation, 2001

ISBN 0–387–90168–X Springer-Verlag New York Heidelberg Berlin
ISBN 3–540–90168–X Springer-Verlag Berlin Heidelberg New York
ISBN 7-5062-0062-7 World Publishing Corporation China

PREFACE

The present volume completes the series of texts on algebra which the author began more than ten years ago. The account of field theory and Galois theory which we give here is based on the notions and results of general algebra which appear in our first volume and on the more elementary parts of the second volume, dealing with linear algebra. The level of the present work is roughly the same as that of Volume II.

In preparing this book we have had a number of objectives in mind. First and foremost has been that of presenting the basic field theory which is essential for an understanding of modern algebraic number theory, ring theory, and algebraic geometry. The parts of the book concerned with this aspect of the subject are Chapters I, IV, and V dealing respectively with finite dimensional field extensions and Galois theory, general structure theory of fields, and valuation theory. Also the results of Chapter III on abelian extensions, although of a somewhat specialized nature, are of interest in number theory. A second objective of our account has been to indicate the links between the present theory of fields and the classical problems which led to its development. This purpose has been carried out in Chapter II, which gives Galois' theory of solvability of equations by radicals, and in Chapter VI, which gives Artin's application of the theory of real closed fields to the solution of Hilbert's problem on positive definite rational functions. Finally, we have wanted to present the parts of field theory which are of importance to analysis. Particularly noteworthy here is the Tarski-Seidenberg decision method for polynomial equations and inequalities in real closed fields which we treat in Chapter VI.

As in the case of our other two volumes, the exercises form an important part of the text. Also we are willing to admit that quite a few of these are intentionally quite difficult.

Again, it is a pleasure for me to acknowledge my great indebtedness to my friends, Professors Paul Cohn and George Seligman, for their care in reading a preliminary version of this material. Many of their suggestions have been incorporated in the present volume. I am indebted also to Professors Cohn and James Reid and to my wife for help with the proof reading. Finally, I wish to acknowledge my appreciation to the U. S. Air Force Office of Scientific Development whose support during a summer and half of an academic year permitted the completion of this work at an earlier date than would have been possible otherwise.

N. J.

New Haven, Conn.
January 20, 1964

此为试读，需要完整PDF请访问：www.ertongbook.com

CONTENTS

Introduction

In this book we shall assume that the reader is familiar with the general notions of algebra and the results on fields which appear in Vol. I, and with the more elementary parts of Vol. II. In particular, we presuppose a knowledge of the characteristic of a field, prime field, construction of the field of fractions of a commutative integral domain, construction of simple algebraic and transcendental extensions of a field. These ideas appear in Chaps. II and III of Vol. I. We shall need also the elementary factorization theory of Chap. IV. From Vol. II we require the basic notions of vector space over a field, dimensionality, linear transformation, linear function, compositions of linear transformations, bilinear form. On the other hand, the deeper results on canonical forms of linear transformations and bilinear forms will not be needed.

In this Introduction we shall re-do some things we have done before. Our motivation for this is twofold. In the first place, it will be useful for the applications that we shall make to sharpen some of the earlier results. In the second place, it will be convenient to list for easy reference some of the results that will be used frequently in the sequel. The topics that we shall treat here are: extension of homomorphisms (cf. Vol. I, Chap. III), algebras (Vol. II, Chap. VII), and tensor products * of vector spaces and algebras (Vol. II, Chap. VII). The notion of extension of homomorphism is one of the main tools in the theory of fields. The concept of an algebra arises naturally when one studies a field relative to a selected subfield as base field. The concept of tensor product is of lesser importance in field theory and it per-

* In Vol. II this notion was called the Kronecker product. Current usage favors the term tensor product, so we shall adopt this in the present volume. Also we shall use the currently standard notation $\otimes$ for the $\times$ of Vol. II.

haps could be avoided altogether. However, this notion has attained enormous importance throughout algebra and algebraic topology in recent years. For this broader reason it is a good idea for the student to become adept in handling tensor products, and we shall use these freely when it seems appropriate.

