

GALOIS THEORY

Emil Artin

NOTRE DAME MATHEMATICAL LECTURES

Number 2

GALOIS THEORY

Lectures delivered at the University of Notre Dame

by

DR. EMIL ARTIN

Professor of Mathematics, Princeton University

Edited and supplemented with a Section on Applications

by

DR. ARTHUR N. MILGRAM

Associate Professor of Mathematics, University of Minnesota

Second Edition

With Additions and Revisions

UNIVERSITY OF NOTRE DAME PRESS,
NOTRE DAME, LONDON

Copyright 1942, 1944

UNIVERSITY OF NOTRE DAME

Second Printing, February 1964

Third Printing, July 1965

Fourth Printing, August 1966

New composition with corrections

Fifth Printing, March 1970

Sixth Printing, January 1971

Printed in the United States of America by
NAPCO Graphic Arts, Inc., Milwaukee, Wisconsin

Contents

The sections marked with an asterisk have been herein added to the content of the first edition

Contents	5
1 LINEAR ALGEBRA	6
A. Fields	6
B. Vector Spaces	6
C. Homogeneous Linear Equations	7
D. Dependence and Independence of Vectors	8
E. Non-homogeneous Linear Equations	11
F*. Determinants	12
2 FIELD THEORY	18
A. Extension Fields	18
B. Polynomials	18
C. Algebraic Elements	20
D. Splitting Fields	22
E. Unique Decomposition of Polynomials into Irreducible Factors	24
F. Group Characters	24
G*. Applications and Examples to Theorem 13	27
H. Normal Extensions	28
I. Finite Fields	32
J. Roots of Unity	36
K. Noether Equations	36
L. Kummer Fields	38
M. Simple Extensions	40
N. Existence of a Normal Basis	41
O. Theorem on Natural Irrationalities	42
3 APPLICATIONS <i>By A. N. Milgram</i>	43
A. Solvable Groups	43
B. Permutation Groups	43
C. Solution of Equations by Radicals	44
D. The General Equation of Degree n	45

E. Solvable Equations of Prime Degree	46
F. Ruler and Compass Construction	48

1 LINEAR ALGEBRA

A. Fields

A field is a set of elements in which a pair of operations called **multiplication** and **addition** is defined analogous to the operations of multiplication and addition in the real number system (which is itself an example of a field). In each field \mathbb{F} there exist unique elements called 0 and 1 which, under the operations of addition and multiplication, behave with respect to all the other elements of \mathbb{F} exactly as their correspondents in the real number system. In two respects, the analogy is not complete: 1) multiplication is not assumed to be commutative in every field, and 2) a field may have only a finite number of elements.

More exactly, a field is a set of elements which, under the above mentioned operation of addition, forms an **additive abelian group** and for which the elements, exclusive of zero, form a multiplicative group and, finally, in which the two group operations are **connected** by the distributive law. Furthermore, the product of 0 and any element is defined to be 0.

If multiplication in the field is commutative, then the field is called a **commutative field**.

B. Vector Spaces

If V is an additive abelian group with elements A, B, \dots , \mathbb{F} a field with elements a, b, \dots , and if for each $a \in \mathbb{F}$ and $A \in V$ the product aA denotes an element of V , then V is called a (left) vector space over \mathbb{F} if the following assumptions hold:

1. $a(A + B) = aA + aB$
2. $(a + b)A = aA + bA$
3. $a(bA) = (ab)A$
4. $1A = A$

The reader may readily verify that if V is a vector space over \mathbb{F} , then $o \cdot A = 0$ and $a \cdot 0 = 0$ where o is the zero element of \mathbb{F} and 0 that of V . For example, the first relation follows from the equations:

$$aA = (a + o)A = aA + oA$$

Sometimes products between elements of \mathbb{F} and V are written in the form Aa in which case V is called a right vector space over \mathbb{F} to distinguish it from the previous case where multiplication by field elements is from the left. If, in the discussion, left and right vector spaces do not occur simultaneously, we shall simply use the term “**vector space**”.

C. Homogeneous Linear Equations

If in a field \mathbb{F} , a_{ij} , $i = 1, 2, \dots, m$, $j = 1, 2, \dots, n$ are $m \cdot n$ elements, it is frequently necessary to know conditions guaranteeing the existence of elements in \mathbb{F} such that the following equations are satisfied:

$$\begin{aligned} a_{11}x_1 + a_{12}x_2 + \dots + a_{1n}x_n &= 0, \\ &\vdots \\ a_{m1}x_1 + a_{m2}x_2 + \dots + a_{mn}x_n &= 0. \end{aligned} \tag{1}$$

The reader will recall that such equations are called linear homogeneous equations, and a set of elements, x_1, x_2, \dots, x_n , of \mathbb{F} , for which all the above equations are true, is called a solution of the system. If not **all** of the elements x_1, x_2, \dots, x_n are 0 the solution is called non-trivial; otherwise, it is called trivial.

THEOREM 1. *A system of linear homogeneous equations **always** has a **non-trivial** solution if the number of unknowns **exceeds** the number of equations.*

Proof: The proof of this follows the method familiar to most high school students, namely, successive elimination of unknowns. If no equations in $n > 0$ variables are prescribed, then our unknowns are unrestricted and we may set them all = 1.

We shall proceed by complete induction. Let us suppose that each system of k equations in more than k unknowns has a non-trivial solution when $k < m$. In the system of equations (1) we assume that $n > m$, and denote the expression $a_{i1}x_1 + \dots + a_{in}x_n$ by L_i , $i = 1, 2, \dots, m$.

We seek elements x_1, \dots, x_n not all 0 such that $L_1 = L_2 = \dots = L_m = 0$. If $a_{ij} = 0$ for each i and j , then any choice of x_1, \dots, x_n , will serve as a solution. If not all a_{ij} are 0, then we may assume that all $a_{ij} \neq 0$, for the order in which the equations are written or in which the unknowns are numbered has no influence on the existence or non-existence of a simultaneous solution. We can find a non-trivial solution to our given system of equations, if and only if we can find a non-trivial solution to the following system:

$$\begin{aligned} L_1 &= 0 \\ L_2 - a_{21}a_{11}^{-1}L_1 &= 0 \\ &\vdots \\ L_m - a_{m1}a_{11}^{-1}L_1 &= 0 \end{aligned}$$

For, if x_1, \dots, x_n is a solution of these latter equations then, since $L_1 = 0$, the second term in each of the remaining equations is 0 and, hence, $L_1 = L_2 = \dots = L_m = 0$. Conversely, if (1) is satisfied, then the new system is clearly satisfied. The reader will notice that the new system was set up in such a way as to “eliminate” x_1 from the last $m - 1$ equations. Furthermore, if a non-trivial solution of the last $m - 1$ equations, when viewed as equations in x_2, \dots, x_n , exists then taking $x_1 = -a_{11}^{-1}(a_{12}x_2 + a_{13}x_3 + \dots + a_{1n}x_n)$ would give us a solution to the whole system. However, the last $m - 1$ equations have a solution by our inductive assumption, from which the theorem follows. \square

Remark: If the linear homogeneous equations had been written in the form $\sum_i x_i a_{ij} = 0$, $j = 1, 2, \dots, n$, the above theorem would still hold and with the same proof although with the order in which terms are written changed in a few instances.

D. Dependence and Independence of Vectors

In a vector space V over a field \mathbb{F} , the vectors A_1, \dots, A_n are called dependent if there exist elements x_1, \dots, x_n , not all 0, of \mathbb{F} such that $x_1 A_1 + x_2 A_2 + \dots + x_n A_n = 0$. If the vectors A_1, \dots, A_n are not dependent, they are called independent.

The **dimension** of a vector space V over a field \mathbb{F} is the **maximum** number of independent elements in V . Thus, the dimension of V is n if there are n independent elements in V , but no set of more than n independent elements. A system A_1, \dots, A_n of elements in V is called a **generating system** of V if **each** element A of V can be expressed linearly in terms of A_1, \dots, A_m , i.e., $A = \sum_{i=1}^m a_i A_i$ for a suitable choice of $a_i, i = 1, \dots, m$ in \mathbb{F} .

THEOREM 2. *In any generating system the maximum number of independent vectors is equal to the dimension of the vector space.*

Let A_1, \dots, A_n be a generating system of a vector space V of dimension n . Let r be the maximum number of independent elements in the generating system. By a suitable reordering of the generators we may assume A_1, \dots, A_r independent. By the definition of dimension it follows that $r \leq n$. For each j , $\{A_1, \dots, A_r, A_{r+j}\}$ are dependent, and in the relation

$$a_1 A_1 + a_2 A_2 + \dots + a_r A_r + a_{r+j} A_{r+j} = 0$$

expressing this, $a_{r+j} \neq 0$, for the contrary would assert the dependence of A_1, \dots, A_r . Thus,

$$A_{r+j} = -a_{r+j}^{-1} [a_1 A_1 + a_2 A_2 + \dots + a_r A_r].$$

It follows that A_1, \dots, A_r is also a generating system since in the linear relation for any element of V the terms involving $A_{r+j}, j \neq 0$, can all be replaced by linear expressions in A_1, \dots, A_r .

Now, let B_1, \dots, B_t , be any system of vectors in V where $t \geq r$, then there exist a_{ij} such that $B_j = \sum_{i=1}^r a_{ij} A_i, j = 1, 2, \dots, t$, since the A_i s form a generating system. If we can show that B_1, \dots, B_t are dependent, this will give us $r \geq n$, and the theorem will follow from this together with the previous inequality $r \leq n$. Thus, we must exhibit the existence of a non-trivial solution out of \mathbb{F} of the equation

$$x_1 B_1 + x_2 B_2 + \dots + x_r B_r = 0.$$

To this end, it will be sufficient to choose the x_i s so as to satisfy the linear equations $\sum_{j=1}^t x_j a_{ij} = 0, i = 1, 2, \dots, r$, since these expressions will be the coefficients of A_i when in $\sum_{j=1}^t x_j B_j$ the B_j s are replaced by $\sum_{i=1}^r a_{ij} A_i$ and terms are collected. A solution to the equation $\sum_{i=1}^t x_i a_{ij}$ always exists by Theorem 1. \square

Remark: Any n independent vectors A_1, \dots, A_n in an n dimensional vector space form a generating system. For any vector A , the vectors A_1, \dots, A_{n+1} , are dependent and the coefficient of A_{n+1} , in the

dependence relation, cannot be zero. Solving for A in terms of A_1, \dots, A_n exhibits A_1, \dots, A_n as a generating system.

A subset of a vector space is called a **subspace** if it is a subgroup of the vector space and if, in addition, the multiplication of any element in the subset by any element of the field is also in the subset. If A_1, \dots, A_s are elements of a vector space V , then the set of all elements of the form $a_1 A_1 + \dots + a_s A_s$ clearly forms a subspace of V . It is also evident, from the definition of dimension, that the dimension of **any** subspace **never** exceeds the dimension of the whole vector space.

An s -tuple of elements (a_1, \dots, a_s) in a field \mathbb{F} will be called a **row-vector**. The totality of such s -tuples form a vector space if we define

$$\alpha) (a_1, a_2, \dots, a_s) = (b_1, b_2, \dots, b_s) \text{ if and only if } a_i = b_i, i = 1, \dots, s;$$

$$\beta) (a_1, a_2, \dots, a_s) + (b_1, b_2, \dots, b_s) = (a_1 + b_1, a_2 + b_2, \dots, a_s + b_s);$$

$$\gamma) b(a_1, a_2, \dots, a_s) = (ba_1, ba_2, \dots, ba_s), \text{ for } b \text{ an element of } \mathbb{F}.$$

When the s -tuples are written vertically, $\begin{pmatrix} a_1 \\ a_2 \\ \vdots \\ a_s \end{pmatrix}$ they will be called column vectors.

THEOREM 3. *The row (column) vector space \mathbf{F}^n of all n -tuples from a field \mathbb{F} is a vector space of dimension n over \mathbb{F} .*

The n elements

$$\epsilon_1 = (1, 0, 0, \dots, 0)$$

$$\epsilon_2 = (0, 1, 0, \dots, 0)$$

$$\vdots$$

$$\epsilon_n = (0, 0, \dots, 0, 1)$$

are independent and generate \mathbf{F}^n . Both remarks follow from the relation $(a_1, a_2, \dots, a_n) = \sum a_i \epsilon_i$.

We call a rectangular array

$$\begin{pmatrix} a_{11} & a_{12} & \dots & a_{1n} \\ a_{21} & a_{22} & \dots & a_{2n} \\ \vdots & \vdots & & \vdots \\ a_{m1} & a_{m2} & \dots & a_{mn} \end{pmatrix}$$

of elements of a field \mathbb{F} a matrix. By the **right row rank** of a matrix, we mean the maximum number of independent row vectors among the rows (a_{i1}, \dots, a_{in}) of the matrix when multiplication by field elements is from the right. Similarly, we define **left row rank**, **right column rank** and **left column rank**.

THEOREM 4. *In **any** matrix the right column rank equals the left row rank and the left column rank equals the right row rank. If the field is commutative, these four numbers are equal to each other and are called the rank of the matrix.*

Call the column vectors of the matrix $\mathbf{C}_1, \dots, \mathbf{C}_n$ and the row vectors $\mathbf{R}_1, \dots, \mathbf{R}_m$. The column vector $\mathbf{0}$ is $\begin{pmatrix} 0 \\ 0 \\ \vdots \\ 0 \end{pmatrix}$ and any dependence $\mathbf{C}_1x_1 + \mathbf{C}_2x_2 + \dots + \mathbf{C}_nx_n = \mathbf{0}$ is equivalent to a solution of the equations

$$\begin{aligned} a_{11}x_1 + a_{12}x_2 + \dots + a_{1n}x_n &= 0 \\ &\vdots \\ a_{m1}x_1 + a_{m2}x_2 + \dots + a_{mn}x_n &= 0. \end{aligned} \tag{2}$$

Any change in the order in which the rows of the matrix are written gives rise to the same system of equations and, hence, does not change the column rank of the matrix, but also does not change the row rank since the changed matrix would have the same set of row vectors. Call c the right column rank and r the left row rank of the matrix. By the above remarks we may assume that the first r rows are independent row vectors. The row vector space generated by all the rows of the matrix has, by Theorem 1, the dimension r and is even generated by the first r rows. Thus, each row after the r^{th} is linearly expressible in terms of the first r rows. Consequently, any solution of the first r equations in (2) will be a solution of the entire system since any of the last $n - r$ equations is obtainable as a linear combination of the first r . Conversely, any solution of (2) will also be a solution of the first r equations. This means that the matrix

$$\begin{pmatrix} a_{11} & a_{12} & \dots & a_{1n} \\ a_{21} & a_{22} & \dots & a_{2n} \\ \vdots & \vdots & & \vdots \\ a_{r1} & a_{r2} & \dots & a_{rn} \end{pmatrix}$$

consisting of the first r rows of the original matrix has the same right column rank as the original. It has also the same left row rank since the r rows were chosen independent. But the column rank of the amputated matrix cannot exceed r by Theorem 3. Hence, $c \leq r$. Similarly, calling c' the left column rank and r' the right row rank, $c' \leq r'$. If we form the transpose of the original matrix, that is, replace rows by columns and columns by rows, then the left row rank of the transposed matrix equals the left column rank of the original. If then to the transposed matrix we apply the above considerations we arrive at $r \leq c$ and $r' \leq c'$.

E. Non-homogeneous Linear Equations

The system of non-homogeneous linear equations

$$\begin{aligned} a_{11}x_1 + a_{12}x_2 + \cdots + a_{1n}x_n &= b_1 \\ &\vdots \\ a_{m1}x_1 + a_{m2}x_2 + \cdots + a_{mn}x_n &= b_m. \end{aligned} \tag{3}$$

has a solution if and only if the column vector $\begin{pmatrix} b_1 \\ b_2 \\ \vdots \\ b_n \end{pmatrix}$ lies in the space generated by the vectors

$$\begin{pmatrix} a_{11} \\ a_{21} \\ \vdots \\ a_{m1} \end{pmatrix}, \dots, \begin{pmatrix} a_{1n} \\ a_{2n} \\ \vdots \\ a_{mn} \end{pmatrix}$$

This means that there is a solution if and only if the right column rank of the matrix

$$\begin{pmatrix} a_{11} & a_{12} & \cdots & a_{1n} \\ a_{21} & a_{22} & \cdots & a_{2n} \\ \vdots & \vdots & & \vdots \\ a_{m1} & a_{m2} & \cdots & a_{mn} \end{pmatrix}$$

is the same as the right column rank of the augmented matrix

$$\begin{pmatrix} a_{11} & a_{12} & \cdots & a_{1n} & b_1 \\ a_{21} & a_{22} & \cdots & a_{2n} & b_2 \\ \vdots & \vdots & & \vdots & \\ a_{m1} & a_{m2} & \cdots & a_{mn} & b_n \end{pmatrix}$$

since the vector space generated by the original must be the **same** as the vector space generated by the augmented matrix and in either case the dimension is the same as the rank of the matrix by Theorem 2.

By Theorem 4, this means that the row ranks are equal. Conversely, if the row rank of the augmented matrix is the same as the row rank of the original matrix, the column ranks will be the same and the equations will have a solution.

If the equations (3) have a solution, then any relation among the rows of the original matrix subsists among the rows of the augmented matrix. For equations (3) this merely means that like combinations of equals are equal. Conversely, if each relation which subsists between the rows of the original matrix also subsists between the rows of the augmented matrix, then the row rank of the augmented matrix is the same as the row rank of the original matrix. In terms of the equations this means that there will exist a solution if and only if the equations are consistent, i.e., if and only if any dependence between the left hand sides of the equations also holds between the right sides.

THEOREM 5. *If in equations (3) $m = n$, there exists a **unique** solution if and only if the corresponding homogeneous equations*

$$\begin{aligned} a_{11}x_1 + a_{12}x_2 + \cdots + a_{1n}x_n &= 0 \\ &\vdots \\ a_{n1}x_1 + a_{n2}x_2 + \cdots + a_{nn}x_n &= 0 \end{aligned}$$

*have only the **trivial** solution.*

Proof If they have only the trivial solution, then the column vectors are independent. It follows that the original n equations in n unknowns will have a unique solution if they have any solution, since the difference, term by term, of two distinct solutions would be a *non-trivial* solution of the homogeneous equations. A solution would exist since the n independent column vectors form a generating system for the n -dimensional space of column vectors.

