IAIN T. ADAMSON

INTRODUCTION TO Field Theory

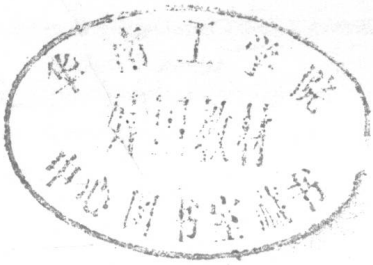
Second edition

INTRODUCTION TO FIELD THEORY

IAIN T. ADAMSON

Senior Lecturer in Mathematics, University of Dundee

SECOND EDITION



CAMBRIDGE UNIVERSITY PRESS

Cambridge

London New York New Rochelle

Melbourne Sydney

Published by the Press Syndicate of the University of Cambridge
The Pitt Building, Trumpington Street, Cambridge CB2 1RP
32 East 57th Street, New York, NY 10022, USA
296 Beaconsfield Parade, Middle Park, Melbourne 3206, Australia

First published by Oliver & Boyd 1964
Second edition published by Cambridge University Press 1982

Printed in Great Britain at the
University Press, Cambridge

Library of Congress catalogue card number: 82–1164

British Library cataloguing in publication data

Adamson, Iain T.
Introduction to field theory. – 2nd ed.

1. Galois theory
I. Title

512′.32 QA211

ISBN 0 521 24388 2 hard covers
ISBN 0 521 28658 1 paperback

INTRODUCTION TO FIELD THEORY

PREFACE

AMID all the current interest in modern algebra, field theory has been rather neglected—most of the recent textbooks in algebra have been concerned with groups or vector spaces. But field theory is a very attractive branch of algebra, with many fascinating applications; and its central result, the Fundamental Theorem of Galois Theory, is by any standards one of the really "big" theorems of mathematics. This book aims to bring the reader from the basic definitions to important results and to introduce him to the spirit and some of the techniques of abstract algebra. It presupposes only a little knowledge of elementary group theory and a willingness on the reader's part to remember definitions precisely and to engage in close argument.

Chapter 1 develops *ab initio* the elementary properties of rings, fields and vector spaces. Chapter 2 describes extensions of fields and various ways of classifying them. In Chapter 3 we give an exposition of the Galois theory of normal separable extensions of finite degree, closely following Artin's approach. Chapter 4 provides a wide variety of applications of the preceding theory, including the classification of all fields with a finite number of elements, ruler-and-compasses constructions and the impossibility of solving by radicals the generic polynomial of degree greater than 4.

I had the great good fortune to persuade my colleague Dr Hamish Anderson to read the first draft of this book, and as a result of his careful scrutiny and penetrating comments many blemishes were removed; I am deeply

grateful to him for his invaluable help. In preparing the book for the press I have had the assistance of Dr Joan Aldous, Mr William Blackburn and Mr Brian Kennedy, and I gratefully acknowledge this here. It is a pleasure also to record my great gratitude to Professor D. E. Rutherford, whose lectures on groups first aroused my interest in algebra, for his constant encouragement and help at all stages in the preparation of the book. Finally I must not forget to thank several generations of honours students in The Queen's University of Belfast and Queen's College, Dundee who patiently listened to and commented on the successive lecture courses which eventually turned into this book; one of them in particular, in a spontaneous exclamation, provided me with an appropriate conclusion to Chapter 4.

IAIN T. ADAMSON

DUNDEE
August 1964

CONTENTS

CHAPTER IV

APPLICATIONS

CHAPTER I

ELEMENTARY DEFINITIONS

§ 1. **Rings and fields.** Modern algebra, of which field theory is a part, may be very roughly described as the study of sets equipped with laws of composition. To amplify this description we make the following definition: a **law of composition** on a set E is an operation which assigns to every ordered pair (a, b) of elements of E a definite element of E which may be denoted by $a+b$, in which case it is called the **sum** of a and b and the operation is called **addition**, or alternatively by $a \times b$ or $a \,.\, b$ or simply ab, in which case it is called the **product** of a and b and the operation is called **multiplication**. Quite clearly ordinary addition and multiplication of real numbers are laws of composition on the set of real numbers **R**.