1. Extension of homomorphisms. Throughout this book we shall adopt the convention that the rings we consider all have identity elements $1 \neq 0$. The term subring will therefore mean subring in the old sense (as in Vol. I) containing 1, and by a homomorphism of a ring $\mathfrak{A}$ into a ring $\mathfrak{B}$ we shall understand a homomorphism in the old sense sending the 1 of $\mathfrak{A}$ into the 1 of $\mathfrak{B}$.

Now let $\mathfrak{o}$ be a subring of a field P and let Φ be the subfield of P generated by $\mathfrak{o}$. We recall that the elements of Φ can be expressed as simple fractions $\alpha\beta^{-1}$ of elements $\alpha, \beta \in \mathfrak{o}$ $(\beta \neq 0)$. Hence Φ is the subring of P generated by $\mathfrak{o}$ and the inverses of the elements of the set $\mathfrak{o}^*$ of non-zero elements of $\mathfrak{o}$. The set $\mathfrak{o}^*$ contains 1 and is closed under the multiplication of $\mathfrak{o}$. It is sometimes useful to generalize this situation in the following way: We are given a subring $\mathfrak{o}$ of P and a subset M of $\mathfrak{o}^*$ containing 1 and closed under multiplication. We shall refer to such a subset as a sub-semigroup of the multiplicative group of the field. We are interested in the subring $\mathfrak{o}_M$ generated by $\mathfrak{o}$ and the inverses of the elements of M. For example, we could take P to be the field R_0 of rational numbers and $M = \{2^k | k = 0, 1, 2, \cdots\}$. Then $\mathfrak{o}_M$ is the subring of rational numbers whose denominators are powers of 2. In the general case,

$$\mathfrak{o}_M = \{\alpha\beta^{-1} | \alpha \in \mathfrak{o}, \quad \beta \in M\};$$

for, if we denote the set on the right-hand side of this equation by $\mathfrak{o}'$, then clearly $\mathfrak{o}' \subseteq \mathfrak{o}_M$ and $\mathfrak{o}'$ contains $\mathfrak{o} = \{\alpha = \alpha 1^{-1}\}$. Also $\mathfrak{o}'$ contains every $\beta^{-1} = 1\beta^{-1}$ for $\beta \in M$. One checks directly that $\mathfrak{o}'$ is a subring of P. Then it follows that $\mathfrak{o}' = \mathfrak{o}_M$.

Now suppose P′ is a second field and we have a homomorphism s of $\mathfrak{o}$ into P′ such that $\beta^s \neq 0$ for every $\beta \in M$. Our first homomorphism extension theorem concerns this situation. This is the following result.

I. *Let* $\mathfrak{o}$ *be a subring* (*with* 1) *of a field* P, M *a subset of non-zero elements of* $\mathfrak{o}$ *containing* 1 *and closed under multiplication,* $\mathfrak{o}_M$ *the*

subring of P *generated by* $\mathfrak{o}$ *and the inverses of the elements of* M. *Let* s *be a homomorphism of* $\mathfrak{o}$ *into a field* P′ *such that* $\beta^s \neq 0$ *for every* $\beta \in M$. *Then* s *has a unique extension to a homomorphism* S *of* $\mathfrak{o}_M$ *into* P′. *Moreover,* S *is an isomorphism if and only if* s *is an isomorphism.*

Proof. Let $\alpha_1\beta_1^{-1} = \alpha_2\beta_2^{-1}$, $\alpha_i \in \mathfrak{o}$, $\beta_i \in M$. Then $\alpha_1\beta_2 = \alpha_2\beta_1$ and consequently $\alpha_1^s\beta_2^s = \alpha_2^s\beta_1^s$. This relation in P′ gives $\alpha_1^s(\beta_1^s)^{-1} = \alpha_2^s(\beta_2^s)^{-1}$. Hence the mapping

$$S: \alpha\beta^{-1} \to \alpha^s(\beta^s)^{-1}, \quad \alpha \in \mathfrak{o}, \quad \beta \in M$$