Conversely, let us suppose our equations have one and only one solution. In this case, the homogeneous equations added term by term to a solution of the original equations would yield a new solution to the original equations. Hence, the homogeneous equations have only the trivial solution. \square

F*. Determinants¹

The theory of determinants that we shall develop in this chapter is not needed in Galois theory. The reader may, therefore, omit this section if he so desires.

We assume our field to be **commutative** and consider the square matrix

$$\begin{pmatrix} a_{11} & a_{12} & \cdots & a_{1n} \\ a_{21} & a_{22} & \cdots & a_{2n} \\ \vdots & \vdots & & \vdots \\ a_{n1} & a_{n2} & \cdots & a_{nn} \end{pmatrix} \quad (4)$$

of n rows and n columns. We shall define a certain function of this matrix whose value is an element of our field. The function will be called the **determinant** and will be denoted by

$$\begin{vmatrix} a_{11} & a_{12} & \cdots & a_{1n} \\ a_{21} & a_{22} & \cdots & a_{2n} \\ \vdots & \vdots & & \vdots \\ a_{n1} & a_{n2} & \cdots & a_{nn} \end{vmatrix}$$

or by $D(A_1, A_2, \dots, A_n)$ if we wish to consider it as a function of the column vectors $\mathbf{A}_1, \mathbf{A}_2, \dots, \mathbf{A}_n$ of (4). If we keep all the columns but \mathbf{A}_1 constant and consider the determinant as a function of \mathbf{A}_1 , then we write $D_k(\mathbf{A}_k)$ and sometimes even only D .

¹Of the preceding theory only Theorem 1, for homogeneous equations and the notion of linear dependence are assumed known.

Definition. A function of the column vectors is a determinant if it satisfies the following three axioms:

1. Viewed as a function of any column A_k it is linear and homogeneous, i.e.,

$$D_k(\mathbf{A}_k + \mathbf{A}'_k) = D_k(\mathbf{A}_k) + D_k(\mathbf{A}'_k) \quad (5)$$

$$D_k(c \cdot \mathbf{A}_k) = c \cdot D_k(\mathbf{A}_k) \quad (6)$$

2. Its value is $= 0$ ² if the adjacent columns \mathbf{A}_k , and \mathbf{A}_{k+1} are equal.
3. Its value is $= 1$ if all \mathbf{A}_k , are the unit vectors \mathbf{U}_k , where

$$\mathbf{U}_1 = \begin{pmatrix} 1 \\ 0 \\ \vdots \\ 0 \end{pmatrix}, \mathbf{U}_2 = \begin{pmatrix} 0 \\ 1 \\ \vdots \\ 0 \end{pmatrix}, \dots, \mathbf{U}_n = \begin{pmatrix} 0 \\ \vdots \\ 0 \\ 1 \end{pmatrix}. \quad (7)$$

The question as to whether determinants exist will be left open for the present. But we derive consequences from the axioms:

- a) If we put $c = 0$ in (5) we get: a determinant is 0 if one of the columns is 0.

- b) $D_k(\mathbf{A}_k) = D_k(\mathbf{A}_k + c \cdot \mathbf{A}_{k+1})$ or a determinant remains unchanged if we add a multiple of one column to an adjacent column. Indeed

$$D_k(\mathbf{A}_k + c \cdot \mathbf{A}_{k+1}) = D_k(\mathbf{A}_k) + c \cdot D_k(\mathbf{A}_k) = D_k(\mathbf{A}_k),$$

because of axiom 2.

- c) Consider the two columns \mathbf{A}_k and \mathbf{A}_{k+1} . We may replace them by \mathbf{A}_k , and $\mathbf{A}_{k+1} + \mathbf{A}_k$; subtracting the second from the first we may replace them by $-\mathbf{A}_{k+1}$ and $\mathbf{A}_{k+1} + \mathbf{A}_k$; adding the first to the second we now have $-\mathbf{A}_{k+1}$ and \mathbf{A}_k . Finally, we factor out -1 . We conclude: a determinant changes sign if we interchange two adjacent columns.

- d) A determinant vanishes if any two of its columns are equal.

Indeed, we may bring the two columns side by side after an interchange of adjacent columns and then use axiom 2. In the same way as in b) and c) we may now prove the more general rules:

- e) Adding a multiple of one column to another does not change the value of the determinant.

- f) Interchanging any two columns changes the sign of D .

- g)) Let $(\nu_1, \nu_2, \dots, \nu_n)$ be a permutation of the subscripts $(1, 2, \dots, n)$. If we rearrange the columns in $D(\mathbf{A}_{\nu_1}, \mathbf{A}_{\nu_2}, \dots, \mathbf{A}_{\nu_n})$ until they are back in the natural order, we see that

$$D(\mathbf{A}_{\nu_1}, \mathbf{A}_{\nu_2}, \dots, \mathbf{A}_{\nu_n}) = \pm D(\mathbf{A}_1, \mathbf{A}_2, \dots, \mathbf{A}_n).$$

Here \pm is a definite sign that does not depend on the special values of the \mathbf{A}_k . If we substitute \mathbf{U}_k for \mathbf{A}_k , we see that $D(\mathbf{U}_{\nu_1}, \mathbf{U}_{\nu_2}, \dots, \mathbf{U}_{\nu_n}) = \pm 1$ and that the sign depends only on the permutation of the unit vectors.

²Henceforth, 0 will denote the zero element of a field.

Now we replace each vector \mathbf{A}_k , by the following linear combination \mathbf{A}'_k of $\mathbf{A}_1, \mathbf{A}_2, \dots, \mathbf{A}_n$:

$$\mathbf{A}'_k = b_{1k}\mathbf{A}_1 + b_{2k}\mathbf{A}_2 + \dots + b_{nk}\mathbf{A}_n. \quad (8)$$

In computing $D(\mathbf{A}'_1, \mathbf{A}'_2, \dots, \mathbf{A}'_n)$ we first apply axiom 1 on \mathbf{A}'_1 , breaking up the determinant into a sum; then in each term we do the same with \mathbf{A}'_2 and so on. We get

$$\begin{aligned} D(\mathbf{A}'_1, \mathbf{A}'_2, \dots, \mathbf{A}'_n) &= \sum_{\nu_1, \nu_2, \dots, \nu_n} D(b_{\nu_1 1} \mathbf{A}_{\nu_1}, b_{\nu_2 2} \mathbf{A}_{\nu_2}, \dots, b_{\nu_n n} \mathbf{A}_{\nu_n}) \\ &= \sum_{\nu_1, \nu_2, \dots, \nu_n} b_{\nu_1 1} \cdot b_{\nu_2 2} \cdots b_{\nu_n n} D(\mathbf{A}_{\nu_1}, \mathbf{A}_{\nu_2}, \dots, \mathbf{A}_{\nu_n}), \end{aligned} \quad (9)$$

where each ν_i runs independently from 1 to n . Should two of the indices ν_i be equal, then $D(\mathbf{A}_{\nu_1}, \mathbf{A}_{\nu_2}, \dots, \mathbf{A}_{\nu_n}) = 0$; we need therefore keep only those terms in which $(\nu_1, \nu_2, \dots, \nu_n)$ is a permutation of $(1, 2, \dots, n)$. This gives

$$D(\mathbf{A}'_1, \mathbf{A}'_2, \dots, \mathbf{A}'_n) = D(\mathbf{A}_1, \mathbf{A}_2, \dots, \mathbf{A}_n) \sum_{(\nu_1, \nu_2, \dots, \nu_n)} \pm b_{\nu_1 1} \cdot b_{\nu_2 2} \cdots b_{\nu_n n}, \quad (10)$$

where $(\nu_1, \nu_2, \dots, \nu_n)$ runs through all the permutations of $(1, 2, \dots, n)$ and where \pm stands for the sign associated with that permutation. It is important to remark that we would have arrived at the same formula (10) if our function D satisfied only the first two of our axioms.

Many conclusions may be derived from (10).

We first assume axiom 3 and specialize the \mathbf{A}_k , to the unit vectors \mathbf{U}_k of (7). This makes $\mathbf{A}'_k = \mathbf{B}_k$, where \mathbf{B} , is the column vector of the matrix of the b_{ik} . (10) yields now:

$$D(\mathbf{B}_1, \mathbf{B}_2, \dots, \mathbf{B}_n) = \sum_{(\nu_1, \nu_2, \dots, \nu_n)} \pm b_{\nu_1 1} \cdot b_{\nu_2 2} \cdots b_{\nu_n n} \quad (11)$$

giving us an explicit formula for determinants and showing that they are uniquely determined by our axioms provided they exist at all.

With expression (11) we return to formula (10) and get

$$D(\mathbf{A}'_1, \mathbf{A}'_2, \dots, \mathbf{A}'_n) = D(\mathbf{A}_1, \mathbf{A}_2, \dots, \mathbf{A}_n) \cdot D(\mathbf{B}_1, \mathbf{B}_2, \dots, \mathbf{B}_n). \quad (12)$$

This is the so-called **multiplication theorem for determinants**. At the left of (12) we have the determinant of an n -rowed matrix whose elements c_{ik} are given by

$$c_{ik} = \sum_{\nu=1}^n a_{i\nu} b_{\nu k}. \quad (13)$$

c_{ik} is obtained by multiplying the elements of the i -th row of $D(\mathbf{A}_1, \mathbf{A}_2, \dots, \mathbf{A}_n)$ by those of the k -th column of $D(\mathbf{B}_1, \mathbf{B}_2, \dots, \mathbf{B}_n)$ and adding.

Let us now replace D in (10) by a function $F(\mathbf{A}_1, \mathbf{A}_2, \dots, \mathbf{A}_n)$ that satisfies only the first two axioms. Comparing with (11) we find

$$F(\mathbf{A}'_1, \mathbf{A}'_2, \dots, \mathbf{A}'_n) = F(\mathbf{A}_1, \mathbf{A}_2, \dots, \mathbf{A}_n) D(\mathbf{B}_1, \mathbf{B}_2, \dots, \mathbf{B}_n).$$

Specializing \mathbf{A}_k , to the unit vectors \mathbf{U}_k , leads to

$$F(\mathbf{B}_1, \mathbf{B}_2, \dots, \mathbf{B}_n) = c \cdot D(\mathbf{B}_1, \mathbf{B}_2, \dots, \mathbf{B}_n) \quad (14)$$

with $c = F(\mathbf{U}_1, \mathbf{U}_2, \dots, \mathbf{U}_n)$.

Next we specialize (12) in the following way: If i is a certain subscript from 1 to $n-l$ we put $\mathbf{A}_k = \mathbf{U}_k$, for $k \neq i, i+1$ $\mathbf{A}_i = \mathbf{U}_i + \mathbf{U}_{i+1}$, $\mathbf{A}_{i+1} = 0$. Then $D(\mathbf{A}_1, \mathbf{A}_2, \dots, \mathbf{A}_n) = 0$ since one column is 0. Thus, $D(\mathbf{A}'_1, \mathbf{A}'_2, \dots, \mathbf{A}'_n) = 0$; but this determinant differs from that of the elements b_{ij} , only in the respect that the $i+l$ -st row has been made equal to the i -th. We therefore see:

A determinant vanishes if two adjacent rows are equal.

Each term in (11) is a product where precisely one factor comes from a given row, say, the i -th. This shows that the determinant is linear and homogeneous if considered as function of this row. If, finally, we select for each row the corresponding unit vector, the determinant is = 1 since the matrix is the same as that in which the columns are unit vectors. This shows that a determinant satisfies our three axioms if we consider it as function of the row vectors. In view of the uniqueness it follows:

A determinant remains unchanged if we transpose the row vectors into column vectors, that is, if we rotate the matrix about its main diagonal.

A determinant vanishes if any two rows are equal. It changes sign if we interchange any two rows. It remains unchanged if we add a multiple of one row to another.

We shall now prove the existence of determinants. For a 1-rowed matrix a_1 the element a_1 itself is the determinant. Let us assume the existence of $(n-1)$ -rowed determinants. If we consider the n -rowed matrix (2) we may associate with it certain $(n-1)$ -rowed determinants in the following way: Let a_{ij} , be a particular element in (2). We cancel the i -th row and k -th column in (2) and take the determinant of the remaining $(n-1)$ -rowed matrix. This determinant multiplied by $(-1)^{i+k}$ will be called the cofactor of a_{ik} and be denoted by A_{ik} .

The distribution of the sign $(-1)^{i+k}$ follows the chessboard pattern, namely,

$$\begin{pmatrix} + & - & + & - & \dots \\ - & + & - & + & \dots \\ \vdots & \vdots & \vdots & & \vdots \\ + & - & + & - & \dots \end{pmatrix}$$

Let i be any number from 1 to n . We consider the following function D of the matrix (2):

$$D = a_{i1}\mathbf{A}_{i1} + a_{i2}\mathbf{A}_{i2} + \dots + a_{in}\mathbf{A}_{in}. \quad (15)$$

It is the sum of the products of the elements of the i -th row and their cofactors. Consider this D in its dependence on a given column, say, \mathbf{A}_k .

For $\nu \neq k$, $\mathbf{A}_{i\nu}$, depends linearly on \mathbf{A}_k , and a_{ik} , does not depend on it; for $\nu = k$, \mathbf{A}_{ik} , does not depend on \mathbf{A}_k , but a_{ik} is one element of this column. Thus, axiom 1 is satisfied. Assume next that two adjacent columns \mathbf{A}_k , and \mathbf{A}_{k+1} are equal. For $\nu \neq k, k+1$, we have then two equal columns in $\mathbf{A}_{i\nu}$ so that

$\mathbf{A}_{i\nu} = 0$. The determinants used in the computation of \mathbf{A}_{ik} and $\mathbf{A}_{i(k+1)}$ are the same but the signs are opposite hence, $\mathbf{A}_{ik} = \mathbf{A}_{i,k+1}$ whereas $a_{ik} = a_{i,k+1}$. Thus $D = 0$ and axiom 2 holds. For the special case $\mathbf{A}_\nu = \mathbf{U}_\nu, (\nu = 1, 2, \dots, n)$ we have $a_{i\nu} = 0$ for $\nu \neq i$ while $a_{ii} = 1, \mathbf{A}_{ii} = 1$. Hence, $D = 1$ and this is axiom 3. This proves both the existence of an n -rowed determinant as well as the truth of formula (15), the so-called development of a determinant according to its i -th row. (15) may be generalized as follows: in our determinant replace the i -th row by the j -th row and develop according to this new row. For $i \neq j$ that determinant is 0 and for $i = j$ it is D :

$$a_{j1}A_{i1} + a_{j2}A_{i2} + \dots + a_{jn}A_{in} = \begin{cases} D & \text{for } j = i \\ 0 & \text{for } j \neq i \end{cases} \quad (16)$$

If we interchange the rows and the columns we get the following formula:

$$a_{1h}A_{1k} + a_{2h}A_{2k} + \dots + a_{nh}A_{nk} = \begin{cases} D & \text{for } h = k \\ 0 & \text{for } h \neq k \end{cases} \quad (17)$$

Now let A represent an n -rowed and B an m -rowed square matrix. By $|B|, |A|$ we mean their determinants. Let C be a matrix of n rows and m columns and form the square matrix of $n + m$ rows

$$\begin{pmatrix} A & C \\ \mathbf{0} & B \end{pmatrix} \quad (18)$$

where $\mathbf{0}$ stands for a zero matrix with m rows and n columns. If we consider the determinant of the matrix (18) as a function of the columns of A only, it satisfies obviously the first two of our axioms. Because of (14) its value is $c \cdot |A|$ where c is the determinant of (18) after substituting unit vectors for the columns of A . This c still depends on B and considered as function of the rows of B satisfies the first two axioms. Therefore the determinant of (18) is $d \cdot |A| \cdot |B|$ where d is the special case of the determinant of (18) with unit vectors for the columns of A as well as of B . Subtracting multiples of the columns of A from C we can replace C by $\mathbf{0}$. This shows $d = 1$ and hence the formula

$$\begin{vmatrix} A & C \\ \mathbf{0} & B \end{vmatrix} = |A| \cdot |B|. \quad (19)$$

In a similar fashion we could have shown

$$\begin{vmatrix} A & \mathbf{0} \\ C & B \end{vmatrix} = |A| \cdot |B|. \quad (20)$$

The formulas (19), (20) are special cases of a general theorem by **Lagrange** that can be derived from them. We refer the reader to any textbook on determinants since in most applications (19) and (20) are sufficient.

We now investigate what it means for a matrix if its determinant is zero. We can easily establish the following facts:

a) If $(\mathbf{A}_1, \mathbf{A}_2, \dots, \mathbf{A}_n)$ are linearly dependent, then $D(\mathbf{A}_1, \mathbf{A}_2, \dots, \mathbf{A}_n) = 0$. Indeed one of the vectors, say \mathbf{A}_k is then a linear combination of the other columns; subtracting this linear combination from the column \mathbf{A}_k , reduces it to 0 and so $D = 0$.

b) If any vector \mathbf{B} can be expressed as linear combination of $(\mathbf{A}_1, \mathbf{A}_2, \dots, \mathbf{A}_n)$ then $D(\mathbf{A}_1, \mathbf{A}_2, \dots, \mathbf{A}_n) \neq 0$. Returning to (8) and (12) we may select the values for b_{ik} in such a fashion that every $\mathbf{A}'_i = \mathbf{U}_i$. For this choice the left side in (12) is 1 and hence $D(\mathbf{A}_1, \mathbf{A}_2, \dots, \mathbf{A}_n)$ on the right side $\neq 0$.

c) Let $(\mathbf{A}_1, \mathbf{A}_2, \dots, \mathbf{A}_n)$ be linearly independent and \mathbf{B} any other vector. If we go back to the components in the equation $\mathbf{A}_1x_1 + \mathbf{A}_2x_2 + \dots + \mathbf{A}_nx_n + \mathbf{B}y = 0$ we obtain n linear homogeneous equations in the $n + 1$ unknowns x_1, x_2, \dots, x_n, y . Consequently, there is a non-trivial solution. y must be $\neq 0$ or else the $(\mathbf{A}_1, \mathbf{A}_2, \dots, \mathbf{A}_n)$ would be linearly dependent. But then we can compute \mathbf{B} out of this equation as a linear combination of $(\mathbf{A}_1, \mathbf{A}_2, \dots, \mathbf{A}_n)$.

Combining these results we obtain:

A determinant vanishes if and only if the column vectors (or the row vectors) are linearly dependent.