When we wish to discuss laws of composition in general, we use a " neutral " symbol, such as $a \circ b$, to denote the result of applying the law of composition to the ordered pair (a, b). With this notation we make some further definitions. A law of composition on a set E is said to be **associative** if for every three elements a, b, c of E we have $a \circ (b \circ c) = (a \circ b) \circ c$; it is said to be **commutative** if for every pair of elements a, b of E we have $a \circ b = b \circ a$. If for any two elements c, d of E we have $c \circ d = d \circ c$ then c and d are said to **commute**. An element n of E is called a **neutral element** for the law of composition if $n \circ a = a = a \circ n$ for every element a of E; if the additive notation is used, a neutral element is called a **zero element**

and is usually denoted by 0, and if the multiplicative notation is used, a neutral element is called an **identity element** and is denoted by e or 1. If a is an element of E, an **inverse** of a relative to a law of composition for which there is a neutral element n is an element a' of E such that $a \circ a' = n = a' \circ a$; when the additive or multiplicative notations are used we write $-a$ or a^{-1} respectively instead of a'. Ordinary addition and multiplication of real numbers are both associative and commutative; the real numbers 0 and 1 are neutral elements for addition and multiplication respectively; every real number has an inverse relative to addition and every real number except 0 has an inverse relative to multiplication. Addition and multiplication of real numbers have a further property: for every three real numbers a, b, c we have

$$a(b+c) = ab+ac \text{ and } (b+c)a = ba+ca.$$

We say that the multiplication is **distributive** with respect to the addition.

Readers of this book will require to have some familiarity with the elementary theory of groups, as contained in practically any introductory text in modern algebra. We recall here that a **group** is a set G equipped with an associative law of composition such that

(1) there is a neutral element for the law of composition;

(2) every element has an inverse relative to the law of composition.

It is unnecessary to state explicitly the "closure" property mentioned by some writers on elementary group theory, since it is built into our definition of a law of composition on G that the result of applying the law to a pair of elements of G is again an element of G. If the law of composition of a group is commutative, the group is said to be **abelian**.

A **ring** is a set R equipped with two laws of composition, which we shall call addition and multiplication, such that the following conditions are satisfied:

A1. The addition is associative, i.e., for every three elements a, b, c of R we have $a+(b+c) = (a+b)+c$.

A2. The addition is commutative, i.e., for every pair of elements a, b of R we have $a+b = b+a$.

A3. There is a neutral element for the addition, i.e., an element, which we call zero and denote by 0, such that for every element a of R we have $a+0 = a = 0+a$.

A4. Every element a of R has an inverse relative to the addition, i.e., an element which we denote by $-a$ such that $a+(-a) = 0 = (-a)+a$.

M1. The multiplication is associative, i.e., for every three elements a, b, c of R we have $a(bc) = (ab)c$.

AM. The multiplication is distributive with respect to the addition, i.e., for every three elements a, b, c of R we have $a(b+c) = ab+ac$ and $(b+c)a = ba+ca$.

A ring R is called a **commutative ring** if, in addition to the defining properties of a ring, it satisfies the further condition:

M2. The multiplication is commutative, i.e., for every pair of elements a, b of R we have $ab = ba$.

A ring R is called a **ring with identity** if it satisfies the conditions **A1**, **A2**, **A3**, **A4**, **M1**, **AM** and the further condition:

M3. There is a neutral element for the multiplication, i.e., an element e, which we call the identity of R, such that for every element a of R we have $ea = a = ae$.