which is defined on the whole of $\mathfrak{o}_M = \{\alpha\beta^{-1}\}$ is single-valued. One checks that S is a homomorphism (Vol. I, p. 92). If $\alpha \in \mathfrak{o}$, then $\alpha^S = (\alpha 1^{-1})^S = \alpha^s 1^s = \alpha^s$, so S is the same as s on $\mathfrak{o}$. Hence S is a homomorphism of $\mathfrak{o}_M$ which extends the given homomorphism of $\mathfrak{o}$. Now let S' be any such extension. Then the relation $\beta\beta^{-1} = 1$ for $\beta \in M$ gives $\beta^{S'}(\beta^{-1})^{S'} = 1$, so $(\beta^{-1})^{S'} = (\beta^{S'})^{-1}$. If $\alpha \in \mathfrak{o}$, then we have $(\alpha\beta^{-1})^{S'} = \alpha^{S'}(\beta^{S'})^{-1} = \alpha^s(\beta^s)^{-1} = (\alpha\beta^{-1})^S$. Hence $S' = S$ and S is unique. Clearly, if S is an isomorphism, then its restriction s to $\mathfrak{o}$ is an isomorphism. Now assume s is an isomorphism and let $\alpha\beta^{-1}$ be in the kernel of the homomorphism S: $0 = (\alpha\beta^{-1})^S = \alpha^s(\beta^s)^{-1}$. Then $\alpha^s = 0$, $\alpha = 0$, and $\alpha\beta^{-1} = 0$. This shows that the kernel of S is 0; hence S is an isomorphism.

We consider next an arbitrary commutative ring $\mathfrak{A}$ and the polynomial ring $\mathfrak{A}[x]$, x an element which is transcendental relative to $\mathfrak{A}$ (Vol. I, p. 93). The elements of $\mathfrak{A}[x]$ have the form $a_0 + a_1x + a_2x^2 + \cdots + a_nx^n$ where the $a_i \in \mathfrak{A}$ and $a_0 + a_1x + \cdots + a_nx^n = 0$ only if all the $a_i = 0$. We now have the following homomorphism theorem.

II. *Let* $\mathfrak{A}$ *be a commutative ring,* $\mathfrak{A}[x]$ *the polynomial ring over* $\mathfrak{A}$ *in a transcendental element* x *and let* s *be a homomorphism of* $\mathfrak{A}$ *into a commutative ring* $\mathfrak{B}$. *If* u *is any element of* $\mathfrak{B}$ *there exists a unique homomorphism* S *of* $\mathfrak{A}[x]$ *into* $\mathfrak{B}$ *such that:* $a^S = a^s$, $a \in \mathfrak{A}$, $x^S = u$.

The reader is referred to Vol. I, p. 97, for the proof. This result has an immediate extension to a polynomial ring $\mathfrak{A}[x_1, x_2, \cdots, x_r]$ where the x_i are algebraically independent elements. We recall that the algebraic independence of the x_i means the following:

此为试读，需要完整PDF请访问：www.ertongbook.com

If $(m_1, m_2, \cdots, m_r)$ is an r-tuple of non-negative integers m_i, then a relation $\sum_{mi} a_{m_1 \cdots m_r} x_1^{m_1} \cdots x_r^{m_r} = 0$, $a_{m_1 \cdots m_r} \in \mathfrak{A}$, can hold only if every $a_{m_1 \cdots m_r} = 0$. From now on we shall refer to elements x_i which belong to a commutative ring and are algebraically independent relative to a subring $\mathfrak{A}$ as *indeterminates* (relative to $\mathfrak{A}$). Then we have

III. *Let $\mathfrak{A}[x_1, \cdots, x_r]$ be a commutative polynomial ring in x_i which are indeterminates (relative to $\mathfrak{A}$) and let s be a homomorphism of $\mathfrak{A}$ into a commutative ring $\mathfrak{B}$. If $u_1, u_2, \cdots, u_r$ are arbitrary elements of $\mathfrak{B}$, then there exists a unique homomorphism S of $\mathfrak{A}[x_i]$ into $\mathfrak{B}$ such that* 1) $a^S = a^s$, $a \in \mathfrak{A}$; 2) $x_i^S = u_i$, $i = 1, 2, \cdots, r$.