Another way of expressing this result is:

The set of n linear homogeneous equations

$$a_{i1}x_1 + a_{i2}x_2 + \dots + a_{in}x_n = 0, \quad (i = 1, 2, \dots, n)$$

in n unknowns has a non-trivial solution if and only if the determinant of the coefficients is zero.

Another result that can be deduced is:

If $(\mathbf{A}_1, \mathbf{A}_2, \dots, \mathbf{A}_n)$ are given, then their linear combinations can represent any other vector \mathbf{B} if and only if $D(\mathbf{A}_1, \mathbf{A}_2, \dots, \mathbf{A}_n) \neq 0$.

Or:

The set of linear equations

$$a_{i1}x_1 + a_{i2}x_2 + \dots + a_{in}x_n = b_i \quad (i = 1, 2, \dots, n) \quad (21)$$

has a solution for arbitrary values of the b_{ik} if and only if the determinant of a_{ik} is $\neq 0$. In that case the solution is unique.

We finally express the solution of (21) by means of determinants if the determinant D of the a_{ik} is $\neq 0$.

We multiply for a given k the i -th equation with \mathbf{A}_i , and add the equations. (17) gives

$$D \cdot x_k = A_{1k}b_1 + A_{2k}b_2 + \dots + A_{nk}b_n, \quad (k = 1, 2, \dots, n) \quad (22)$$

and this gives x_k . The right side in (14) may also be written as the determinant obtained from D by replacing the k -th column by (b_1, b_2, \dots, b_n) . The rule thus obtained is known as **Cramer's rule**.

2 FIELD THEORY

A. Extension Fields

If \mathbb{E} is a field and \mathbb{F} a subset of \mathbb{E} which, under the operations of addition and multiplication in \mathbb{E} , itself forms a field, that is, if \mathbb{F} is a subfield of \mathbb{E} , then we shall call \mathbb{E} an **extension** of \mathbb{F} . The relation of being an extension of \mathbb{F} will be briefly designated by $\mathbb{F} \subset \mathbb{E}$. If $\alpha, \beta, \gamma, \dots$ are elements of \mathbb{E} , then by $\mathbb{F}(\alpha, \beta, \gamma, \dots)$ we shall mean the set of elements in \mathbb{E} which can be expressed as quotients of polynomials in $\alpha, \beta, \gamma, \dots$ with coefficients in \mathbb{F} . It is clear that $\mathbb{F}(\alpha, \beta, \gamma, \dots)$ is a field and is the smallest extension of \mathbb{F} which contains the elements $\alpha, \beta, \gamma, \dots$. We shall call $\mathbb{F}(\alpha, \beta, \gamma, \dots)$ the field obtained after the adjunction of the elements $\alpha, \beta, \gamma, \dots$ to \mathbb{F} , or the field generated out of \mathbb{F} by the elements $\alpha, \beta, \gamma, \dots$. In the sequel all fields will be assumed commutative.

If $\mathbb{F} \subset \mathbb{E}$, then ignoring the operation of multiplication defined between the elements of \mathbb{E} , we may consider $\mathbb{E} \equiv \mathcal{E}^3$ as a vector space over \mathbb{F} . By the degree of \mathbb{E} over \mathbb{F} , written (\mathbb{E}/\mathbb{F}) , we shall mean the dimension of the vector space \mathcal{E} over \mathbb{F} . If (\mathbb{E}/\mathbb{F}) is finite, \mathbb{E} will be called a finite extension.

THEOREM 6. *If $\mathbb{F}, \mathbb{B}, \mathbb{E}$ are three fields such that $\mathbb{F} \subset \mathbb{B} \subset \mathbb{E}$, then $(\mathbb{E}/\mathbb{F}) = (\mathbb{B}/\mathbb{F})(\mathbb{E}/\mathbb{B})$.*

Proof. Let $\mathbf{A}_1, \mathbf{A}_2, \dots, \mathbf{A}_n$ be elements of \mathcal{E} which are linearly independent with respect to \mathcal{B} and let $\mathbf{C}_1, \mathbf{C}_2, \dots, \mathbf{C}_s$ be elements of \mathcal{B} which are independent with respect to \mathcal{F} . Then the products $\mathbf{C}_i \mathbf{A}_j$ where $i = 1, 2, \dots, s$ and $j = 1, 2, \dots, r$ are elements of \mathcal{E} which are independent with respect to \mathcal{F} . For if $\sum_{i,j} a_{ij} \mathbf{C}_i \mathbf{A}_j = 0$, then $\sum_j (\sum_i a_{ij} \mathbf{C}_i) \mathbf{A}_j$ is a linear combination of the \mathbf{A}_j , with coefficients in \mathbb{B} and because the \mathbf{A}_j were independent with respect to \mathcal{B} we have $\sum_i a_{ij} \mathbf{C}_i = 0$ for each j . The independence of the \mathbf{C}_i with respect to \mathcal{F} then requires that each $a_{ij} = 0$. Since there are $r \cdot s$ elements $\mathbf{C}_i \mathbf{A}_j$ we have shown that for each $r \leq (\mathbb{E}/\mathbb{B})$ and $s \leq (\mathbb{B}/\mathbb{F})$ the degree $(\mathbb{E}/\mathbb{F}) \geq r \cdot s$. Therefore, $(\mathbb{E}/\mathbb{F}) \geq (\mathbb{B}/\mathbb{F})(\mathbb{E}/\mathbb{B})$. If one of the latter numbers is infinite, the theorem follows. If both (\mathbb{E}/\mathbb{B}) and (\mathbb{B}/\mathbb{F}) are finite, say r and s respectively, we may suppose that the \mathbf{A}_j and the \mathbf{C}_i are generating systems of \mathcal{E} and \mathcal{B} respectively, and we show that the set of products $\mathbf{C}_i \mathbf{A}_j$ is a generating system of \mathcal{E} over \mathbb{F} . Each $\mathbf{A} \in \mathcal{E}$ can be expressed linearly in terms of the \mathbf{A}_j with coefficients in \mathbb{B} . Thus, $\mathbf{A} = \sum \mathbf{B}_j \mathbf{A}_j$. Moreover, each \mathbf{B}_j being an element of \mathcal{B} can be expressed linearly with coefficients in \mathbb{F} in terms of the \mathbf{C}_i , i.e., $\mathbf{B}_j = \sum a_{ij} \mathbf{C}_i$, $j = 1, 2, \dots, r$. Thus, $\mathbf{A} = \sum a_{ij} \mathbf{C}_i \mathbf{A}_j$ and the \mathbf{C}_i form an independent generating system of \mathcal{E} over \mathbb{F} . \square

Corollary. *If $\mathbb{F} \subset \mathbb{F}_1 \subset \mathbb{F}_2 \subset \mathbb{F}_3 \subset \dots \subset \mathbb{F}_n$, then $(\mathbb{F}_n/\mathbb{F}) = (\mathbb{F}_2/\mathbb{F}_1) \cdot (\mathbb{F}_3/\mathbb{F}_2) \cdots (\mathbb{F}_n/\mathbb{F}_{n-1})$.*

B. Polynomials

An expression of the form

$$a_0 x^n + a_1 x^{n-1} + \cdots + a_n$$

³The calligraphic symbols $\mathcal{E}, \mathcal{B}, \mathcal{F}, \dots$ denote the vector spaces builded on the respective fields $\mathbb{E}, \mathbb{B}, \mathbb{F}, \dots$ (tex-editor's note).

is called a **polynomial** in \mathbb{F} of degree n if the coefficients a_0, a_1, \dots, a_n , are elements of the field \mathbb{F} and $a_0 \neq 0$. Multiplication and addition of polynomials are performed in the usual way⁴.

A polynomial in \mathbb{F} is called **reducible** in \mathbb{F} if it is equal to the product of two polynomials in \mathbb{F} each of degree at least one. Polynomials which are not reducible in \mathbb{F} are called **irreducible** in \mathbb{F} .

If $f(x) = g(x) \cdot h(x)$ is a relation which holds between the polynomials $f(x), g(x), h(x)$ in a field \mathbb{F} , then we shall say that $g(x)$ divides $f(x)$ in \mathbb{F} , or that $g(x)$ is a **factor** of $f(x)$. It is readily seen that the **degree** of $f(x)$ is equal to the sum of the degrees of $g(x)$ and $h(x)$, so that if neither $g(x)$ nor $h(x)$ is a constant then each has a degree less than $f(x)$. It follows from this that by a finite number of factorizations a polynomial can always be expressed as a product of irreducible polynomials in a field \mathbb{F} .

For any two polynomials $f(x)$ and $g(x)$ the **division algorithm** holds, i.e., $f(x) = q(x) \cdot g(x) + r(x)$ where $q(x)$ and $r(x)$ are unique polynomials in \mathbb{F} and the degree of $f(x)$ is less than that of $g(x)$. This may be shown by the same argument as the reader met in elementary algebra in the case of the field of real or complex numbers. We also see that $r(x)$ is the uniquely determined polynomial of a degree less than that of $g(x)$ such that $f(x) - r(x)$ is divisible by $g(x)$. We shall call $r(x)$ the **remainder** of $f(x)$.

Also, in the usual way, it may be shown that if u is a root of the polynomial $f(x)$ in \mathbb{F} then $x - u$ is a factor of $f(x)$, and as a consequence of this that a polynomial in a field cannot have more roots in the field than its degree.

Lemma. *If $f(x)$ is an irreducible polynomial of degree n in \mathbb{F} , then there do not exist two polynomials each of degree less than n in \mathbb{F} whose product is divisible by $f(x)$.*

Let us suppose to the contrary that $g(x)$ and $h(x)$ are polynomials of degree less than n whose product is divisible by $f(x)$. Among all polynomials occurring in such pairs we may suppose $g(x)$ has the smallest degree. Then since $f(x)$ is a factor of $g(x) \cdot h(x)$ there is a polynomial $k(x)$ such that

$$k(x) \cdot f(x) = g(x) \cdot h(x)$$

By the division algorithm,

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

where the degree of $r(x)$ is less than that of $g(x)$ and $r(x) \neq 0$ since $f(x)$ was assumed irreducible. Multiplying

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

by $h(x)$ and transposing, we have

$$r(x) \cdot h(x) = f(x) \cdot h(x) - q(x) \cdot g(x) \cdot h(x) = f(x) \cdot h(x) - q(x) \cdot k(x) \cdot f(x)$$

from which it follows that $r(x) \cdot h(x)$ is divisible by $f(x)$. Since $r(x)$ has a smaller degree than $g(x)$, this last is in contradiction to the choice of $g(x)$, from which the lemma follows.

As we saw, many of the theorems of elementary algebra hold in any field \mathbb{F} . However, the so-called **Fundamental Theorem of Algebra**, at least in its customary form, does not hold. It will be replaced

⁴If we speak of the set of all polynomials of degree lower than n , we shall agree to include the polynomial 0 in this set, though it has no degree in the proper sense

by a theorem due to **Kronecker** which guarantees for a given polynomial in \mathbb{F} the existence of an extension field in which the polynomial has a root. We shall also show that, in a given field, a polynomial cannot only be factored into irreducible factors, but that this factorization is unique up to a constant factor. The uniqueness depends on the theorem of Kronecker.

C. Algebraic Elements

Let \mathbb{F} be a field and \mathbb{E} an extension field of \mathbb{F} . If α is an element of \mathbb{E} we may ask whether there are polynomials with coefficients in \mathbb{F} which have α as root. α is called **algebraic** with respect to \mathbb{F} if there are such polynomials. Now let α be algebraic and select among all polynomials in \mathbb{F} which have α as root, one, $f(x)$, of lowest degree.

We may assume that the highest coefficient of $f(x)$ is 1. We contend that this $f(x)$ is uniquely determined, that it is irreducible and that each polynomial in \mathbb{F} with the root α is divisible by $f(x)$. If, indeed, $g(x)$ is a polynomial in \mathbb{F} with $g(\alpha) = 0$, we may divide $g(x) = f(x)q(x) + r(x)$ where $r(x)$ has a degree smaller than that of $f(x)$. Substituting $x = \alpha$ we get $r(\alpha) = 0$; now $r(x)$ has to be identically 0 since otherwise $r(x)$ would have the root α and would be of lower degree than $f(x)$: so $g(x)$ is divisible by $f(x)$. This also shows the uniqueness of $f(x)$. If $f(x)$ were not irreducible, one of the factors would have to vanish for $x = \alpha$ contradicting again the choice of $f(x)$.

We consider now the subset \mathbf{E}_0 of the following elements θ of \mathbb{E} :

$$\theta = g(\alpha) = c_0 + c_1\alpha + c_2\alpha^2 + \cdots + c_{n-1}\alpha^{n-1}$$

where $g(x)$ is a polynomial in \mathbb{F} of degree less than n (n being the degree of $f(x)$). This set \mathbf{E}_0 , is closed under addition and multiplication. The latter may be verified as follows:

If $g(x)$ and $h(x)$ are two polynomials of degree less than n we put $g(x)h(x) = q(x)f(x) + r(x)$ and hence $g(\alpha)h(\alpha) = r(\alpha)$. Finally we see that the constants c_0, c_1, \dots, c_{n-1} are uniquely determined by the element θ . Indeed two expressions for the same θ would lead after subtracting to an equation for α of lower degree than n .

We remark that the internal structure of the set \mathbf{E}_0 does not depend on the nature of α but only on the irreducible $f(x)$. The knowledge of this polynomial enables us to perform the operations of addition and multiplication in our set \mathbf{E}_0 . We shall see very soon that \mathbf{E}_0 is a field; in fact, \mathbf{E}_0 is nothing but the field $\mathbb{F}(\alpha)$. As soon as this is shown we have at once the degree, $(\mathbb{F}(\alpha)/\mathbb{F})$, determined as n , since the space $\mathbb{F}(\alpha)$ is generated by the linearly independent $1, \alpha, \alpha^2, \dots, \alpha^{n-1}$.

We shall now try to imitate the set \mathbf{E}_0 without having an extension field \mathbb{E} and an element α at our disposal. We shall assume only an irreducible polynomial

$$f(x) = x^n + a_{n-1}x^{n-1} + \cdots + \alpha_0$$

as given.

We select a symbol ξ and let \mathbf{E}_1 be the set of all formal polynomials

$$g(\xi) = c_0 + c_1\xi + \cdots + c_{n-1}\xi^{n-1}$$

of a degree lower than n . This set forms a group under addition. We now introduce besides the ordinary multiplication a new kind of multiplication of two elements $g(\xi)$ and $h(\xi)$ of \mathbf{E}_1 denoted by $g(\xi) \times h(\xi)$. It is defined as the remainder $r(\xi)$ of the ordinary product $g(\xi)h(\xi)$ under division by $f\xi$. We first remark that any product of m terms $g_1(\xi) \cdot g_2(\xi) \cdots g_m(\xi)$ is again the remainder of the ordinary product $g_1(\xi) \times g_2(\xi) \times \cdots \times g_m(\xi)$. This is true by definition for $m = 2$ and follows for every m by induction if we just prove the easy **lemma**: *The remainder of the product of two remainders (of two polynomials) is the remainder of the product of these two polynomials.* This fact shows that our new product is associative and commutative and also that the new product $g_1(\xi) \times g_2(\xi) \times \cdots \times g_m(\xi)$ will coincide with the old product $g_1(\xi)g_2(\xi) \cdots g_m(\xi)$ if the latter does not exceed n in degree. The distributive law for our multiplication is readily verified.

The set \mathbf{E}_1 contains our field \mathbb{F} and our multiplication in \mathbf{E}_1 has for \mathbb{F} the meaning of the old multiplication. One of the polynomials of \mathbf{E}_1 is ξ . Multiplying it i -times with itself, clearly will just lead to ξ^i as long as $i < n$. For $i = n$ this is not any more the case since it leads to the remainder of the polynomial ξ^n .

This remainder is

$$\xi^n - f(\xi) = -a_{n-1}\xi^{n-1} - a_{n-2}\xi^{n-2} - \cdots - a_0.$$

We now give up our old multiplication altogether and keep only the new one; we also change notation, using the point (or juxtaposition) as symbol for the new multiplication. Computing in this sense $c_0 + c_1\xi + c_2\xi^2 + \cdots + c_{n-1}\xi^{n-1}$ will readily lead to this element, since all the degrees involved are below n . But

$$\xi^n = -a_{n-1}\xi^{n-1} - a_{n-2}\xi^{n-2} - \cdots - a_0$$

. Transposing we see that $f(\xi) = 0$.

We thus have constructed a set \mathbf{E}_1 and an addition and multiplication in \mathbf{E}_1 that already satisfies most of the field axioms. \mathbf{E}_1 contains \mathbb{F} as subfield and ξ satisfies the equation $f(\xi) = 0$. We next have to show: If $g(\xi) \neq 0$ and $h(\xi)$ are given elements of \mathbf{E}_1 , there is an element

$$X(\xi) = x_0 + x_1\xi + \cdots + x_{n-1}\xi^{n-1}$$

in \mathbf{E}_1 such that

$$g(\xi) \cdot X(\xi) = h(\xi).$$

To prove it we consider the coefficients x_i of $X(\xi)$ as unknowns and compute nevertheless the product on the left side, always reducing higher powers of ξ to lower ones. The result is an expression $L_0 + L_1\xi + \cdots + L_{n-1}\xi^{n-1}$ where each L_i is a linear combination of the x_i with coefficients in \mathbb{F} . This expression is to be equal to $h(\xi)$; this leads to the n equations with n unknowns:

$$L_0 = b_0, L_1 = b_1, \dots, L_{n-1} = b_{n-1}$$

where the b_i are the coefficients of $h(\xi)$. This system will be soluble if the corresponding homogeneous equations

$$L_0 = 0, L_1 = 0, \dots, L_{n-1} = 0$$

bave only the trivial solution.

The homogeneous problem would occur if we should ask for the set of elements $X(Q)$ satisfying $g(\xi) \cdot X(\xi) = 0$. Going back for a moment to the old multiplication this would mean that the ordinary product $g(\xi)X(\xi)$ has the remainder 0, and is therefore divisible by $f(\xi)$. According to the lemma, page (19), this is only possible for $X(\xi) = 0$. Therefore \mathbf{E}_1 is a field.

Assume now that we have also our old extension \mathbb{E} with a root α of $f(x)$, leading to the set \mathbf{E}_1 . We see that \mathbf{E}_0 has in a certain sense the same structure as \mathbf{E}_1 if we map the element $g(\xi)$ of \mathbf{E}_1 onto the element $g(\alpha)$ of \mathbf{E}_0 . This mapping will have the property that the image of a sum of elements is the sum of the images, and the image of a product is the product of the images.