Finally, a commutative ring with identity is called a

field if it contains at least two elements and satisfies all the conditions listed so far, together with the following:

M4. Every non-zero element a of R has an inverse relative to the multiplication, i.e., an element a^{-1} such that $aa^{-1} = e = a^{-1}a$.

A field F is said to be **finite** or **infinite** according as the number of elements of F is finite or infinite.

Example 1. The most familiar example of a ring is the set of ordinary integers (positive, negative and zero) equipped with their ordinary operations of addition and multiplication; we shall always denote this ring by $\mathbf{Z}$. It is a commutative ring with identity (the number 1 is clearly the identity), but not a field—indeed the only integers with multiplicative inverses in $\mathbf{Z}$ are 1 itself and -1.

Example 2. The sets of rational numbers, real numbers and complex numbers, with the ordinary definitions of addition and multiplication, are easily seen to satisfy all the conditions for fields. We denote these fields respectively by $\mathbf{Q}$, $\mathbf{R}$ and $\mathbf{C}$.

Example 3. If R is any ring and n is any positive integer, then the set of $n \times n$ matrices with elements in R, equipped with ordinary matrix addition and multiplication, is a ring which we denote by $M_n(R)$. The ring $M_n(R)$ is in general not commutative; it has an identity if R does.

Example 4. Let m be any positive integer greater than 1; if a and b are integers such that $a-b$ is divisible by m we say that a is **congruent** to b **modulo** m, and we write $a \equiv b \bmod. m$. The **residue class** of an integer a modulo m is the set of all integers congruent to a modulo m; it is clear that there are exactly m distinct residue classes, since every integer is congruent modulo m to precisely one of the integers $0, 1, \ldots, m-1$. We denote the set of residue classes modulo m by $\mathbf{Z}_m$ and we proceed to turn it into a

ring by defining appropriate operations of addition and multiplication. Let C_1 and C_2 be any two residue classes; choose any integer a_1 from C_1 and any integer a_2 from C_2; we define C_1+C_2 and C_1C_2 to be the residue classes of a_1+a_2 and a_1a_2 respectively. At first sight it appears that these residue classes may depend upon the choice of a_1 and a_2, but we shall show that this is not in fact so. Namely, if b_1, b_2 are integers in the residue classes C_1, C_2 respectively, then $a_1 \equiv b_1$ and $a_2 \equiv b_2$ mod. m, and so there are integers k_1 and k_2 such that $a_1 = b_1+k_1m$ and $a_2 = b_2+k_2m$. It follows that $a_1+a_2 = b_1+b_2+(k_1+k_2)m$ and $a_1a_2 = b_1b_2+(k_1b_2+k_2b_1+k_1k_2m)m$; so we have $a_1+a_2 \equiv b_1+b_2$ mod. m and $a_1a_2 \equiv b_1b_2$ mod. m. Thus a_1+a_2 and b_1+b_2 belong to the same residue class modulo m and so do a_1a_2 and b_1b_2. Hence C_1+C_2 and C_1C_2 depend only upon C_1 and C_2 and not upon the choices involved in their definition.

It is easy to verify that with these laws of composition $\mathbf{Z}_m$ is a commutative ring with identity; the zero and identity elements O and E are the residue classes containing the integers 0 and 1 respectively, and the additive inverse of the residue class containing a is the residue class containing $-a$.

We say that an integer is **relatively prime** to m if it has no factor in common with m except 1 and -1. It is clear that if one integer in a residue class C modulo m is relatively prime to m then so are all the integers in C; in this case we say that C is a **relatively prime residue class**. Let $\mathbf{R}_m$ be the set of relatively prime residue classes modulo m. We shall now show that a residue class modulo m has a multiplicative inverse in $\mathbf{Z}_m$ if and only if it belongs to $\mathbf{R}_m$.

Suppose first that the residue class C has a multiplicative inverse C' in $\mathbf{Z}_m$; then $CC' = E$, and so, if a and a' are integers in C and C' respectively, we have $aa' \equiv 1$ mod. m.