We now suppose we have a commutative ring $\mathfrak{C}$, $\mathfrak{A}$ a subring, s a homomorphism of $\mathfrak{A}$ into another commutative ring $\mathfrak{B}$. Let $t_1, t_2, \cdots, t_r$ be elements of $\mathfrak{C}$ and let $\mathfrak{A}[t_1, t_2, \cdots, t_r]$ be the subring of $\mathfrak{C}$ generated by $\mathfrak{A}$ and the t_i. Under what conditions can s be extended to a homomorphism S of $\mathfrak{A}[t_i] \equiv \mathfrak{A}[t_1, t_2, \cdots, t_r]$ into $\mathfrak{B}$ so that $t_i^S = u_i$, $1 \leq i \leq r$, where the u_i are prescribed elements of $\mathfrak{B}$? The answer to this basic question is

IV. *Let $\mathfrak{B}$ and $\mathfrak{C}$ be commutative rings, $\mathfrak{A}$ a subring of $\mathfrak{C}$, s a homomorphism of $\mathfrak{A}$ into $\mathfrak{B}$. Let $t_1, \cdots, t_r$ be elements of $\mathfrak{C}$, $u_1, \cdots, u_r$ elements of $\mathfrak{B}$. Then there exists a homomorphism S of $\mathfrak{A}[t_1, \cdots, t_r]$ into $\mathfrak{B}$ such that $a^S = a^s$, $a \in \mathfrak{A}$ and $t_i^S = u_i$, $i = 1, 2, \cdots, r$, if and only if for every polynomial $f(x_1, \cdots, x_r) \in \mathfrak{A}[x_i]$, x_i indeterminates, such that $f(t_1, \cdots, t_r) = 0$ we have $f^s(u_1, \cdots, u_r) = 0$. Here $f^s(x_1, \cdots, x_r)$ is obtained by applying s to the coefficients of $f(x_1, \cdots, x_r)$. If S exists, it is unique.*

Proof. The set $\mathfrak{K}$ of polynomials $f(x_1, \cdots, x_r)$ such that $f(t_1, \cdots, t_r) = 0$ is the kernel of the homomorphism $h(x_1, \cdots, x_r) \rightarrow h(t_1, \cdots, t_r)$ of $\mathfrak{A}[x_i]$ into $\mathfrak{A}[t_i]$. Hence we have the isomorphism $\tau: h(t_1, \cdots, t_r) \rightarrow h(x_1, \cdots, x_r) + \mathfrak{K}$ of $\mathfrak{A}[t_i]$ onto the difference ring $\mathfrak{A}[x_i]/\mathfrak{K}$. Next we consider the homomorphism $h(x_1, \cdots, x_r) \rightarrow h^s(u_1, \cdots, u_r)$ of $\mathfrak{A}[x_i]$ into $\mathfrak{B}$ (cf. III). Assume that $f^s(u_1, \cdots, u_r) = 0$ for every $f \in \mathfrak{K}$. Then every $f \in \mathfrak{K}$ is mapped into 0 by the homomorphism $h(x_1, \cdots, x_r) \rightarrow h^s(u_1, \cdots, u_r)$ so $\mathfrak{K}$ is contained in the kernel of this homomorphism. It follows (Vol. I, p. 70) that we have the homomorphism $h(x_1, \cdots, x_r) +$

$\mathfrak{K} \to h^s(u_1, \cdots, u_r)$ of $\mathfrak{A}[x_i]/\mathfrak{K}$ into $\mathfrak{B}$. Combining this with the isomorphism τ we obtain the homomorphism

$$S: h(t_1, \cdots, t_r) \to h^s(u_1, \cdots, u_r) \tag{1}$$

of $\mathfrak{A}[t_i]$ into $\mathfrak{B}$. This is the required extension of s. If S' is any extension of s to a homomorphism of $\mathfrak{A}[t_i]$ into $\mathfrak{B}$ such that $a^{S'} = a^s$ and $t_i^{S'} = u_i$, then $h(t_1, \cdots, t_r)^{S'} = h^s(u_1, \cdots, u_r)$; hence $S' = S$ and S is unique. Also, it is trivial that, if $f(t_1, \cdots, t_r) = 0$, then $0 = f(t_1, \cdots, t_r)^S = f^s(u_1, \cdots, u_r)$ if S is a homomorphism of $\mathfrak{A}[t_1, \cdots, t_r]$ satisfying our conditions. Hence it is clear that the condition stated in the theorem is necessary for the existence of the extension S.