Let us therefore define: A mapping σ of one field onto another which is one to one in both directions such that $\sigma(\alpha + \beta) = \sigma(\alpha) + \sigma(\beta)$ and $\sigma(\alpha \cdot \beta) = \sigma(\alpha) \cdot \sigma(\beta)$ is called an **isomorphism**. If the fields in question are not distinct - i.e., are both the same field - the isomorphism is called an **automorphism**. Two fields for which there exists an isomorphism mapping one on another are called isomorphic. If not every element of the image field is the image under σ of an element in the first field, then σ is called an isomorphism of the first field into the second. Under each isomorphism it is clear that $\sigma(0) = 0$ and $\sigma(1) = 1$.

We see that \mathbf{E}_0 is also a field and that it is isomorphic to \mathbf{E}_1 .

We now mention a few theorems that follow from our discussion:

THEOREM 7. (Kronecker) *If $f(x)$ is a polynomial in a field \mathbb{F} , there exists an extension \mathbb{E} of \mathbb{F} in which $f(x)$ has a root.*

Proof: Construct an extension field in which an irreducible factor of $f(x)$ has a root. □

THEOREM 8. *Let σ be an isomorphism mapping a field \mathbb{F} on a field \mathbb{F}' . Let $f(x)$ be an irreducible polynomial in \mathbb{F} and $f'(x)$ the corresponding polynomial in \mathbb{F}' . If $\mathbb{E} = \mathbb{F}(\beta)$ and $\mathbb{E}' = \mathbb{F}'(\beta')$ are extensions of \mathbb{F} and \mathbb{F}' , respectively, where $f(\beta) = 0$ in \mathbb{E} and $f'(\beta') = 0$ in \mathbb{E}' , then σ can be extended to an isomorphism between \mathbb{E} and \mathbb{E}' .*

Proof: \mathbb{E} and \mathbb{E}' are both isomorphic to \mathbf{E}_0 . □

D. Splitting Fields

If \mathbb{F} , \mathbb{B} and \mathbb{E} are three fields such that $\mathbb{F} \subset \mathbb{B} \subset \mathbb{E}$, then we shall refer to \mathbb{B} as an intermediate field.

If \mathbb{E} is an extension of a field \mathbb{F} in which a polynomial $p(x)$ in \mathbb{F} can be factored into linear factors, and if $p(x)$ cannot be so factored in any intermediate field, then we call \mathbb{E} a **splitting field** for $p(x)$. Thus, if \mathbb{E} is a splitting field of $p(x)$, the roots of $p(x)$ generate \mathbb{E} .

A splitting field is of finite degree since it is constructed by a finite number of adjunctions of algebraic elements, each defining an extension field of finite degree. Because of the corollary on page (19), the total degree is finite.

THEOREM 9. *If $p(x)$ is a polynomial in a field \mathbb{F} , there exists a splitting field \mathbb{E} of $p(x)$.*

Proof. We factor $p(x)$ in \mathbb{F} into irreducible factors $f_1(x) \cdots f_r(x) = p(x)$. If each of these is of the first degree then \mathbb{F} itself is the required splitting field. Suppose then that $f_1(x)$ is of degree higher than the first. By Theorem 7 there is an extension \mathbb{F}_1 of \mathbb{F} in which $f_1(x)$ has a root. Factor each of the factors $f_1(x), \dots, f_r(x)$ into irreducible factors in \mathbb{F}_1 and proceed as before. We finally arrive at a field in which $p(x)$ can be split into linear factors. The field generated out of \mathbb{F} by the roots of $p(x)$ is the required splitting field. \square

The following theorem asserts that up to isomorphisms, the splitting field of a polynomial is unique.

THEOREM 10. *Let σ be an isomorphism mapping the field \mathbb{F} on the field \mathbb{F}' , let $p(x)$ be a polynomial in \mathbb{F} and $p'(x)$ the polynomial in \mathbb{F}' with coefficients corresponding to those of $p(x)$ under σ . Finally, let \mathbb{E} be a splitting field of $p(x)$ and \mathbb{E}' a splitting field of $p'(x)$.*

Under these conditions the isomorphism σ can be extended to an isomorphism between \mathbb{E} and \mathbb{E}' .

Proof. If $f(x)$ is an irreducible factor of $p(x)$ in \mathbb{F} , then \mathbb{E} contains a root of $f(x)$. For let $p(x) = (x - a_1)(x - a_2) \cdots (x - a_s)$ be the splitting of $p(x)$ in \mathbb{E} . Then $(x - a_r)(x - a_{r+1}) \cdots (x - a_s) = f(x) \cdot g(x)$. We consider $f(x)$ as a polynomial in \mathbb{E} and construct the extension field $\mathbb{B} = \mathbb{E}(a)$ in which $f(a) = 0$. Then $(a - a_1)(a - a_2) \cdots (a - a_s) = f(a) \cdot g(a) = 0$ and $a - a_i$ being elements of the field \mathbb{B} can have a product equal to 0 only if for one of the factors, say the first, we have $a - a_1 = 0$. Thus, $a = a_1$, and a_1 is a root of $f(x)$.

Now in case all roots of $p(x)$ are in \mathbb{F} , then $\mathbb{E} = \mathbb{F}$ and $p(x)$ can be split in \mathbb{F} . This factored form has an image in \mathbb{F}' which is a splitting, of $p'(x)$, since the isomorphism σ preserves all operations of addition and multiplication in the process of multiplying out the factors of $p(x)$ and collecting to get the original form. Since $p'(x)$ can be split in \mathbb{F}' , we must have $\mathbb{F}' = \mathbb{E}'$. In this case, σ itself is the required extension and the theorem is proved if **all** roots of $p(x)$ are in \mathbb{F} .

We proceed by complete induction. Let us suppose the theorem proved for all cases in which the number of roots of $p(x)$ outside of \mathbb{F} is less than $n > 1$, and suppose that $p(x)$ is a polynomial having n roots outside of \mathbb{F} . We factor $p(x)$ into irreducible factors in \mathbb{F}' $p(x) = f_1(x) \cdot f_2(x) \cdots f_n(x)$. Not all of these factors can be of degree 1, since otherwise $p(x)$ would split in \mathbb{F} , contrary to assumption.

Hence, we may suppose the degree of $f_1(x)$ to be $r > 1$. Let $f'_1(x) \cdot f'_2(x) \cdots f'_m(x) = p'(x)$ be the factorization of $p'(x)$ into the polynomials corresponding to $f_1(x), \dots, f_m(x)$ under σ . $f_i(x)$ is irreducible in \mathbb{F}' , for a factorization of $f_i(x)$ in \mathbb{F}' would induce⁵ a factorization of $f(x)$, which was however taken to be irreducible.

By Theorem 8, the isomorphism σ can be extended to an isomorphism σ_1 , between the fields $\mathbb{F}(a)$ and $\mathbb{F}'(a')$. Since $\mathbb{F} \subset \mathbb{F}(a)$, $p(x)$ is a polynomial in $\mathbb{F}(U)$ and \mathbb{E} is a splitting field for $p(x)$ in $\mathbb{F}(a)$. Similarly for $p'(x)$. There are now less than n roots of $p(x)$ outside the new ground field $\mathbb{F}(a)$. Hence by our inductive assumption σ_1 can be extended from an isomorphism between $\mathbb{F}(a)$ and $\mathbb{F}'(a')$ to an isomorphism σ_2 between \mathbb{E} and \mathbb{E}' . Since σ_1 , is an extension of σ^{-1} , and σ_2 an extension of σ_1 , we conclude σ_2 is an extension of σ and the theorem follows. \square

Corollary *If $p(x)$ is a polynomial in a field \mathbb{F} , then any two splitting fields for $p(x)$ are isomorphic.*

⁵See the following for the definition of σ^{-1} under σ^{-1}

Proof. This follows from Theorem 10 if we take $\mathbb{F} = \mathbb{F}'$ and σ to be the identity mapping, i.e., $\sigma(x) = x$. \square

As a consequence of this corollary we see that we are justified in using the expression *the splitting field of $p(x)$* since any two differ only by an isomorphism. Thus, if $p(x)$ has repeated roots in one splitting field, so also in **any other** splitting field it will have repeated roots. The statement *$p(x)$ has repeated roots* will be significant without reference to a particular splitting field.

E. Unique Decomposition of Polynomials into Irreducible Factors

THEOREM 11. *If $p(x)$ is a polynomial in a field \mathbb{F} , and if $p(x) = p_1(x) \cdot p_2(x) \cdots p_r(x) = q_1(x) \cdot q_2(x) \cdots q_s(x)$ are two factorizations of $p(x)$ into irreducible polynomials each of degree **at least one**, then $r = s$ and after a suitable change in the order in which the q 's are written, $p_i(x) = c_i q_i(x)$, $i = 1, 2, \dots, r$ and $c_i \in \mathbb{F}$.*

Proof. Let $\mathbb{F}(a)$ be an extension of \mathbb{F} in which $p_1(a) = 0$. We may suppose the leading coefficients of the $p_i(x)$ and the $q_i(x)$ to be 1, for, by factoring out all leading coefficients and combining, the constant multiplier on each side of the equation must be the leading coefficient of $p(x)$ and hence can be divided out of both sides of the equation. Since $0 = p_1(a) \cdot p_2(a) \cdots p_r(a) = p(a) = q_1(a) \cdots q_s(a)$ and since a product of elements of $\mathbb{F}(a)$ can be 0 only if one of these is 0, it follows that one of the $q_i(a)$, say $q_1(a)$, is 0. This gives $p_1(x) = q_1(x)$. Thus $p_1(x) \cdot p_2(x) \cdots p_r(x) = p_1(x) \cdot q_2(x) \cdots q_s(x)$ or $p_1(x) \cdot [p_2(x) \cdots p_r(x) - q_2(x) \cdots q_s(x)] = 0$. Since the product of two polynomials is 0 only if one of the two is the 0 polynomial, it follows that the polynomial within the brackets is 0 so that $p_2(x) \cdots p_r(x) = q_2(x) \cdots q_s(x)$.

If we repeat the above argument r times we obtain $p_i(x) = q_i(x)$, $i = 1, 2, \dots, r$. Since the remaining q 's must have a product 1, it follows that $r = s$.

F. Group Characters

If G is a multiplicative group, \mathbb{F} a field and σ a homomorphism mapping G into \mathbb{F} , then σ is called a **character** of G in \mathbb{F} . By **homomorphism** is meant a mapping σ such that for α, β any two elements of G , $\sigma(\alpha) \cdot \sigma(\beta) = \sigma(\alpha \cdot \beta)$ and $\sigma(\alpha) \neq 0$ for any α .

(If $\sigma(\alpha) = 0$ for one element α , then $\sigma(x) = 0$ for each $x \in G$, since $\sigma(\alpha \cdot y) = \sigma(\alpha) \cdot \sigma(y) = 0$ and $\alpha \cdot y$ takes all values in G when y assumes all values in G).

The characters $\sigma_1, \sigma_2, \dots, \sigma_n$ are called dependent if there exist elements a_1, a_2, \dots, a_n not all zero in \mathbb{F} such that $a_1 \sigma_1(x) + a_2 \sigma_2(x) + \cdots + a_n \sigma_n(x) = 0$ for each $x \in G$. Such a dependence relation is called *non-trivial*. If the characters are not dependent they are called independent.

THEOREM 12. *If G is a group and $\sigma_1, \sigma_2, \dots, \sigma_n$ are n mutually distinct characters of G in a field \mathbb{F} , then $\sigma_1, \sigma_2, \dots, \sigma_n$ are independent.*

One character cannot be dependent, since a $a_1 \sigma_1(x) = 0$ implies $a_1 = 0$ due to the assumption that

$\sigma_1(x) \neq 0$. Suppose $n > 1$. We make the inductive assumption that no set of less than n distinct characters is dependent. Suppose now that $a_1\sigma_1(x), a_2\sigma_2(x), \dots, a_n\sigma_n(x) = 0$ is a *non-trivial* dependence between the σ 's. None of the elements a_i is zero, else we should have a dependence between less than n characters contrary to our inductive assumption. Since σ_1 and σ_n are distinct, there exists an element a in G such that $\sigma_1(a) \neq \sigma_n(a)$. Multiplying the relation between the σ 's by a_n^{-1} we obtain a relation

$$(*) \quad b_1\sigma_1(x) + \dots + b_{n-1}\sigma_{n-1}(x) + \sigma_n(x) = 0, \quad b_i = a_n^{-1}a_i \neq 0.$$

Replace in this relation x by ax . We have

$$b_1\sigma_1(a)\sigma_1(x) + \dots + b_{n-1}\sigma_{n-1}(a)\sigma_{n-1}(x) + \sigma_n(a)\sigma_n(x) = 0$$

or

$$\sigma_n^{-1}(a)b_1\sigma_1(a)\sigma_1(x) + \dots + \sigma_n(x) = 0.$$

Subtracting the latter from $(*)$ we have

$$(**) \quad [b_1 - \sigma_n^{-1}(a)b_1\sigma_1(a)]\sigma_1(x) + \dots + [b_{n-1} - \sigma_n^{-1}(a)b_{n-1}\sigma_{n-1}(a)]\sigma_{n-1}(x) = 0.$$

The coefficient of $\sigma_1(x)$ in this relation is not 0, otherwise we should have

$$b_1 = \sigma_n^{-1}(a)b_1\sigma_1(a),$$

so that $\sigma_n(a)b_1 = b_1\sigma_1(a)$, and since $b_1 \neq 0$, we get $\sigma_n(a) = \sigma_1(a)$ contrary to the choice of a .

Thus, $(**)$ is a non-trivial dependence between $\sigma_1, \sigma_2, \dots, \sigma_{n-1}$ which is *contrary* to our inductive assumption.

Corollary. *If \mathbb{E} and \mathbb{E}' are two fields, and $\sigma_1, \sigma_2, \dots, \sigma_n$ are n mutually distinct isomorphisms mapping \mathbb{E} into \mathbb{E}' , then $\sigma_1, \sigma_2, \dots, \sigma_n$ are **independent**. (Where independent again means there exists no non-trivial dependence $a_1\sigma_1(x) + \dots + a_n\sigma_n(x) = 0$ which holds for every $x \in \mathbb{E}$).*

This follows from Theorem 12 since \mathbb{E} without the 0 is a **group** and the σ 's defined in this group are mutually distinct characters. \square

If $\sigma_1, \sigma_2, \dots, \sigma_n$ are isomorphisms of a field \mathbb{E} into a field \mathbb{E}' , then each element a of \mathbb{E} such that $\sigma_1(a) = \sigma_2(a) = \dots = \sigma_n(a)$ is called a **fixed point** of \mathbb{E} under $\sigma_1, \sigma_2, \dots, \sigma_n$. This name is chosen because in the case where the σ 's are automorphisms and σ_1 is the identity, i.e., $\sigma_1(x) = x$, we have $\sigma_i(x) = x$ for a fixed point.

Lemma. *The set of fixed points of \mathbb{E} is a subfield of \mathbb{E} . We shall call this subfield the **fixed field**.*

For if a and b are fixed points, then

$$\sigma_i(a+b) = \sigma_i(a) + \sigma_i(b) = \sigma_j(a) + \sigma_j(b) = \sigma_j(a+b)$$

and

$$\sigma_i(a \cdot b) = \sigma_i(a) \cdot \sigma_i(b) = \sigma_j(a) \cdot \sigma_j(b) = \sigma_j(a \cdot b).$$

Finally from $\sigma_i(a) = \sigma_j(a)$ we have $(\sigma_i(a))^{-1} = (\sigma_j(a))^{-1} = \sigma_i(a^{-1}) = \sigma_j(a^{-1})$.

Thus, the sum and product of two fixed points is a fixed point, and the inverse of a fixed point is a fixed point. Clearly, the negative of a fixed point is a fixed point.

THEOREM 13. *If $\sigma_1, \sigma_2, \dots, \sigma_n$ are n mutually distinct isomorphisms of a field \mathbb{E} into a field \mathbb{E}' , and if \mathbb{F} is the fixed field of \mathbb{E} , then $(\mathbb{E}/\mathbb{F}) > n$.*

Suppose to the contrary that $(\mathbb{E}/\mathbb{F}) = r < n$. We shall show that we are led to a contradiction. Let $\omega_1, \omega_2, \dots, \omega_r$, be a generating system of \mathcal{E} over \mathbb{F} . In the homogeneous linear equations

$$\begin{aligned} \sigma_1(\omega_1)x_1 + \sigma_2(\omega_1)x_2 + \cdots + \sigma_n(\omega_1)x_n &= 0 \\ \sigma_1(\omega_2)x_1 + \sigma_2(\omega_2)x_2 + \cdots + \sigma_n(\omega_2)x_n &= 0 \\ &\vdots \\ \sigma_1(\omega_r)x_1 + \sigma_2(\omega_r)x_2 + \cdots + \sigma_n(\omega_r)x_n &= 0 \end{aligned}$$

there are more unknowns than equations so that there exists a nontrivial solution which, we may suppose, x_1, x_2, \dots, x_n , denotes. For any element a in \mathbb{E} we can find a_1, a_2, \dots, a_r in \mathbb{F} such that $a = a_1\omega_1 + a_2\omega_2 + \cdots + a_r\omega_r$. We multiply the first equation by $\sigma_1(a_1)$, the second by $\sigma_1\omega_2$ and so on. Using that $a_i \in \mathbb{F}$, hence that $\sigma_1(a_i) = \sigma_j(a_i)$ and also that $\sigma_j(a_i)\sigma_j(\omega_i) = \sigma_j(a_i\omega_i)$, we obtain

$$\begin{aligned} \sigma_1(a_1\omega_1)x_1 + \cdots + \sigma_n(a_1\omega_1)x_n &= 0 \\ &\vdots \\ \sigma_1(a_r\omega_r)x_1 + \cdots + \sigma_n(a_r\omega_r)x_n &= 0 \end{aligned}$$

Adding these last equations and using

$$\sigma_i(a_1\omega_1) + \sigma_i(a_2\omega_2) + \cdots + \sigma_i(a_r\omega_r) = \sigma_i(a_1\omega_1 + \cdots + a_r\omega_r) = \sigma_i(a)$$

we obtain

$$\sigma_1(a)x_1 + \sigma_2(a)x_2 + \cdots + \sigma_n(a)x_n = 0.$$

This, however, is a *non-trivial* dependence relation between $\sigma_1, \sigma_2, \dots, \sigma_n$ which cannot exist according to the corollary of Theorem 12.