Thus there is an integer k such that $aa' + km = 1$. It follows that if r is any common factor of a and m then r is a factor of $aa' + km = 1$; hence r is either 1 or -1. So if C has a multiplicative inverse in $\mathbf{Z}_m$, C belongs to $\mathbf{R}_m$. We note incidentally that since C' also has an inverse in $\mathbf{Z}_m$ (C is the inverse of C'), C' also belongs to $\mathbf{R}_m$.

Conversely, suppose that C belongs to $\mathbf{R}_m$; we shall show that C has a multiplicative inverse in $\mathbf{Z}_m$. To this end we choose an integer a from C; then a is relatively prime to m. We now consider the set of positive integers which can be expressed in the form $xa+ym$ where x and y are integers. This set is clearly non-empty and hence contains a least element, $d = x_0a+y_0m$ say. Dividing a by d we obtain integers q, r such that $a = qd+r$, $0 \leqq r < d$; from this it follows that

$$r = a-q(x_0a+y_0m) = (1-qx_0)a+(-qy_0)m.$$

If r were non-zero this would contradict our choice of d as the least positive integer of the form $xa+ym$; hence $r = 0$ and d is a factor of a. An exactly similar argument shows that d is a factor of m. Thus d is a positive common factor of a and m and so $d = 1$. We have now shown that there exist integers x_0 and y_0 such that $x_0a+y_0m = 1$, whence $x_0a \equiv 1 \bmod. m$. Hence if C' is the residue class of x_0 modulo m we have $CC' = E$; that is to say, C' is a multiplicative inverse of C.

Since the product of two integers relatively prime to m is also relatively prime to m it follows that the product of two residue classes in $\mathbf{R}_m$ is also in $\mathbf{R}_m$; thus the multiplication in $\mathbf{Z}_m$ is an associative law of composition on $\mathbf{R}_m$. The identity residue class E belongs to $\mathbf{R}_m$ and the preceding arguments show that every residue class in $\mathbf{R}_m$ has a multiplicative inverse which is also in $\mathbf{R}_m$. It follows that $\mathbf{R}_m$, equipped with the multiplication operation of $\mathbf{Z}_m$, is an abelian group.

Example 5. Let p be a prime number and form the

ring $\mathbf{Z}_p$ according to the procedure described in Example 4; we claim that $\mathbf{Z}_p$ is a field. Since we have already proved that $\mathbf{Z}_p$ is a commutative ring with identity, the only property which remains to be established is **M4**. But this follows at once from our discussion in Example 4 since every non-zero residue class modulo p is relatively prime.

§ 2. **Elementary properties.** We notice that conditions **A1** to **A4** can be summed up by saying that the set of elements of a ring R, equipped only with the addition operation, forms an abelian group. This group is called the **additive group** of the ring and is denoted by R^+.

It is easy to show that the zero element 0 of R and the additive inverse $-a$ of each element a of R are unique. Suppose first that 0 and 0′ are zero elements. Then $0+0' = 0$ (since 0′ is a zero element) and $0+0' = 0'$ (since 0 is a zero element); hence $0 = 0'$. Next suppose $-a$ and a' are additive inverses of a. Then we have $(a'+a)+(-a) = 0+(-a) = -a$ (since a' is an inverse) and $(a'+a)+(-a) = a'+(a+(-a)) = a'+0 = a'$ (since the addition is associative and $-a$ is an inverse); hence $a' = -a$. It now follows at once that for every element a of R we have $-(-a) = a$; for both these elements are additive inverses of $-a$.

The existence of an additive inverse for every element in a ring implies that in a ring subtraction is always possible. For the problem of subtracting an element b from an element a can be reformulated as the problem of finding an element x such that $a = x+b$; and clearly $x = a+(-b)$ satisfies this requirement, since

$$(a+(-b))+b = a+((-b)+b) = a+0 = a.$$

We usually abbreviate $a+(-b)$ to $a-b$. Since the addition operation in a ring is commutative, we have $a-b = (-b)+a$.