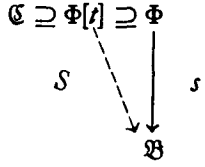
We have noted in the proof that the set $\mathfrak{K}$ of polynomials $f(x_1, \cdots, x_r)$ such that $f(t_1, \cdots, t_r) = 0$ is the kernel of a homomorphism. Hence this is an ideal in the polynomial ring $\mathfrak{A}[x_1, x_2, \cdots, x_r]$. Now let $X = \{g\}$ be a set of generators of $\mathfrak{K}$: $X \subseteq \mathfrak{K}$ and every element $f \in \mathfrak{K}$ has the form $\Sigma a_i(x_1, \cdots, x_r)g_i(x_1, \cdots, x_r)$ where the $a_i(x_1, \cdots, x_r) \in \mathfrak{A}[x_1, x_2, \cdots, x_r]$ and the $g_i(x_1, \cdots, x_r) \in X$. It is clear that, if $g^s(u_1, \cdots, u_r) = 0$ holds for every $g \in X$, then also $f^s(u_1, \cdots, u_r) = 0$ for every $f \in \mathfrak{K}$. Hence we can obtain from IV the following result which is often easier to apply than IV itself:

IV′. *Let $\mathfrak{B}$ and $\mathfrak{C}$ be commutative rings, $\mathfrak{A}$ a subring of $\mathfrak{C}$, and s a homomorphism of $\mathfrak{A}$ into $\mathfrak{B}$. Let X be a set of generators of the ideal $\mathfrak{K}$ of polynomials f in $\mathfrak{A}[x_1, x_2, \cdots, x_r]$, x_i indeterminates, such that $f(t_1, t_2, \cdots, t_r) = 0$. Then there exists a homomorphism S of $\mathfrak{A}[t_1, t_2, \cdots, t_r]$ into $\mathfrak{B}$ such that $a^S = a^s$, $a \in \mathfrak{A}$, and $t_i^S = u_i$, $1 \leq i \leq r$, if and only if $g^s(u_1, \cdots, u_r) = 0$ for every $g \in X$. If S exists, then it is unique.*

We now consider the important special case of IV′ in which $\mathfrak{A} = \Phi$ a field and $r = 1$. Then we know that $\Phi[x]$ is a principal ideal domain (Vol. I, p. 100). Hence the ideal $\mathfrak{K} = (f(x))$, where $(f(x))$ denotes the ideal of polynomial multiples of the polynomial $f(x) \in \mathfrak{K}$. It is clear that $\mathfrak{K} \neq (1) = \Phi[x]$ since, otherwise, $0 = \Phi[x]/\mathfrak{K} \cong \Phi[t] \supseteq \Phi$ which contradicts $1 \neq 0$. Since $(\alpha) = (1)$ if α is a non-zero element of Φ, it is clear that the possibilities for $\mathfrak{K}$ are $\mathfrak{K} = (0)$ or $\mathfrak{K} = (f(x))$ where $f(x)$ is a non-zero poly-

nomial in $\Phi[x]$ of positive degree. In the first case we have $\Phi[x] \cong \Phi[t]$ and t is transcendental. Then II (or IV) is applicable and shows that s can be extended to a homomorphism S sending t into any $u \in \mathfrak{B}$. Now suppose that $f(x) \neq 0$. In this case we call the element $t \in \mathfrak{C}$ *algebraic over* Φ since we have a non-zero polynomial $f(x)$ such that $f(t) = 0$. The ideal $\mathfrak{R}$ is, by definition, the set of polynomials $g(x)$ such that $g(t) = 0$. The polynomial $f(x)$ is a polynomial of least degree in $\mathfrak{R}$ and every other polynomial contained in $\mathfrak{R} = (f(x))$ has the form $g(x)f(x)$. We can normalize $f(x)$ by multiplying it by the inverse of its leading coefficient to obtain a polynomial with leading coefficient 1. If we let $f(x)$ be this polynomial, then clearly f can be characterized by the properties that it is the polynomial of least degree belonging to $\Phi[x]$ with leading coefficient 1 satisfying $f(t) = 0$. We shall call $f(x)$ the *minimum polynomial* (*over* Φ) of the algebraic element $t \in \mathfrak{C}$. We can now state the following result which is a special case of IV'.