Corollary. *If $\sigma_1, \sigma_2, \dots, \sigma_n$ are automorphisms of the field \mathbb{E} , and \mathbb{F} is the fixed field, then $(\mathbb{E}/\mathbb{F}) \geq n$.*

If \mathbb{F} is a subfield of the field \mathbb{E} , and σ an automorphism of \mathbb{E} , we shall say that σ leaves \mathbb{F} fixed if for **each** element a of \mathbb{F} , $\sigma(a) = a$. If σ and τ are two automorphisms of \mathbb{E} , then the mapping $\sigma(\tau(x))$ written briefly $\sigma\tau$ is an automorphism, as the reader may readily verify. [E.g., $\sigma\tau(x \cdot y) = \sigma(\tau(x \cdot y)) = \sigma(\tau(x) \cdot \tau(y)) = \sigma(\tau(x)) \cdot \sigma(\tau(y))$]. \square

We shall call $\sigma\tau$ the product of σ and τ . If σ is an automorphism ($\sigma(x) = y$), then we shall call σ^{-1} the mapping of y into x , i.e., $\sigma^{-1}(y) = x$ the **inverse** of σ . The reader may readily verify that σ^{-1} is an automorphism. The automorphism $1(x) = x$ shall be called the unit automorphism.

Lemma. *If \mathbb{E} is an extension field of \mathbb{F} , the set G of automorphisms which leave \mathbb{F} fixed is a group.*

The product of two automorphisms which leave \mathbb{F} fixed clearly leaves \mathbb{F} fixed. Also, the inverse of any automorphism in G is in G . The reader will observe that G , the set of automorphisms which leave \mathbb{F} fixed, does not necessarily have \mathbb{F} as its fixed field. It may be that certain elements in \mathbb{E} which do not belong to \mathbb{F} are left fixed by every automorphism which leaves \mathbb{F} fixed. Thus, the fixed field of G may be larger than \mathbb{F} .

G*. Applications and Examples to Theorem 13

Theorem 13 is very powerful as the following examples show:

1) Let \mathbb{K} be a field and consider the field $\mathbb{E} = \mathbb{K}(x)$ of all rational functions of the variable x . If we map each of the functions $f(x)$ of \mathbb{E} onto $f(L)$ we obviously obtain an automorphism of \mathbb{E} . Let us consider the following six automorphisms where $f(x)$ is mapped onto $f(x)$ (identity), $f(1-x)$, $f(\frac{1}{x})$, $f(1-\frac{1}{x})$, $f(\frac{1}{1-x})$ and $f(\frac{x}{x-1})$ and call \mathbb{F} the fixed point field. \mathbb{F} consists of all rational functions satisfying

$$f(x) = f(1-x) = f\left(\frac{1}{x}\right) = f\left(1-\frac{1}{x}\right) = f\left(\frac{1}{1-x}\right) = f\left(\frac{x}{x-1}\right). \quad (23)$$

It suffices to check the first two equalities, the others being consequences.

The function

$$I = I(x) = \frac{(x^2 - x + 1)^3}{x^2(x-1)^2} \quad (24)$$

belongs to \mathbb{F} as is readily seen. Hence, the field $\mathbb{S} = \mathbb{K}(I)$ of all rational functions of I will belong to \mathbb{F} .

We contend: $\mathbb{F} = \mathbb{S}$ and $(\mathbb{E}/\mathbb{F}) = 6$.

Indeed, from Theorem 13 we obtain $(\mathbb{E}/\mathbb{F}) \geq 6$. Since $\mathbb{S} \subset \mathbb{F}$ it suffices to prove $(\mathbb{E}/\mathbb{F}) < 6$. Now $\mathbb{E} = \mathbb{S}(x)$. It is thus sufficient to find some 6-th degree equation with coefficients in \mathbb{S} satisfied by x .

The following one is obviously satisfied;

$$(x^2 - x + 1)^3 - 1 \cdot x^2(x-1)^2 = 0.$$

The reader will find the study of these fields a profitable exercise. At a later occasion he will be able to derive all intermediate fields.

2) Let \mathbb{K} be a field and $\mathbb{E} = \mathbb{K}(x_1, x_2, \dots, x_n)$ the field of all rational functions of n variables x_1, x_2, \dots, x_n . If $(\nu_1, \nu_2, \dots, \nu_n)$ is a permutation of $(1, 2, \dots, n)$ we replace in each function $f(x_1, x_2, \dots, x_n)$ of \mathbb{E} the variable x_1 , by x_{ν_1} , x_2 by x_{ν_2} , ..., x_n by x_{ν_n} . The mapping of \mathbb{E} onto itself obtained in this way is obviously an automorphism and we may construct $n!$ automorphisms in this fashion (including the identity).

Let \mathbb{F} be the fixed point field, that is, the set of all so-called *symmetric functions*. Theorem 13 shows that $(\mathbb{E}/\mathbb{F}) \geq n!$.

Let us introduce the polynomial:

$$f(t) = (t - x_1)(t - x_2) \cdots (t - x_n) = t^n + a_1 t^{n-1} + \cdots + a_n \quad (25)$$

where $a_1 = -(x_1 + x_2 + \cdots + x_n)$, $a_2 = +(x_1 x_2 + x_1 x_3 + \cdots + x_{n-1} x_n)$ and more generally a_i is $(-1)^i$ times the sum of all products of i different variables of the set x_1, x_2, \dots, x_n . The functions a_1, a_2, \dots, a_n are called the *elementary symmetric functions* and the field $\mathbb{S} = \mathbb{K}(a_1, a_2, \dots, a_n)$ of all rational functions of a_1, a_2, \dots, a_n is obviously a part of \mathbb{F} . Should we succeed in proving $(\mathbb{E}/\mathbb{S}) < n!$ we would have shown $\mathbb{S} = \mathbb{F}$ and $(\mathbb{E}/\mathbb{F}) = n!$.

We construct to this effect the following tower of fields:

$$\mathbb{S} = \mathbb{S}_n \subset \mathbb{S}_{n-1} \subset \mathbb{S}_{n-2} \subset \cdots \subset \mathbb{S}_2 \subset \mathbb{S}_1 = \mathbb{E}$$

by the definition

$$\mathbb{S}_n = \mathbb{S}; \mathbb{S}_i = \mathbb{S}(x_{i+1}, x_{i+2}, \dots, x_n) = \mathbb{S}_{i+1}(x_{i+1}). \quad (26)$$

It would be sufficient to prove $(\mathbb{S}_{i-1}/\mathbb{S}_i) \leq i$ or that the generator x_i for \mathbb{S}_{i-1} out of \mathbb{S} satisfies an equation of degree i with coefficients in \mathbb{S}_i .

Such an equation is easily constructed. Put

$$F_i(t) = \frac{f(t)}{(t - x_{i+1})(t - x_{i+2}) \cdots (t - x_n)} = \frac{F_{i+1}(t)}{(t - x_{i+1})}(t - x_{i+1}) \quad (27)$$

and $F_n(t) = f(t)$. Performing the division we see that $F_i(t)$ is a polynomial in t of degree i whose highest coefficient is 1 and whose coefficients are polynomials in the variables a_1, a_2, \dots, a_n , and $x_{i+1}, x_{i+2}, \dots, x_n$. Only integers enter as coefficients in these expressions. Now x_i is obviously a root of $F_i(t) = 0$.

Now let $g(x_1, x_2, \dots, x_n)$ be a polynomial x_1, x_2, \dots, x_n . Since $F_1(x_1) = 0$ is of first degree in x_1 , we can express x_1 as a polynomial of the a_1 , and of x_2, x_3, \dots, x_n . We introduce this expression in $g(x_1, x_2, \dots, x_n)$. Since $F_2(x_2) = 0$ we can express x_2^2 or higher powers as polynomials in x_3, \dots, x_n and the a_i . Since $F_3(x_3) = 0$ we can express x_3^3 and higher powers as polynomials of x_4, x_5, \dots, x_n and the a_i . Introducing these expressions in $g(x_1, x_2, \dots, x_n)$ we see that we can express it as a polynomial in the x_ν , and the a_ν , such that the degree in x_i is below i . So $g(x_1, x_2, \dots, x_n)$ is a linear combination of the following $n!$ terms:

$$x_1^{\nu_1} x_2^{\nu_2} \cdots x_n^{\nu_n} \quad \text{where each } \nu_i \leq i - 1. \quad (28)$$

The coefficients of these terms are polynomials in the a_i . Since the expressions (28) are linearly independent in \mathbb{S} (this is our previous result), the expression is unique.

This is a generalization of the *theorem of symmetric functions* in its usual form. The latter says that a symmetric polynomial can be written as a polynomial in a_1, a_2, \dots, a_n . Indeed, if $g(x_1, \dots, x_n)$ is symmetric we have already an expression as linear combination of the terms (28) where only the term 1 corresponding to $\nu_1 = \nu_2 = \dots = \nu_n = 0$ has a coefficient $\neq 0$ in \mathbb{S} , namely, $g(x_1, \dots, x_n)$. So $g(x_1, x_2, \dots, x_n)$ is a polynomial in a_1, a_2, \dots, a_n .

Hut, our theorem gives an expression of any polynomial, symmetric or not.

H. Normal Extensions

An extension field \mathbb{E} of a field \mathbb{F} is called a normal extension if the group G of automorphisms of \mathbb{E} which leave \mathbb{F} fixed has \mathbb{F} for its fixed field, and (\mathbb{E}/\mathbb{F}) is finite.

Although the result in Theorem 13 cannot be sharpened in general, there is one case in which the equality sign will always occur, namely, in the case in which $\sigma_1, \sigma_2, \dots, \sigma_n$ is a set of automorphisms which form a group. We prove

THEOREM 14. *If $\sigma_1, \sigma_2, \dots, \sigma_n$ is a group of automorphisms of a field \mathbb{E} and if \mathbb{F} is the fixed field of $\sigma_1, \sigma_2, \dots, \sigma_n$ then $(\mathbb{E}/\mathbb{F}) = n$.*

If $\sigma_1, \sigma_2, \dots, \sigma_n$ is a group, then the identity occurs, say, $\sigma_1 = 1$. The fixed field consists of those elements x which are not moved by any of the σ_i 's, i.e., $\sigma_i(x) = x$, $i = 1, 2, \dots, n$. Suppose that $(\mathbb{E}/\mathbb{F}) > n$. Then there exist $n + 1$ elements $a_1, a_2, \dots, a_n, a_{n+1}$ of \mathbb{E} which are linearly independent with respect to \mathbb{F} . By Theorem 1, there exists a non-trivial solution in \mathbb{E} to the system of equations

$$\begin{aligned} x_1\sigma_1(a_1) + x_2\sigma_1(a_2) + \dots + x_{n+1}\sigma_1(a_{n+1}) &= 0 \\ x_1\sigma_2(a_1) + x_2\sigma_2(a_2) + \dots + x_{n+1}\sigma_2(a_{n+1}) &= 0 \\ &\vdots \\ x_1\sigma_n(a_1) + x_2\sigma_n(a_2) + \dots + x_{n+1}\sigma_n(a_{n+1}) &= 0 \end{aligned} \tag{29}$$

We note that the solution cannot lie in \mathbb{F} , otherwise, since σ_1 is the identity, the first equation would be a dependence between $a_1, a_2, \dots, a_n, a_{n+1}$.

Among all non-trivial solutions $x_1, x_2, \dots, x_n, x_{n+1}$ we choose one which has the least number of elements different from 0. We may suppose this solution to be $a_1, a_2, \dots, a_r, 0, \dots, 0$, where the first r terms are different from 0. Moreover, $r \neq 1$ because $a_1\sigma_1(a_1) = 0$ implies $a_1 = 0$ since $\sigma_1(a_1) = a_1 \neq 0$. Also, we may suppose $a_r = 1$, since if we multiply the given solution by a_r^{-1} we obtain a new solution in which the r -th term is 1. Thus, we have

$$(*) \quad a_1\sigma_i(a_1) + a_2\sigma_i(a_2) + \dots + a_{r-1}\sigma_i(a_{r-1}) + \sigma_i(a_r) = 0$$

for $i = 1, 2, \dots, n$. Since a_1, \dots, a_{r-1} cannot all belong to \mathbb{F} , one of these, say a_1 , is in \mathbb{E} but not in \mathbb{F} . There is an automorphism σ_k for which $\sigma_k(a_1) \neq a_1$. If we use the fact that $\sigma_1, \sigma_2, \dots, \sigma_n$ form a group, we see $\sigma_k \cdot \sigma_1, \sigma_k \cdot \sigma_2, \dots, \sigma_k \cdot \sigma_n$ is a permutation of $\sigma_1, \sigma_2, \dots, \sigma_n$.

Applying σ_k to the expressions in (*) we obtain

$$\sigma_k(a_1) \cdot \sigma_k\sigma_j(a_1) + \dots + \sigma_k(a_{r-1}) \cdot \sigma_k\sigma_j(a_{r-1}) + \sigma_k\sigma_j(a_r) = 0$$

for $j = 1, 2, \dots, n$. So that from $\sigma_k\sigma_j = \sigma_i$ we have

$$(**) \quad \sigma_k(a_1) \cdot \sigma_i(a_1) + \dots + \sigma_k(a_{r-1}) \cdot \sigma_i(a_{r-1}) + \sigma_i(a_r) = 0$$

and if we subtract (**) from (*) we have

$$[a_1 - \sigma_k(a_1)] \cdot \sigma_i(a_1) + \dots + [a_{r-1} - \sigma_k(a_{r-1})] \sigma_i(a_{r-1}) = 0$$

which is a non-trivial solution to the system (refeq:27) having fewer than r elements different from 0, contrary to the choice of r .

Corollary 1. *If \mathbb{F} is the fixed field for the finite group G , then each automorphism σ that leaves \mathbb{F} fixed must belong to G .*

$(\mathbb{E}/\mathbb{F}) = \text{order of } G = n$. Assume there is a σ not in G . Then \mathbb{F} would remain fixed under the $n + 1$ elements consisting of σ and the elements of G , thus contradicting the corollary to Theorem 13. \square

Corollary 2. *There are no two finite groups G_1 and G_2 with the **same** fixed field.*

This follows immediately from Corollary 1. \square

If $f(x)$ is a polynomial in \mathbb{F} , then $f(x)$ is called separable if its irreducible factors do not have repeated roots. If \mathbb{E} is an extension of the field \mathbb{F} , the element a of \mathbb{E} is called separable if it is root of a separable polynomial $f(x)$ in \mathbb{F} , and \mathbb{E} is called a separable extension if each element of \mathbb{E} is separable.

THEOREM 15. \mathbb{E} is a normal extension of \mathbb{F} if and only if \mathbb{E} is the splitting field of a separable polynomial $p(x)$ in \mathbb{F} .

Sufficiency. Under the assumption that \mathbb{E} splits $p(x)$ we prove that \mathbb{E} is a normal extension of \mathbb{F} .

If all roots of $p(x)$ are in \mathbb{F} , then our proposition is trivial, since then $\mathbb{E} = \mathbb{F}$ and only the unit automorphism leaves \mathbb{F} fixed.

Let us suppose $p(x)$ has $n > 1$ roots in \mathbb{E} but not in \mathbb{F} . We make the inductive assumption that for all pairs of fields with fewer than n roots of $p(x)$ outside of \mathbb{F} our proposition holds.

Let $p(x) = p_1(x) \cdot p_2(x) \cdots p_r(x)$ be a factorization of $p(x)$ into irreducible factors. We may suppose one of these to have a degree greater than one, for otherwise $p(x)$ would split in \mathbb{F} . Suppose $\deg p_1(x) = s > 1$. Let a_1 be a root of $p_1(x)$. Then $(\mathbb{F}(a_1)/\mathbb{F}) = \deg p_1(x) = s$. If we consider $\mathbb{F}(a_1)$ as the new ground field, fewer roots of $p(x)$ than n are outside. From the fact that $p(x)$ lies in $\mathbb{F}(a_1)$ and \mathbb{E} is a splitting field of $p(x)$ over $\mathbb{F}(a_1)$, it follows by our inductive assumption that \mathbb{E} is a normal extension of $\mathbb{F}(a_1)$. Thus, each element in \mathbb{E} which is not in $\mathbb{F}(a_1)$ is moved by at least one automorphism which leaves $\mathbb{F}(a_1)$ fixed.

$p(x)$ being separable, the roots a_1, a_2, \dots, a_s of $p_1(x)$ are distinct elements of \mathbb{E} . By Theorem 8 there exist isomorphisms $\sigma_1, \sigma_2, \dots, \sigma_s$, mapping $\mathbb{F}(a_1)$ on $\mathbb{F}(a_1), \mathbb{F}(a_2), \dots, \mathbb{F}(a_s)$, respectively, which are each the identity on \mathbb{F} and map a_1 on a_1, a_2, \dots, a_s respectively. We now apply Theorem 10. \mathbb{E} is a splitting field of $p(x)$ in $\mathbb{F}(a_1)$ and is also a splitting field of $p(x)$ in $\mathbb{F}(a_i)$. Hence, the isomorphism σ_i , which makes $p(x)$ in $\mathbb{F}(a_1)$ correspond to the same $p(x)$ in $\mathbb{F}(a_i)$, can be extended to an isomorphic mapping of \mathbb{E} onto \mathbb{E} , that is, to an automorphism of \mathbb{E} that we denote again by σ_i . Hence, $\sigma_1, \sigma_2, \dots, \sigma_s$ are automorphisms of \mathbb{E} that leave \mathbb{F} fixed and map a_1 onto a_1, a_2, \dots, a_s .

Now let θ be an element that remains fixed under all automorphisms of \mathbb{E} that leave \mathbb{F} fixed. We know already that it is in $\mathbb{F}(a_1)$ and hence has the form

$$\theta = c_0 + c_1 a_1 + c_2 a_1^2 + \cdots + c_{s-1} a_1^{s-1}$$

where the c_i are in \mathbb{F} . If we apply σ_i to this equation we get, since $\sigma_i(\theta) = \theta$:

$$\theta = c_0 + c_1 a_i + c_2 a_i^2 + \cdots + c_{s-1} a_i^{s-1}$$

The polynomial $c_{s-1}x^{s-1} + c_{s-2}x^{s-2} + \cdots + c_1x + (c_0 - \theta)$ has therefore the s distinct roots a_1, a_2, \dots, a_s . These are more than its degree. So all coefficients of it must vanish, among them $(c_0 - \theta)$. This shows θ in \mathbb{F} .