Although the zero element of a ring is originally singled out for special attention by virtue of its additive property,

the distributive condition **AM** implies that it also enjoys the multiplicative property which we are accustomed to associate with the real number zero—namely, that if one of the factors in a product is zero then the product is zero. So let a be any element of R; we shall prove that $a0 = 0$. Since 0 is a neutral element for addition, we have $0+0 = 0$ and hence $a(0+0) = a0$. Using **AM** we deduce that $a0+a0 = a0$. Now, by **A4**, $a0$ has an additive inverse $-(a0)$; adding $-(a0)$ to both sides, we obtain

$$-(a0)+(a0+a0) = -(a0)+a0 = 0.$$

Applying the associative condition **A1** on the left side, we have $(-(a0)+a0)+a0 = 0$, whence $0+a0 = 0$, i.e., $a0 = 0$ as we claimed. Similarly we may show that $0a = 0$ for every element a of R. It follows that in a field the zero and identity elements 0 and e are distinct; for if a is a non-zero element we have $a0 = 0$, but $ae = a$.

Rather similar arguments can be used to prove that if a and b are any two elements of a ring R then $a(-b) = -(ab)$, $(-a)b = -(ab)$ and $(-a)(-b) = ab$. For example, to establish the first of these, we notice that $b+(-b) = 0$ and hence $a(b+(-b)) = a0$. Thus, by **AM** and what we have just proved, $ab+a(-b) = 0$; so $a(-b)$ is an additive inverse of ab. But $-(ab)$ is the unique additive inverse of ab; hence $a(-b) = -(ab)$. The other results are obtained by analogous arguments.

We have shown for every ring R that if one of the factors in a product of elements of R is zero then the product is zero. The converse of this result is not true in general; for example, in the ring $M_2(\mathbf{C})$ of 2×2 matrices with complex elements, we have

$$\begin{bmatrix} 1 & i \\ i & -1 \end{bmatrix}\begin{bmatrix} 1 & i \\ i & -1 \end{bmatrix} = \begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix}.$$

The converse *is* true, however, in the case of fields. For,

suppose a and b are elements of a field F such that $ab = 0$; we shall show that either $a = 0$ or $b = 0$—in other words, that if a is non-zero then $b = 0$. If a is non-zero, then it has a multiplicative inverse a^{-1}. Multiplying by a^{-1} we obtain $a^{-1}(ab) = a^{-1}0$, and hence, by **M1**,

$$b = eb = (a^{-1}a)b = a^{-1}(ab) = a^{-1}0 = 0.$$

This discussion shows that the product of two non-zero elements of a field is non-zero. Hence in a field the multiplication operation is a law of composition on the set of non-zero elements. Conditions **M1**, **M2**, **M3** and **M4** now imply that the set of non-zero elements of a field F, equipped only with the multiplication operation, forms an abelian group. We call this group the **multiplicative group** of the field F and denote it by F^*. By arguments similar to those used in the additive group we can easily establish that the identity element e and the multiplicative inverse of each non-zero element of a field F are unique, and that, for every non-zero element a of F, $(a^{-1})^{-1} = a$.

Finally, in a field F, division (except by the zero element) is always possible. To divide an element a by a non-zero element b we must find an element x such that $a = xb$; $x = ab^{-1}$ clearly satisfies this requirement. Since the multiplication operation in a field is commutative, we have $ab^{-1} = b^{-1}a$. We frequently use the " fraction " notation a/b instead of ab^{-1}.

Let F be any field. We now define an operation which assigns to each integer n and each element a of F an element of F which we denote by na. We make the definition inductively by setting

(i) $0a = 0$;

(ii) $(k+1)a = ka+a$ for all integers $k \geqq 0$;

(iii) $(-k)a = -(ka)$ for all integers $k > 0$.