V. *Let* $\mathfrak{B}$ *and* $\mathfrak{C}$ *be commutative rings,* Φ *a subfield of* $\mathfrak{C}$, t *an element of* $\mathfrak{C}$ *which is algebraic over* Φ, *and* s *an isomorphism of* Φ *into* $\mathfrak{B}$:



Then s *can be extended to a homomorphism* S *of* $\Phi[t]$ *into* $\mathfrak{B}$ *so that* $t^S = u$, *if and only if* $f^s(u) = 0$ *for the minimum polynomial* $f(x)$ *of* t *over* Φ. *When the extension exists it is unique.*

Remarks. The condition one has to put on u to insure the existence of S can be stated also in the following way: u is algebraic over the image Φ^s of Φ and its minimum polynomial over Φ^s is a factor of $f^s(x)$. The equation (1) giving the form of S now becomes

$$S: g(t) \rightarrow g^s(u). \tag{2}$$

It is immediate from this that S is an isomorphism if and only if $f^s(x)$ is the minimum polynomial of u.

2. Algebras. We recall the definition of an algebra $\mathfrak{A}$ over a field Φ (Vol. II, p. 36 and p. 225): $\mathfrak{A}$ is a vector space over Φ in which a product $xy \in \mathfrak{A}$ is defined for x, y in $\mathfrak{A}$ such that

$$(x_1 + x_2)y = x_1y + x_2y, \quad x(y_1 + y_2) = xy_1 + xy_2$$
$$\alpha(xy) = (\alpha x)y = x(\alpha y), \quad \alpha \in \Phi. \tag{3}$$

We shall be interested only in algebras which have identities 1 and which are associative; hence in this volume "algebra" will always mean just this.

We shall usually encounter algebras in the following way: We are given a ring $\mathfrak{A}$ and a subfield Φ of the center of $\mathfrak{A}$. Then we can consider $\mathfrak{A}$ as a vector space over Φ by taking αx, $\alpha \in \Phi$, $x \in \mathfrak{A}$, to be the ring product of α and x in $\mathfrak{A}$. Clearly this makes $\mathfrak{A}$ a vector space over Φ. Also (3) is clear since α is in the center. Hence we have an algebra $\mathfrak{A}/\Phi$ ($\mathfrak{A}$ over Φ).* This procedure for defining an algebra will be used in studying a field P relative to a subfield Φ. Then we obtain the algebra P/Φ.

Another algebra which is basic is the algebra $\mathfrak{L}_\Phi(\mathfrak{M})$ of linear transformations of a vector space $\mathfrak{M}$ over a field Φ. Here $A + B$, AB and αA for $A, B \in \mathfrak{L}_\Phi(\mathfrak{M})$ and $\alpha \in \Phi$ are defined by $x(A + B) = xA + xB$, $x(AB) = (xA)B$, $x(\alpha A) = \alpha(xA) = (\alpha x)A$. The dimensionality $[\mathfrak{L}_\Phi(\mathfrak{M}):\Phi]$ of $\mathfrak{L}_\Phi(\mathfrak{M})$ over Φ is finite if and only if $[\mathfrak{M}:\Phi]$ is finite. If $[\mathfrak{M}:\Phi] = m$, then $[\mathfrak{L}_\Phi(\mathfrak{M}):\Phi] = m^2$ (Vol. II, p. 41).