Necessity. If \mathbb{E} is a normal extension of \mathbb{F} , then \mathbb{E} is splitting field of a separable polynomial $p(x)$. We first prove the

Lemma. *If \mathbb{E} is a normal extension of \mathbb{F} , then \mathbb{E} is a separable extension of \mathbb{F} . Moreover any element of \mathbb{E} is a root of an equation over \mathbb{F} which splits completely in \mathbb{E} .*

Proof. Let $\sigma_1, \sigma_2, \dots, \sigma_s$ be the group G of automorphisms of \mathbb{E} whose fixed field is \mathbb{F} . Let a be an element of \mathbb{E} , and let a_1, a_2, \dots, a_r be the set of distinct elements in the sequence $\sigma_1(a), \sigma_2(a), \dots, \sigma_s(a)$. Since G is a group,

$$\sigma_j(a_i) = \sigma_j(\sigma_k(a)) = \sigma_j\sigma_k(a) = \sigma_i(a) = a_i.$$

Therefore, the elements a_1, a_2, \dots, a_r are permuted by the automorphisms of G . The coefficients of the polynomial $f(x) = (x - a_1)(x - a_2) \cdots (x - a_r)$ are left fixed by each automorphism of G , since in its factored form the factors of $f(x)$ are only permuted. Since the only elements of \mathbb{E} which are left fixed by all the automorphisms of G belong to \mathbb{F} , $f(x)$ is a polynomial in \mathbb{F} . If $g(x)$ is a polynomial in \mathbb{F} which also has a as root, then applying the automorphisms of G to the expression $g(a) = 0$ we obtain $g(a_i) = 0$, so that the degree of $g(x) > s$. Hence $f(x)$ is irreducible, and the lemma is established. \square

To complete the proof of the theorem, let $\omega_1, \omega_2, \dots, \omega_t$ be a generating system for the vector space \mathcal{E} over \mathbb{F} . Let $f_i(x)$ be the separable polynomial having ω_i as a root. Then \mathbb{E} is the splitting field of $p(x) = f_1(x) \cdot f_2(x) \cdots f_t(x)$. \square

If $f(x)$ is a polynomial in a field \mathbb{F} , and \mathbb{E} the splitting field of $f(x)$, then we shall call the group of automorphisms of \mathbb{E} over \mathbb{F} the group of the equation $f(x) = 0$. We come now to a theorem known in algebra as the **Fundamental Theorem of Galois Theory** which gives the relation between the structure of a splitting field and its group of automorphisms.

THEOREM 16. (Fundamental Theorem). *If $p(x)$ is a separable polynomial in a field \mathbb{F} , and G the group of the equation $p(x) = 0$ where \mathbb{E} is the splitting field of $p(x)$, then:*

- (1) *Each intermediate field, \mathbb{B} , is the fixed field for a subgroup G_B , of G , and distinct subgroups have distinct fixed fields. We say \mathbb{B} and G , belong to each other.*
- (2) *The intermediate field \mathbb{B} is a normal extension of \mathbb{F} if and only if the subgroup G_B , is a normal subgroup of G . In this case the group of automorphisms of \mathbb{B} which leaves \mathbb{F} fixed is isomorphic to the factor group (G/G_B) .*
- (3) *For each intermediate field \mathbb{B} , we have $(\mathbb{B}/\mathbb{F}) = \text{index of } G_B$, and $(\mathbb{E}/\mathbb{B}) = \text{order of } G_B$.*

Proof. The first part of the theorem comes from the observation that \mathbb{E} is the splitting field for $p(x)$ when $p(x)$ is taken to be any intermediate field. Hence, \mathbb{E} is a normal extension of each intermediate field \mathbb{B} , so that \mathbb{B} is the fixed field of the subgroup of G consisting of the automorphisms which leave \mathbb{B} fixed. That distinct subgroups have distinct fixed fields is stated in Corollary 2 to Theorem 14.

Let \mathbb{B} be any intermediate field. Since \mathbb{B} is the fixed field for the subgroup G_B , of G , by Theorem 14 we have $(\mathbb{E}/\mathbb{B}) = \text{order of } G_B$. Let us call $o(G)$ the order of a group G and $i(G)$ its index. Then $o(G) = o(G_B) \cdot i(G_B)$. But $(\mathbb{E}/\mathbb{F}) = o(G)$, and $(\mathbb{E}/\mathbb{F}) = (\mathbb{E}/\mathbb{B}) \cdot (\mathbb{B}/\mathbb{F})$ from which $(\mathbb{B}/\mathbb{F}) = i(G_B)$, which proves the third part of the theorem.

The number $i(G_B)$ is equal to the number of left cosets of G_B . The elements of G_B being automorphisms of \mathbb{E} , are isomorphisms of \mathbb{B} ; that is, they map \mathbb{B} isomorphically into some other subfield of \mathbb{E} and are the identity on \mathbb{F} . The elements of G in any one coset of G_B map \mathbb{B} in the same way. For let

$\sigma\sigma_1$ and $\sigma\sigma_2$ be two elements of the coset σG_B . Since σ_1 and σ_2 leave \mathbb{B} fixed, for each a in \mathbb{B} we have $\sigma\sigma_1(a) = \sigma(a) = \sigma\sigma_2(a)$. Elements of different cosets give different isomorphisms, for if σ and τ give the same isomorphism, $\sigma(a) = \tau(a)$ for each a in \mathbb{B} , then $\sigma^{-1}\tau(a) = a$ for each a in \mathbb{B} . Hence, $\sigma^{-1}\tau = \sigma_1$ where σ_1 is an element of G_B . But then $\tau = \sigma\sigma_1$, and $\tau G_B = \sigma\sigma_1 G_B = \sigma G_B$, so that σ and τ belong to the same coset.

Each isomorphism of \mathbb{B} which is the identity on \mathbb{F} is given by an automorphism belonging to G . For let σ be an isomorphism mapping \mathbb{B} on \mathbb{B}' and the identity on \mathbb{F} . Then under σ , $p(x)$ corresponds to $p(x)$, and \mathbb{E} is the splitting field of $p(x)$ in \mathbb{B} and of $p(x)$ in \mathbb{B}' . By Theorem 10, σ can be extended to an automorphism σ' of \mathbb{E} , and since σ' leaves \mathbb{F} fixed it belongs to G . Therefore, the number of distinct isomorphisms of \mathbb{B} is equal to the number of cosets of G , and is therefore equal to (\mathbb{B}/\mathbb{F}) .

The field $\sigma\mathbb{B}$ onto which σ maps \mathbb{B} has obviously $\sigma G \sigma^{-1}$ as corresponding group, since the elements of $\sigma\mathbb{B}$ are left invariant by precisely this group.

If \mathbb{B} is a normal extension of \mathbb{F} , the number of distinct automorphisms of \mathbb{B} which leave \mathbb{F} fixed is (\mathbb{B}/\mathbb{F}) by Theorem 14. Conversely, if the number of automorphisms is (\mathbb{B}/\mathbb{F}) then \mathbb{B} is a normal extension, because if \mathbb{F}' is the fixed field of all these automorphisms, then $\mathbb{F} \subset \mathbb{F}' \subset \mathbb{B}$, and by Theorem 14, (\mathbb{B}/\mathbb{F}') is equal to the number of automorphisms in the group, hence $(\mathbb{B}/\mathbb{F}') = (\mathbb{B}/\mathbb{F})$. From $(\mathbb{B}/\mathbb{F}) = (\mathbb{B}/\mathbb{F}') \cdot (\mathbb{F}'/\mathbb{F})$ we have $(\mathbb{F}'/\mathbb{F}) = 1$ or $\mathbb{F} = \mathbb{F}'$. Thus, \mathbb{B} is a normal extension of \mathbb{F} if and only if the number of automorphisms of \mathbb{B} is (\mathbb{B}/\mathbb{F}) .

\mathbb{B} is a normal extension of \mathbb{F} if and only if each isomorphism of \mathbb{B} into \mathbb{E} is an automorphism of \mathbb{B} . This follows from the fact that each of the above conditions are equivalent to the assertion that there are the same number of isomorphisms and automorphisms. Since, for each σ , $\mathbb{B} = \sigma\mathbb{B}$ is equivalent to $\sigma G_B \sigma^{-1} \subset G_B$, we can finally say that \mathbb{B} is a normal extension of \mathbb{F} and only if G_B is a normal subgroup of G .

As we have shown, each isomorphism of \mathbb{B} is described by the effect of the elements of some left coset of G_B . If \mathbb{B} is a normal extension these isomorphisms are all automorphisms, but in this case the cosets are elements of the factor group (G/G_B) . Thus, each automorphism of \mathbb{B} corresponds uniquely to an element of (G/G_B) and conversely. Since multiplication in (G/G_B) is obtained by iterating the mappings, the correspondence is an isomorphism between (G/G_B) and the group of automorphisms of \mathbb{B} which leave \mathbb{F} fixed. This completes the proof of Theorem 16. \square

I. Finite Fields

It is frequently necessary to know the nature of a finite subset of a field which under multiplication in the field is a group. The answer to this question is particularly simple.

THEOREM 17. *If \mathbb{S} is a finite subset ($\neq 0$) of a field \mathbb{F} which is a group under multiplication in \mathbb{F} , then \mathbb{S} is a cyclic group.*

Proof: The proof is based on the following lemmas for abelian groups.

Lemma 1. *If in an abelian group A and B are two elements of orders a and b , and if c is the least*

common multiple of a and b , then there is an element C of order c in the group.

Proof: (a) If a and b are relatively prime, $C = AB$ has the required order ab . The order of $C^a = B^a$ is b and therefore c is divisible by b . Similarly it is divisible by a . Since $C^{ab} = 1$ it follows $c = ab$.

(b) If d is a divisor of a , we can find in the group an element of order d . Indeed $A^{\frac{a}{d}}$ is this element.

(c) Now let us consider the general case. Let p_1, p_2, \dots, p_r , be the prime numbers dividing either a or b and let

$$\begin{aligned} a &= p_1^{n_1} \cdot p_2^{n_2} \cdots p_r^{n_r}; \\ b &= p_1^{m_1} \cdot p_2^{m_2} \cdots p_r^{m_r}. \end{aligned}$$

Call t_i the larger of the two numbers n_i and m_i . Then

$$c = p_1^{t_1} \cdot p_2^{t_2} \cdots p_r^{t_r}.$$

According to (b) we can find in the group an element of order $p_i^{n_i}$ and one of order $p_i^{m_i}$. Thus there is one of order $p_i^{t_i}$. Part (a) shows that the product of these elements will have the desired order c .

Lemma 2: *If there is an element C in an abelian group whose order c is maximal (as is always the case if the group is finite) then c is divisible by the order a of every element A in the group; hence $x^c = 1$ is satisfied by **each** element x in the group.*

Proof: If a does not divide c , the greatest common multiple of a and c would be larger than c and we could find an element of that order, thus contradicting the choice of c . \square

We now prove Theorem 17. Let n be the order of \mathbb{S} and r the largest order occurring in \mathbb{S} . Then $x^r - 1 = 0$ is satisfied for all elements of \mathbb{S} . Since this polynomial of degree r in the field cannot have more than r roots, it follows that $r \geq n$. On the other hand $r \leq n$ because the order of each element divides n . \mathbb{S} is therefore a cyclic group consisting of $1, \epsilon, \epsilon^2, \dots, \epsilon^{n-1}$ where $\epsilon^n = 1$. \square

Theorem 17 could also have been based on the decomposition theorem for abelian groups having a finite number of generators. Since this theorem will be needed later, we interpolate a proof of it here.

Let G be an abelian group, with group operation written as $+$. The element g_1, \dots, g_k , will be said to generate G if each element g of G can be written as sum of multiples of g_1, \dots, g_k , $g = n_1 g_1 + \cdots + n_k g_k$. If no set of fewer than k elements generate G , then g_1, \dots, g_k will be called a minimal generating system. Any group having a finite generating system admits a minimal generating system. In particular, a finite group **always** admits a minimal generating system.

From the identity $n_1(g_1 + m g_2) + (n_2 - n_1 m)g_2 = n_1 g_1 + n_2 g_2$ it follows that if g_1, \dots, g_k generate G , also $g_1 + m g_2, g_2, \dots, g_k$, generate G .

An equation $m_1 g_1 + m_2 g_2 + \cdots + m_k g_k = 0$ will be called a relation between the generators, and m_1, \dots, m_k will be called the coefficients in the relation.

We shall say that the abelian group G is the direct product of its subgroups G_1, G_2, \dots, G_k if each $g \in G$ is uniquely representable as a sum $g = x_1 + x_2 + \cdots + x_k$ where $x_i \in G_i$, $i = 1, \dots, k$.

(Decomposition Theorem) Each abelian group having a finite number of generators is the direct product of cyclic subgroups G_1, G_2, \dots, G_n where the order of G_i divides the order of G_{i+1} , $i = 1, \dots, n-1$.

and n is the number of elements in a minimal generating system. (G_r, G_{r+1}, \dots, G_n may each be infinite, in which case, to be precise, $O(G_i) | O(G_{i+1})$ for $i = 1, 2, \dots, r-2$).

Proof: We assume the theorem true for all groups having minimal generating systems of $k-l$ elements. If $n = 1$ the group is cyclic and the theorem trivial. Now suppose G is an abelian group having a minimal generating system of k elements. If no minimal generating system satisfies a non-trivial relation, then let g_1, \dots, g_k be a minimal generating system and G_1, G_2, \dots, G_k be the cyclic groups generated by them. For each $g \in G$, $g = n_1 g_1 + \dots + n_k g_k$ where the expression is unique; otherwise we should obtain a relation. Thus the theorem would be true. Assume now that some non-trivial relations hold for some minimal generating systems. Among all relations between minimal generating systems, let

$$m_1 g_1 + \dots + m_k g_k = 0 \quad (30)$$

be a relation in which the smallest positive coefficient occurs. After an eventual reordering of the generators we can suppose this coefficient to be m_1 . In any other relation between g_1, \dots, g_k

$$n_1 g_1 + \dots + n_k g_k = 0 \quad (31)$$

we must have $m_1 | n_1$. Otherwise $n_1 = qm_1 + r$, $0 < r < m_1$ and q times relation (30) subtracted from relation (31) would yield a relation with a coefficient $r < m_1$. Also in relation (30) we must have $m_1 | m_i$, $i = 2, \dots, k$. For suppose m_i does not divide one coefficient, say m_2 . Then $m_2 = qm_1 + r$, $0 < r < m_1$. In the generating system $g_1 + g_2, g_2, \dots, g_k$ we should have a relation $m_1(g_1 + qg_2) + rg_2 + m_3 g_3 + \dots + m_k g_k = 0$ where the coefficient r contradicts the choice of m_1 . Hence $m_2 = q_2 m_1, m_3 = q_3 m_1, \dots, m_k = q_k m_1$.

The system $\bar{g} = g_1 + q_1 g_1 + \dots + q_k g_k, g_2, \dots, g_k$ is minimal generating, and $m_1 \bar{g}_1 = 0$. In any relation $0 = n_1 \bar{g}_1 + n_2 g_2 + \dots + n_k g_k$ since m_1 is a coefficient in a relation between $\bar{g}_1, g_2, \dots, g_k$ our previous argument yields $m_1 | n_1$, and hence $n_1 g_1 = 0$.

Let G' be the subgroup of G generated by g_2, \dots, g_k and G_1 the cyclic group of order m , generated by \bar{g}_1 . Then G is the direct product of G_1 and G' . Each element g of G can be written

$$g = n_1 \bar{g}_1 + n_2 g_2 + \dots + n_k g_k = n_1 \bar{g}_1 + g'$$

The representation is unique, since $n_1 \bar{g}_1 + g = n'_1 \bar{g}_1 + g''$ implies the relation $(n_1 - n'_1) \bar{g}_1 + (g' - g'') = 0$, hence $n_1 - n'_1 = 0$, so that $n_1 \bar{g}_1 = n'_1 \bar{g}_1$ and also $g' = g''$.

By our inductive hypothesis, G_1 is the direct product of $k-l$ cyclic groups generated by elements $\bar{g}_2, \bar{g}_3, \dots, \bar{g}_k$ whose respective orders t_2, \dots, t_k satisfy $t_i | t_{i+1}$, $i = 2, \dots, k-l$. The preceding argument applied to the generators $\bar{g}_1, \bar{g}_2, \dots, \bar{g}_k$ yields $m_1 | t_2$, from which the theorem follows. \square

By a finite field is meant one having only a finite number of elements.

Corollary. *The non-zero elements of a finite field form a cyclic group.* \square

If a is an element of a field \mathbb{F} , let us denote the n -fold of a , i.e., the element of \mathbb{F} obtained by adding a to itself n times, by na . It is obvious that $n \cdot (m \cdot a) = (nm) \cdot a$ and $(n \cdot a)(m \cdot b) = nm \cdot ab$. If for one element $a \neq 0$, there is an integer n such that $n \cdot a = 0$ then $n \cdot b = 0$ for each b in \mathbb{F} , since

$n \cdot b = (n \cdot a)(a^{-1} \cdot b) = 0 \cdot (a^{-1}b) = 0$. If there is a positive integer p such that $p \cdot a = 0$ for each a in \mathbb{F} , and if p is the smallest integer with this property, then \mathbb{F} is said to have the characteristic p . If no such positive integer exists then we say \mathbb{F} has characteristic 0. The characteristic of a field is **always a prime number**, for if $p = r \cdot s$ then $pa = r \cdot s \cdot a = r \cdot (s \cdot a)$. However, $s \cdot a = b \neq 0$ if $a \neq 0$ and $rb \neq 0$ since both r and s are less than p , so that $pa \neq 0$ contrary to the definition of the characteristic. If $na = 0$ for $a \neq 0$, then p divides n , for $n = qp + r$ where $0 < r < p$ and $na = (qp + r)a = qpa + ra$. Hence $na = 0$ implies $ra = 0$ and from the definition of the characteristic since $r < p$, we must have $r = 0$.

If \mathbb{F} is a finite field having q elements and \mathbb{E} an extension of \mathbb{F} such that $(\mathbb{E}/\mathbb{F}) = n$, then \mathbb{E} has q^n elements. For if $\omega_1, \dots, \omega_n$ is a basis of \mathcal{E} over \mathbb{F} , each element of E can be uniquely represented as a linear combination $x_1\omega_1 + x_2\omega_2 + \dots + x_n\omega_n$ where the x_i belong to \mathbb{F} . Since each x_i can assume q values in \mathbb{F} , there are q^n distinct possible choices of x_1, \dots, x_n and hence q^n distinct elements of \mathbb{E} . \mathbb{E} is finite, hence, there is an element a of \mathbb{E} so that $\mathbb{E} = \mathbb{F}(a)$. (The nonzero elements of \mathbb{E} form a cyclic group generated by a).