Evidently an algebra is a ring relative to the $+$ of the vector space and the multiplication ab. A *subalgebra* $\mathfrak{B}$ of an algebra $\mathfrak{A}$ over Φ is a subspace of $\mathfrak{A}$ which is also a subring. An *ideal* of $\mathfrak{A}/\Phi$ is a subspace which is an ideal of $\mathfrak{A}$ as a ring. A *homomorphism* s of the algebra $\mathfrak{A}/\Phi$ into the algebra $\mathfrak{B}/\Phi$ is a mapping of $\mathfrak{A}$ into $\mathfrak{B}$ which is Φ-linear and a ring homomorphism. Isomorphisms and automorphisms are defined in a similar fashion. If $\mathfrak{K}$ is an ideal in $\mathfrak{A}/\Phi$, then the factor space $\mathfrak{A}/\mathfrak{K}$ is an algebra over Φ relative to its vector space compositions and the multiplication $(a + \mathfrak{K})(b + \mathfrak{K}) = ab + \mathfrak{K}$. We have the algebra homomorphism $a \to a + \mathfrak{K}$ of $\mathfrak{A}/\Phi$ onto $\mathfrak{A}/\mathfrak{K}$ over Φ. If s is a homomorphism of $\mathfrak{A}/\Phi$ into $\mathfrak{B}/\Phi$, then the image $\mathfrak{A}^s$ is a subalgebra of $\mathfrak{B}$ and the

* We shall use the notation $\mathfrak{A}/\mathfrak{B}$ also for the difference ring of $\mathfrak{A}$ relative to the ideal $\mathfrak{B}$. Which of these meanings is intended will always be clear from the context.

kernel $\mathfrak{R}$ of s is an ideal in $\mathfrak{A}$. We have the isomorphism $a + \mathfrak{R} \to a^s$ of $\mathfrak{A}/\mathfrak{R}$ onto $\mathfrak{A}^s$. The basic results on ring homomorphisms extend to algebras and we shall use these without comment.

We shall now record some elementary results on finite dimensional algebras which will be used frequently in the sequel. The first concerns a dimensionality relation for $\mathfrak{A}/\Phi$ and $\mathfrak{A}/E$, where E is a subfield of Φ. Evidently if E is a subfield of Φ, then we can restrict the multiplication αx, $\alpha \in \Phi$, $x \in \mathfrak{A}$ to α in E. This turns $\mathfrak{A}$ into an algebra $\mathfrak{A}$ over E. Also since E is a subfield of Φ we can define the algebra Φ/E. We now have

VI. *Let $\mathfrak{A}$ be an algebra over Φ, E a subfield of Φ. Suppose $[\mathfrak{A}:\Phi] < \infty$ and $[\Phi:E] < \infty$. Then*

$$[\mathfrak{A}:E] = [\mathfrak{A}:\Phi][\Phi:E]. \tag{4}$$

Proof. Let (u_i), $1 \leq i \leq n$, be a basis for $\mathfrak{A}/\Phi$, (γ_j), $1 \leq j \leq m$, a basis for Φ/E. Then (4) will follow if we can show that $(\gamma_j u_i)$ is a basis for $\mathfrak{A}/E$. First let $a \in \mathfrak{A}$. Then $a = \sum_1^n \alpha_i u_i$, $\alpha_i \in \Phi$, and $\alpha_i = \sum_{j=1}^m \epsilon_{ij}\gamma_j$ where $\epsilon_{ij} \in E$. Then $a = \Sigma \epsilon_{ij}\gamma_j u_i$ is a linear combination of the elements $\gamma_j u_i$ with coefficients ϵ_{ij} in E. Now suppose $\Sigma \epsilon_{ij}\gamma_j u_i = 0$ where the $\epsilon_{ij} \in E$. Then we have $\Sigma \alpha_i u_i = 0$ for $\alpha_i = \sum_j \epsilon_{ij}\gamma_j$ in Φ. Since the u_i are Φ-independent, this gives $\alpha_i = 0$, $1 \leq i \leq n$. Then the formulas $\alpha_i = \Sigma \epsilon_{ij}\gamma_j$ and the E-independence of the γ_j give $\epsilon_{ij} = 0$ for all i, j. This proves that the elements $\gamma_j u_i$ are E-independent and so these form a basis for $\mathfrak{A}/E$.