If we denote by $P \equiv [0, 1, 2, \dots, p-1]$ the set of multiples of the unit element in a field \mathbb{F} of characteristic p , then P is a subfield of \mathbb{F} having p distinct elements. In fact, P is isomorphic to the field of integers *reduced mod p* . If \mathbb{F} is a finite field, then the degree of \mathbb{F} over P is finite, say $(\mathbb{F}/P) = n$, and \mathbb{F} contains p^n elements. In other words, the order of any finite field is a power of its characteristic.

If \mathbb{F} and \mathbb{F}' are two finite fields having the same order q , then by the preceding, they have the same characteristic since q is a power of the characteristic. The multiples of the unit in \mathbb{F} and \mathbb{F}' form two fields \mathbb{P} and \mathbb{P}' which are isomorphic. The non-zero elements of \mathbb{F} and \mathbb{F}' form a group of order $q-1$ and, therefore, satisfy the equation $x^{q-1} - 1 = 0$. The fields \mathbb{F} and \mathbb{F}' are splitting fields of the equation $x^{q-1} = 1$ considered as lying in \mathbb{P} and \mathbb{P}' respectively. By Theorem 10, the isomorphism between \mathbb{P} and \mathbb{P}' can be extended to an isomorphism between \mathbb{F} and \mathbb{F}' . We have thus proved:

THEOREM 18. *Two finite fields having the same number of elements are **isomorphic**.*

□

Differentiation. If $f(x) = a_0 + a_1x + \dots + a_nx^n$ is a polynomial in a field \mathbb{F} , then we define $f' = a_1 + 2a_2x + \dots + na_nx^{n-1}$.

The reader may readily verify that for each pair of polynomials f and g we have

$$\begin{aligned} (f+g)' &= f' + g' \\ (fg)' &= fg' + gf' \\ (f^n)' &= nf^{n-1} \cdot f' \end{aligned}$$

THEOREM 19. *The polynomial f has repeated roots if and only if in the splitting field \mathbb{E} the polynomials f and f' have a common root. This condition is equivalent to the assertion that f and f' have a common factor of degree greater than 0 in \mathbb{F} .*

Proof: If a is a root of multiplicity k of $f(x)$ then $f = (x-a)^kQ(x)$ where $Q(a) \neq 0$. This gives

$$f' = (x-a)^kQ'(x) + k(x-a)^{k-1}Q(x) = (x-a)^{k-1}[(x-a)Q'(x) + kQ(x)]$$

. If $k > 1$, then a is a root of f' of multiplicity at least $k-1$. If $k = 1$, then $f'(x) = Q(x) + (x-a)Q'(x)$ and $f'(a) = Q(a) \neq 0$. Thus, f and f' have a root a in common if and only if a is a root of f of multiplicity greater than 1.

If f and f' have a root a in common then the irreducible polynomial in \mathbb{F} having a as root divides both f and f' . Conversely, any root of a factor common to both f and f' is a root of f and f' . \square

Corollary. *If \mathbb{F} is a field of characteristic 0 then each irreducible polynomial in \mathbb{F} is separable.*

Proof: Suppose to the contrary that the irreducible polynomial $f(x)$ has a root a of multiplicity greater than 1. Then, $f'(x)$ is a polynomial which is not identically zero (its leading coefficient is a multiple of the leading coefficient of $f(x)$ and is not zero since the characteristic is 0) and of degree 1 less than the degree of $f(x)$. But a is also a root of $f'(x)$ which contradicts the irreducibility of $f(x)$. \square

J. Roots of Unity

If \mathbb{F} is a field having any characteristic p , and \mathbb{E} the splitting field of the polynomial $x^n - 1$ where p does not divide n , then we shall refer to \mathbb{E} as the field generated out of \mathbb{F} by the adjunction of a primitive n -th root of unity.

The polynomial $x^n - 1$ does not have repeated roots in \mathbb{E} , since its derivative, nx^{n-1} , has only the root 0 and has, therefore, no roots in common with $x^n - 1$. Thus, \mathbb{E} is a normal extension of \mathbb{F} .

If $\epsilon_1, \epsilon_2, \dots, \epsilon_n$ are the roots of $x^n - 1$ in \mathbb{E} , they form a group under multiplication and by Theorem 17 this group will be cyclic.

If $1, \epsilon, \epsilon^2, \dots, \epsilon^{n-1}$ are the elements of the group, we shall call ϵ a primitive n -th root of unity. The smallest power of \mathbb{E} which is 1 is the n^{boxth} .

THEOREM 20. *If \mathbb{E} is the field generated from \mathbb{F} by a primitive n -th root of unity, then the group G of \mathbb{E} over \mathbb{F} is abelian for any n and cyclic if n is a prime number.*

\square

Proof: We have $\mathbb{E} = \mathbb{F}(\epsilon)$, since the roots of $x^n - 1$ are powers of ϵ . Thus, if σ and τ are distinct elements of G , $\sigma(\epsilon) \neq \tau(\epsilon)$. But $\sigma(\epsilon)$ is a root of $x^n - 1$ and, hence, a power of ϵ . Thus, $\sigma(\epsilon) = \epsilon^{n_\sigma}$ where n_σ is an integer $1 \leq n_\sigma < n$. Moreover, $\tau\sigma(\epsilon) = \tau(\epsilon^{n_\sigma}) = (\tau(\epsilon))^{n_\sigma} = \epsilon^{n_\tau n_\sigma} = \sigma\tau(\epsilon)$. Thus, $n_{\sigma\tau} = n_\sigma n_\tau \bmod n$. Thus, the mapping of σ on n_σ is a homomorphism of G into a multiplicative subgroup of the integers $\bmod n$. Since $\tau \neq \sigma$ implies $\tau(\epsilon) \neq \sigma(\epsilon)$, it follows that $\tau \neq \sigma$ implies $n_\sigma \neq n_\tau \bmod n$. Hence, the homomorphism is an isomorphism. If n is a **prime number**, the multiplicative group of numbers forms a cyclic group. \square

K. Noether Equations

If \mathbb{E} is a field, and $G = (\sigma, \tau, \dots)$ a group of automorphisms of \mathbb{E} , any set of elements x_σ, x_τ, \dots in \mathbb{E} will be said to provide a solution to Noether equations if $x_\sigma \cdot \sigma(x_\tau) = x_{\sigma\tau}$ for each σ and τ in G . If one element $x_\sigma = 0$ then $x_\tau = 0$ for each $\tau \in G$. As τ *traces* G , $\sigma\tau$ assumes all values in G , and in the

above equation $x_{\sigma\tau} = 0$ when $x_\sigma = 0$. Thus, in any solution of the Noether equations no element $n_\sigma = 0$ unless the solution is completely trivial. We shall assume in the sequel that the trivial solution has been excluded.

THEOREM 21. *The system x_σ, x_τ, \dots is a solution to Noether's equations if and only if there exists an element a in \mathbb{E} , such that $x_\sigma = \frac{a}{\sigma(a)}$ for each σ .*

Proof: For any a , it is clear that $x_\sigma = \frac{a}{\sigma(a)}$ is a solution to the equations, since

$$\frac{a}{\sigma(a)} \cdot \sigma\left(\frac{a}{\tau(a)}\right) = \frac{a}{\sigma(a)} \cdot \frac{\sigma(a)}{\sigma\tau(a)} = \frac{a}{\sigma\tau(a)}.$$

Conversely, let x_σ, x_τ, \dots be a non-trivial solution. Since the automorphisms σ, τ, \dots are distinct they are linearly independent, and the equation $x_\sigma\sigma(z) + x_\tau\tau(z) + \dots = 0$ does not hold identically. Hence, there is an element a in \mathbb{E} such that $x_\sigma\sigma(a) + x_\tau\tau(a) + \dots = a \neq 0$. Applying σ to a gives

$$\sigma(a) = \sum_{\tau \in G} \sigma(x_\tau) \cdot \sigma\tau(a).$$

Multiplying by x_σ gives

$$x_\sigma\sigma(a) = \sum_{\tau \in G} x_\sigma\sigma(x_\tau) \cdot \sigma\tau(a).$$

Replacing $x_\sigma\sigma(x_\tau)$ by $x_{\sigma\tau}$ and noting that $\sigma\tau$ assumes all values in G when τ does, we have

$$x_\sigma\sigma(a) = \sum_{\tau \in G} x_{\sigma\tau}(a)$$

so that

$$x_\sigma = a/\sigma(a).$$

□

A solution to the Noether equations defines a mapping \mathcal{C} of G into \mathbb{E} , namely, $\mathcal{C}(a) = x_\sigma$. If \mathbb{F} is the fixed field of G , and the elements x_σ lie in \mathbb{F} , then \mathcal{C} is a character of G . For

$$\mathcal{C}(\sigma\tau) = x_{\sigma\tau} = x_\sigma \cdot \sigma(x_\tau) = x_\sigma x_\tau = \mathcal{C}(\sigma) \cdot \mathcal{C}(\tau)$$

since $\sigma(x_\tau) = x_\tau$, if $x_\tau \in \mathbb{F}$. Conversely, each character \mathcal{C} of G in \mathbb{F} provides a solution to the Noether equations. Call $\mathcal{C}(\sigma) = x_\sigma$. Then, since $x_\sigma \in \mathbb{F}$, we have $\sigma(x_\tau) = x_\tau$. Thus,

$$x_\sigma \cdot \sigma(x_\tau) = x_\sigma x_\tau = \mathcal{C}(\sigma) \cdot \mathcal{C}(\tau) = \mathcal{C}(\sigma\tau) = x_{\sigma\tau}.$$

We therefore have, by combining this with Theorem 21,

THEOREM 22. *If G is the group of the normal field \mathbb{E} over \mathbb{F} , then for each character \mathcal{C} of G into \mathbb{F} there exists an element a in \mathbb{E} such that $\mathcal{C}(a) = a/\sigma(a)$ and, conversely, if $a/\sigma(a)$ is in \mathbb{F} for each σ , then $\mathcal{C}(a) = a/\sigma(a)$ is a character of G . If r is the least common multiple of the orders of elements of G , then $a^r \in \mathbb{F}$.*

We have already shown all but the last sentence of Theorem 22.

To prove this we need only show $\sigma(a^r) = a^r$ for each $\sigma \in G$. But

$$a^r / \sigma(a^r) = (a / \sigma(a))^r = (\mathcal{C}(\sigma))^r = \mathcal{C}(\sigma^r) = \mathcal{C}(1) = 1.$$

□

L. Kummer Fields

If \mathbb{F} contains a primitive n -th root of unity, any splitting field \mathbb{E} of a polynomial $(x^n - a_1)(x^n - a_2) \cdots (x^n - a_r)$ where $a_i \in \mathbb{F}$ for $i = 1, 2, \dots, r$ will be called a Kummer extension of \mathbb{F} , or more briefly, a Kummer field.

If a field \mathbb{F} contains a primitive n -th root of unity, the number n is not divisible by the characteristic of \mathbb{F} . Suppose, to the contrary, \mathbb{F} has characteristic p and $n = qp$. Then $y^p - 1 = (y - 1)^p$ since in the expansion of $(y - 1)^p$ each coefficient other than the first and last is divisible by p and therefore is a multiple of the p -fold of the unit of \mathbb{F} and thus is equal to 0. Therefore $x^n - 1 = (x^q)^p - 1 = (x^q - 1)^n$ and $x^n - 1$ cannot have more than q distinct roots. But we assumed that \mathbb{F} has a primitive n -th root of unity and $1, \epsilon, \epsilon^2, \dots, \epsilon^{n-1}$ would be n distinct roots of $x^n - 1$. It follows that n is not divisible by the characteristic of \mathbb{F} . For a Kummer field \mathbb{E} , none of the factors $x^n - a_i, a_i \neq 0$ has repeated roots since the derivative, nx^{n-1} , has only the root 0 and has therefore no roots in common with $x^n - a_i$. Therefore, the irreducible factors of $x^n - a_i$, are separable, so that \mathbb{E} is a normal extension of \mathbb{F} .

Let a_i be a root of $x^n - a_i$ in \mathbb{E} . If $\epsilon_1, \epsilon_2, \dots, \epsilon_n$ are the n distinct n -th roots of unity in \mathbb{F} , then $a_i\epsilon_1, a_i\epsilon_2, \dots, a_i\epsilon_n$ will be n distinct roots of $x^n - a_i$, and hence will be the roots of $x^n - a_i$, so that $\mathbb{E} = \mathbb{F}(a_1, a_2, \dots, a_r)$. Let σ and τ be two automorphisms in the group G of \mathbb{E} over \mathbb{F} . For each a_i , both σ and τ map a_i on some other root of $x^n - a_i$. Thus $\tau(a_i) = \epsilon_{i\tau}(a_i)$ and $\sigma(a_i) = \epsilon_{i\sigma}(a_i)$ where $\epsilon_{i\tau}$, and $\epsilon_{i\sigma}$ are n -th roots of unity in the basic field \mathbb{F} . It follows that

$$\tau(\sigma(a_i)) = \tau(\epsilon_{i\sigma}(a_i)) = \epsilon_{i\sigma}(\tau(a_i)) = \epsilon_{i\tau}\epsilon_{i\sigma}(a_i) = \sigma(\tau(a_i))$$

Since σ and τ are commutative over the generators of \mathbb{E} , they commute over each element of \mathbb{E} . Hence, G is commutative. If $\sigma \in G$, then $\sigma(a_i) = \epsilon_{i\sigma}(a_i)$, $\sigma^2(a_i) = \epsilon_{i\sigma}^2(a_i)$, etc. Thus, $\sigma^{n_i}(a_i) = a_i$ for n_i such that $\epsilon_{i\sigma}^{n_i} = 1$. Since the order of an n -th root of unity is a divisor of n , we have n_i a divisor of n and the least common multiple m of n_1, n_2, \dots, n_r is a divisor of n . Since $\sigma^m(a_i) = a_i$ for $i = 1, 2, \dots, r$ it follows that m is the order of σ . Hence, the order of each element of G is a divisor of n and, therefore, the least common multiple r of the orders of the elements of G is a divisor of n . If ϵ is a primitive n -th root of unity, then $\epsilon^{n/r}$ is a primitive r -th root of unity. These remarks can be summarized in the following.

THEOREM 23. *If E is a Kummer field, i.e., a splitting field of $p(x) = (x^n - a_1)(x^n - a_2) \cdots (x^n - a_r)$ where a_i lie in \mathbb{F} , and \mathbb{F} contains a primitive n -th root of unity, then:*

- (a) \mathbb{E} is a normal extension of \mathbb{F} ;
- (b) the group G of \mathbb{E} over \mathbb{F} is abelian,
- (c) the least common multiple of the orders of the elements of G is a divisor of n .

□

Corollary. *If \mathbb{E} is the splitting field of $x^p - a$, and \mathbb{F} contains a primitive p -th root of unity where p is a prime number, then either $\mathbb{E} = \mathbb{F}$ and $x^p - a$ is split in \mathbb{F} , or $x^p - a$ is irreducible and the group of \mathbb{E} over \mathbb{F} is cyclic of order p .*

Proof: The order of each element of G is, by Theorem 23, a divisor of p and, hence, if the element is not the unit its order must be p . If ϵ is a root of $x^p - a$, then $a, \epsilon a, \dots, \epsilon^{p-1}a$ are all the roots of $x^p - a$ so that $\mathbb{F}(a) = \mathbb{E}$ and $(\mathbb{E}/\mathbb{F}) \leq p$. Hence, the order of G does not exceed p so that if G has one element different from the unit, it and its powers must constitute all of G . Since G has p distinct elements and their behavior is determined by their effect on a , then a must have p distinct images. Hence, the irreducible equation in \mathbb{F} for a must be of degree p and is therefore $x^p - a = 0$. □

The properties (a), (b) and (c) in Theorem 23 actually **characterize** Kummer fields.

Let us suppose that \mathbb{E} is a normal extension of a field \mathbb{F} , whose group G over \mathbb{F} is abelian. Let us further assume that \mathbb{F} contains a primitive r -th root of unity where r is the least common multiple of the orders of elements of G . The group of characters X of G into the group of r -th roots of unity is isomorphic to G . Moreover, to each $\sigma \in G$, if $\sigma \neq 1$, there exists a character $\mathcal{C} \in X$ such that $\mathcal{C}(\sigma) \neq 1$. Write G as the direct product of the cyclic groups G_1, G_2, \dots, G_t of orders m_1, m_2, \dots, m_t . Each $\sigma \in G$ may be written $\sigma = \sigma_1^{\nu_1} \sigma_2^{\nu_2} \dots \sigma_t^{\nu_t}$. Call \mathcal{C}_i the character sending σ_i into ϵ_i , a primitive m_i -th root of unity and σ_j into 1 for $j \neq i$. Let \mathcal{C} be any character. $\mathcal{C}(\sigma_i) = \sigma_i^{\mu_i}$ then we have $\mathcal{C} = \mathcal{C}_1^{\mu_1} \cdot \mathcal{C}_2^{\mu_2} \dots \mathcal{C}_t^{\mu_t}$. Conversely, $\mathcal{C} = \mathcal{C}_1^{\mu_1} \cdot \mathcal{C}_2^{\mu_2} \dots \mathcal{C}_t^{\mu_t}$ defines a character. Since the order of \mathcal{C}_i is m_i , the character group X of G is isomorphic to G . If $\sigma \neq 1$, then in $\sigma = \sigma_1^{\nu_1} \sigma_2^{\nu_2} \dots \sigma_t^{\nu_t}$ at least one ν_i , say ν_1 , is not divisible by m_i . Thus $\mathcal{C}_1(\sigma) = \epsilon_1^{\nu_1} \neq 1$.

Let A denote the set of those non-zero elements a of \mathbb{E} for which $a \in \mathbb{F}$ and let F_1 denote the non-zero elements of \mathbb{F} . It is obvious that A is a multiplicative group and that F_1 is a subgroup of A . Let A^r denote the set of r -th powers of elements in A and F_1^r the set of r -th powers of elements of F_1 . The following theorem provides in most applications a convenient method for computing the group G .