VII. *Let $\mathfrak{A}$ be a finite dimensional algebra over a field Φ. Then $\mathfrak{A}$ is a division ring if and only if $\mathfrak{A}$ is an integral domain.*

Proof. We know that division rings are integral domains (Vol. I, p. 54). Now suppose $\mathfrak{A}$ is an integral domain and let a be any non-zero element of $\mathfrak{A}$. Consider the right multiplication a_R: $x \to xa$ determined by a. This is a linear transformation in $\mathfrak{A}/\Phi$ and, since $ba = 0$ in $\mathfrak{A}$ implies $b = 0$, the null space of a_R is 0. It follows that a_R is surjective (that is, maps $\mathfrak{A}$ onto $\mathfrak{A}$). Hence there exists an element a' such that $a'a = a'a_R = 1$. Thus a

has a left inverse. A similar argument using the left multiplication a_L shows that a has a right inverse. Hence every non-zero element of $\mathfrak{A}$ is a unit and $\mathfrak{A}$ is a division ring.

We consider next algebras $\mathfrak{A} = \Phi[t]$ which have a single generator t (cf. § 1). We have the homomorphism $g(x) \to g(t)$ of $\Phi[x]$, x an indeterminate, onto $\mathfrak{A}$. If $\mathfrak{K}$ is the kernel, then $\mathfrak{A} \cong \Phi[x]/\mathfrak{K}$. Also we have seen in § 1 that $\mathfrak{K} = (f(x))$ where $f(x) = 0$ or is a non-zero polynomial with leading coefficient 1. In the first case, t is transcendental and the homomorphism we indicated is an isomorphism. In the second case, t is algebraic and $f(x)$ is its minimum polynomial. Then we have

VIII. *Let $\mathfrak{A} = \Phi[t]$ be an algebra over Φ generated by a single algebraic element t whose minimum polynomial is $f(x)$. Then*

$$[\mathfrak{A}:\Phi] = \deg f(x), \tag{5}$$

the degree of $f(x)$.

Proof. Let $n = \deg f(x)$. Then we assert that $(1, t, \cdots, t^{n-1})$ is a basis for $\mathfrak{A}/\Phi$. Thus let a be any element of $\mathfrak{A} = \Phi[t]$. This has the form $g(t)$, $g(x)$ in $\Phi[x]$. By the division process in $\Phi[x]$ we can write $g(x) = f(x)q(x) + r(x)$ where $\deg r(x) < \deg f(x)$. Then if we apply the homomorphism of $\Phi[x]/\Phi$ onto $\Phi[t]/\Phi$ sending x into t, we obtain $a = g(t) = 0q(t) + r(t)$. Since $\deg r(x) < n$, this shows that $a = r(t)$ is a Φ-linear combination of $1, t, \cdots, t^{n-1}$. Next we note that $1, t, \cdots, t^{n-1}$ are linearly independent over Φ since otherwise we would have a polynomial $g(x) \neq 0$ of degree $< n$ such that $g(t) = 0$. This contradicts the hypothesis that $f(x)$ is the minimum polynomial. Hence $(1, t, \cdots, t^{n-1})$ is a basis and (5) holds.

We recall that $\Phi[t] \cong \Phi[x]/(f(x))$, $f(x)$ a polynomial of positive degree, is a field if and only if $f(x)$ is irreducible (Vol. I, p. 101). Otherwise, $\Phi[t]$ is not an integral domain. It is useful to have a more complete analysis of the structure of $\Phi[t]$ in terms of the minimum polynomial $f(x)$. We shall indicate the results in the following exercises.

EXERCISES

1. An algebra $\mathfrak{A}$ is a *direct sum* of ideals $\mathfrak{A}_i$ if $\mathfrak{A}$ is a vector space direct sum of the subspaces $\mathfrak{A}_i$. Let $\mathfrak{A} = \Phi[t]$, t algebraic with minimum polynomial $f(x)$.

此为试读，需要完整PDF请访问：www.ertongbook.com