THEOREM 24. *The factor groups (A/F_1) and (A^r/F_1^r) are isomorphic to each other and to the groups G and X .*

Proof: We map A on A^r by making $a \in A$ correspond to $a^r \in A^r$. If $a^r \in F_1^r$, where $a \in F_1$, then $b \in A$ is mapped on a^r if and only if $b^r = a^r$, that is, if b is a solution to the equation $x^r - a^r = 0$. But $a, \epsilon a, \epsilon^2 a, \dots, \epsilon^{r-1}a$ are distinct solutions to this equation and since ϵ and a belong to F_1 , it follows that b must be one of these elements and must belong to F_1 . Thus, the inverse set in A of the subgroup F_1 of A^r is F_1^r , so that the factor groups (A/F_1) and (A^r/F_1^r) are isomorphic.

If a is an element of A , then $(a/\sigma(a))^r = a^r/\sigma(a^r) = 1$. Hence, $a/\sigma(a)$ is an r -th root of unity and lies in F_1 . By Theorem 22, $a/\sigma(a)$ defines a character $\mathcal{C}(\sigma)$ of G in \mathbb{F} . We map a on the corresponding character \mathcal{C} . Each character \mathcal{C} is by Theorem 22, image of some a' . Moreover, $a \cdot a'$ is mapped on the character

$$\mathcal{C}^*(\sigma) = a \cdot a/\sigma(a \cdot a) = a \cdot a/\sigma(a) \cdot \sigma(a') = \mathcal{C}(\sigma)\mathcal{C}'(\sigma) = \mathcal{C}\mathcal{C}'(\sigma),$$

so that the mapping is homomorphism. The kernel of this homomorphism is the set of those elements a

for which $a/\sigma(a) = 1$ for each σ , hence is F_1 . It follows, therefore, that (A/F) is isomorphic to X and hence also to G . In particular, (A/F_1) is a **finite** group. \square

We now prove the equivalence between Kummer fields and fields satisfying (a), (b) and (c) of Theorem 23.

THEOREM 25. *If \mathbb{E} is an extension field over \mathbb{F} , then \mathbb{E} is a Kummer field **if and only if** \mathbb{E} is **normal**, its group G is **abelian** and \mathbb{F} contains a primitive r -th root σ of unity where r is the **least common multiple** of the orders of the elements of G .*

Proof: The necessity is already contained in Theorem 23. We prove the sufficiency. Out of the group A , let $\alpha_1 F_1, \alpha_2 F_1, \dots, \alpha_t F_1$ be the cosets of F_1 . Since $\alpha_i \in A$, we have $a_i^r = \alpha_i \in \mathbb{F}$. Thus, α_i is a root of the equation $x^r - a_i = 0$ and since $\epsilon \alpha_i, \epsilon^2 \alpha_i, \dots, \epsilon^{r-1} \alpha_i$ are also roots, $x^r - a_i$ must split in \mathbb{E} . We prove that \mathbb{E} is the splitting field of $(x^r - a_1)(x^r - a_2) \cdots (x^r - a_t)$ which will complete the proof of the theorem. To this end it suffices to show that $\mathbb{F}(a_1, a_2, \dots, a_t) = \mathbb{E}$.

Suppose that $\mathbb{F}(a_1, a_2, \dots, a_t) \neq \mathbb{E}$. Then $\mathbb{F}(a_1, a_2, \dots, a_t)$ is an intermediate field between \mathbb{F} and \mathbb{E} , and since \mathbb{E} is normal over $\mathbb{F}(a_1, \dots, a_t)$ there exists an automorphism $\sigma \in G$, $\sigma \neq 1$, which leaves $\mathbb{F}(a_1, \dots, a_t)$ fixed. There exists a character \mathcal{C} of G for which $\mathcal{C}(a) \neq 1$. Finally, there exists an element α in \mathbb{E} such that $\mathcal{C}(\sigma) = \alpha/\sigma(\alpha) \neq 1$. But $\alpha^r \in F_1$ by Theorem 22, hence $\alpha \in A$. Moreover, $A \subset \mathbb{F}(a_1, \dots, a_t)$ since all the cosets $\alpha_i F_1$ are **contained** in $\mathbb{F}(a_1, \dots, a_t)$. Since $\mathbb{F}(a_1, \dots, a_t)$ is by assumption **left fixed** by σ , $\sigma(a) = a$ which contradicts $a/\sigma(a) \neq 1$. It follows, therefore, that $\mathbb{F}(a_1, \dots, a_t) = \mathbb{E}$. \square

Corollary. *If \mathbb{E} is a normal extension of \mathbb{F} , of prime order p , and if \mathbb{F} contains a primitive p -th root of unity, then \mathbb{E} is splitting field of an irreducible polynomial $x^p - a \in \mathbb{F}$.*

Proof: \mathbb{E} is generated by elements $\alpha_1, \dots, \alpha_n$, where $\alpha_i \in \mathbb{F}$. Let a_1 be not in \mathbb{F} . Then $x^p - a$ is irreducible, for otherwise $\mathbb{F}(a_1)$ would be an intermediate field between \mathbb{F} and \mathbb{E} of degree less than p , and by the product theorem for the degrees, p would not be a prime number, contrary to assumption. $\mathbb{E} = \mathbb{F}(a_1)$ is the splitting field of $x^p - a$. \square

M. Simple Extensions

We consider the question of determining under what conditions an extension field is generated by a single element, called a primitive. We prove the following

THEOREM 26. *A finite extension \mathbb{E} of \mathbb{F} is **primitive** over \mathbb{F} if and only if there are only a **finite number** of intermediate fields.*

Proof: (a) Let $\mathbb{E} = \mathbb{F}(a)$ and call $f(x) = 0$ the irreducible equation for a in \mathbb{F} . Let \mathbb{B} be an intermediate field and $g(x)$ the irreducible equation for a in \mathbb{B} . The coefficients of $g(x)$ adjoined to \mathbb{F} will generate a field \mathbb{B}' between \mathbb{F} and \mathbb{B} . $g(x)$ is irreducible in \mathbb{B} , hence also in \mathbb{B}' . Since $\mathbb{E} = \mathbb{B}'(a)$ we see $(\mathbb{E}/\mathbb{B}) = (\mathbb{E}/\mathbb{B}')$. This proves $\mathbb{B}' = \mathbb{B}$. So \mathbb{B} is uniquely determined by the polynomial $g(x)$. But $g(x)$ is a divisor of $f(x)$, and there are only a finite number of possible divisors of $f(x)$ in \mathbb{E} . Hence there are only a finite number of possible \mathbb{B} 's.

(b) Assume there are only a finite number of fields between \mathbb{E} and \mathbb{F} . Should \mathbb{F} consist only of a finite number of elements, then \mathbb{E} is generated by one element according to the Corollary on page (53). We may therefore assume \mathbb{F} to contain an infinity of elements. We prove: to any two elements α, β there is a γ in \mathbb{E} such that $\mathbb{F}(\alpha, \beta) = \mathbb{F}(\gamma)$. Let $\gamma = \alpha + a\beta$ with a in \mathbb{F} but for the moment undetermined. Consider all the fields $\mathbb{F}(\gamma)$ obtained in this way. Since we have an infinity of a 's at our disposal, we can find two, say a_1 and a_2 , such that the corresponding γ 's, $\gamma_1 = \alpha + a_1\beta$ and $\gamma_2 = \alpha + a_2\beta$, yield the same field $\mathbb{F}(\gamma_1) = \mathbb{F}(\gamma_2)$. Since both γ_1 and γ_2 are in $\mathbb{F}(\gamma_1)$, their difference (and therefore β) is in this field. Consequently also $\gamma_1 - a_1\beta = \alpha$. So $\mathbb{F}(\alpha, \beta) \subset \mathbb{F}(\gamma_1)$. Since $\mathbb{F}(\gamma_1) \subset \mathbb{F}(\alpha, \beta)$ our contention is proved. Select now η in \mathbb{E} in such a way that $(\mathbb{F}(\eta)/\mathbb{F})$ is as large as possible. Every element ϵ of \mathbb{E} must be in $\mathbb{F}(\eta)$ or else we could find an element δ such that $\mathbb{F}(\delta)$ contains both η and β . This proves $\mathbb{E} = \mathbb{F}(\eta)$. \square

THEOREM 27. *If $\mathbb{E} = \mathbb{F}(a_1, a_2, \dots, a_n)$ is a finite extension of the field \mathbb{F} , and a_1, a_2, \dots, a_n are separable elements in \mathbb{E} , then there exists a primitive θ in \mathbb{E} such that $\mathbb{E} = \mathbb{F}(\theta)$.*

Proof: Let $f_i(x)$ be the irreducible equation of a_i in \mathbb{F} and let \mathbb{B} be an extension of \mathbb{E} that splits $f_1(x), f_2(x), \dots, f_n(x)$. Then \mathbb{B} is normal over \mathbb{F} and contains, therefore, only a finite number of intermediate fields (as many as there are subgroups of G). So the subfield \mathbb{E} contains only a finite number of intermediate fields. Theorem 26 now completes the proof. \square

N. Existence of a Normal Basis

The following theorem is true for any field though we prove it only in the case that \mathbb{F} contains an infinity of elements.

THEOREM 28. *If \mathbb{E} is a normal extension of \mathbb{F} and $\sigma_1, \sigma_2, \dots, \sigma_n$ are the elements of its group G , there is an element θ in \mathbb{E} such that the n elements $\sigma_1(\theta), \sigma_2(\theta), \dots, \sigma_n(\theta)$ are linearly independent with respect to \mathbb{F} .*

Proof: According to Theorem 27 there is an a such that $\mathbb{E} = \mathbb{F}(a)$. Let $f(x)$ be the equation for a , put $\sigma(a) = \alpha_i$, $g(x) = \frac{f(x)}{(x - \alpha_i)f'(\alpha_i)}$ and $g_i(x) = \sigma_i(g(x)) = \frac{f(x)}{(x - \alpha_i)(f'(\alpha_i))}$. $g_i(x)$ is a polynomial in \mathbb{E} having α_k as root for $k \neq i$ and hence

$$(1) \quad g_i(x)g_k(x) = 0 \pmod{f(x)} \text{ for } i \neq k.$$

In the equation

$$(2) \quad g_1(x) + g_2(x) + \dots + g_n(x) - 1 = 0$$

the left side is of degree at most $n - 1$. If (2) is true for n different values of x , the left side must be identically 0. Such n values are $\alpha_1, \alpha_2, \dots, \alpha_n$, since $g_i(\alpha_i) = 1$ and $g_k(\alpha_i) = 0$ for $k \neq i$. Multiplying (2) by $g_i(x)$ and using (1) shows:

$$(3) \quad (g_i(x))^2 = g_i(x) \pmod{f(x)}.$$

We next compute the determinant

$$(4) \quad D(x) = |\sigma_i \sigma_k(g(x))| \quad i, k = 1, 2, \dots, n$$

and prove $D(x) \neq 0$. If we square it by multiplying column by column and compute its value $(\text{mod } f(x))$ we get from (1), (2), (3) a determinant that has 1 in the diagonal and 0 elsewhere.

So

$$(D(x))^2 = 1 \pmod{f(x)}.$$

$D(x)$ can have only a finite number of roots in \mathbb{F} . Avoiding them we can find a value a for x such that $D(a) \neq 0$. Now set $\theta = g(a)$. Then the determinant

$$(5) \quad |\sigma_i \sigma_k(\theta)| \neq 0.$$

Consider any linear relation $x_1 \sigma_1(\theta) + x_2 \sigma_2(\theta) + \cdots + x_n \sigma_n(\theta) = 0$ where the x_i are in \mathbb{F} . Applying the automorphism σ_i to it would lead to n homogeneous equations for the n unknowns x_i . (5) shows that $x_i = 0$ and our theorem is proved. \square

O. Theorem on Natural Irrationalities

Let \mathbb{F} be a field, $p(x)$ a polynomial in \mathbb{F} whose irreducible factors are separable, and let \mathbb{E} be a splitting field for $p(x)$. Let \mathbb{B} be an arbitrary extension of \mathbb{F} , and let us denote by $\mathbb{E}\mathbb{B}$ the splitting field of $p(x)$ when $p(x)$ is taken to lie in \mathbb{B} . If a_1, \dots, a_s are the roots of $p(x)$ in $\mathbb{E}\mathbb{B}$, then $\mathbb{F}(a_1, \dots, a_s)$ is a subfield of $\mathbb{E}\mathbb{B}$ which is readily seen to form a splitting field for $p(x)$ in \mathbb{F} . By Theorem 10, \mathbb{E} and $\mathbb{F}(a_1, \dots, a_s)$ are isomorphic. There is therefore no loss of generality if in the sequel we take $\mathbb{E} = \mathbb{F}(a_1, \dots, a_s)$ and assume therefore that \mathbb{E} is a subfield of $\mathbb{E}\mathbb{B}$. Also, $\mathbb{E}\mathbb{B} = \mathbb{B}(a_1, \dots, a_s)$.

Let us denote by $\mathbb{E} \cap \mathbb{B}$ the intersection of \mathbb{E} and \mathbb{B} . It is readily seen that $\mathbb{E} \cap \mathbb{B}$ is a field and is intermediate to \mathbb{F} and \mathbb{E} .

THEOREM 29. *If G is the group of automorphisms of \mathbb{E} over \mathbb{F} , and H the group of $\mathbb{E}\mathbb{B}$ over \mathbb{B} , then H is isomorphic to the subgroup of G having $\mathbb{E} \cap \mathbb{B}$ as its fixed field.*

Proof: Each automorphism of $\mathbb{E}\mathbb{B}$ over \mathbb{B} simply permutes a_1, \dots, a_s in some fashion and leaves \mathbb{B} , and hence also \mathbb{F} , fixed. Since the elements of $\mathbb{E}\mathbb{B}$ are quotients of polynomial expressions a_1, \dots, a_s with coefficients in \mathbb{B} , the automorphism is completely determined by the permutation it effects on a_1, \dots, a_s . Thus, each automorphism of $\mathbb{E}\mathbb{B}$ over \mathbb{B} defines an automorphism of $\mathbb{E} = \mathbb{F}(a_1, \dots, a_s)$ which leaves \mathbb{F} fixed. Distinct automorphisms, since (a_1, \dots, a_s) belong to \mathbb{E} , have different effects on \mathbb{E} . Thus, the group H of $\mathbb{E}\mathbb{B}$ over \mathbb{B} can be considered as a subgroup of the group G of \mathbb{E} over \mathbb{F} . Each element of H leaves $\mathbb{E} \cap \mathbb{B}$ fixed since it leaves even all of \mathbb{B} fixed. However, any element of \mathbb{E} which is not in $\mathbb{E} \cap \mathbb{B}$ is not in \mathbb{B} , and hence would be moved by at least one automorphism of H . It follows that $\mathbb{E} \cap \mathbb{B}$ is the fixed field of H . \square

Corollary: *If, under the conditions of Theorem 29, the group G is of prime order, then either $H = G$ or H consists of the unit element alone.*

3 APPLICATIONS *By A. N. Milgram*

A. Solvable Groups

Before proceeding with the applications we must discuss certain questions in the theory of groups. We shall assume several simple propositions: (a) If N is a normal subgroup of the group G , then the mapping $f(x) = xN$ is a homomorphism of G on the factor group G/N . f is called the **natural homomorphism**. (b) The image and the inverse image of a normal subgroup under a homomorphism is a normal subgroup. (c) If f is a homomorphism of the group G on G' , then setting $N' = f(N)$, and defining the mapping g as $g(xN) = f(x)N'$, we readily see that g is a homomorphism of the factor group G/N on the factor group G'/N' . Indeed, if N is the inverse image of N' then g is an isomorphism. We now prove

THEOREM 30. (*Zassenhaus*). *If U and V are subgroups of G , u and v normal subgroups of U and V , respectively, then the following three factor groups are isomorphic: $u(U \cap V)/u(U \cap v)$, $v(U \cap V)/V(U \cap V)$, $(u \cap v)/(u \cap v)(v \cap u)$.*

Proof: It is obvious that $U \cap v$ is a normal subgroup of $U \cap V$. Let f be the natural mapping of U on V/u . Call $f(U \cap V) = H$ and $f(U \cap v) = K$. Then $f^{-1}(H) = u(U \cap V)$ and $f^{-1}(K) = u(U \cap v)$ from which it follows that $u(U \cap V)/u(U \cap v)$ is isomorphic to H/K . If, however, we view f as defined only over $U \cap V$, then $f^{-1}(K) = [u \cap (U \cap V)](U \cap v) = (u \cap V)(U \cap v)$ so that $(U \cap V)/(u \cap V)(U \cap v)$ is also isomorphic to H/K . Thus the first and third of the above factor groups are isomorphic to each other. Similarly, the second and third factor groups are isomorphic. \square

Corollary 1. *If H is a subgroup and N a normal subgroup of the group G , then $H/H \cap N$ is isomorphic to HN/N , a subgroup of G/N .*

Proof: Set $G = U$, $N = u$, $H = V$ and the identity $1 = v$ in Theorem 30. \square

Corollary 2. *Under the conditions of Corollary 1, if G/N is abelian, so also is $H/H \cap N$.* \square

Let us call a group G **solvable** if it contains a sequence of subgroups $G = G_0 \supset G_1 \supset \dots \supset G_s = 1$, each a normal subgroup of the preceding, and with G_{i-1}/G_i abelian.

THEOREM 31. *Any subgroup of a solvable group is solvable.*

Proof: For let H be a subgroup of G , and call $H_i = H \cap G_i$. Then that H_{i-1}/H_i is abelian follows from Corollary 2 above, where G_{i-1} , G_i and H_{i-1} , play the role of G , N and H . \square

THEOREM 32. *The homomorphism of a solvable group is solvable.*

Proof: Let $f(G) = G'$, and define $G'_i = f(G_i)$ where G_i belongs to a sequence exhibiting the solvability of G . Then by (c) there exists a homomorphism mapping G_{i-1}/G_i on G'_{i-1}/G'_i . But the homomorphic image of an abelian group is abelian so that the groups G'_i exhibit the solvability of G' . \square

B. Permutation Groups

Any one to one mapping of a set of n objects on itself is called a **permutation**. The iteration of two such mapping is called their **product**. It may be readily verified that the set of all such mappings forms

a group in which the unit is the identity map. The group is called the symmetric group on n letters.

Let us for simplicity denote the set of n objects by the numbers $1, 2, \dots, n$. The mapping S such that $S(i) = i + 1 \bmod n$ will be denoted by $(123 \dots n)$ and more generally $(ij \dots m)$ will denote the mapping T such that $T(i) = j, \dots, T(m) = i$. If $(ij \dots m)$ has k numbers, then it will be called a k -cycle. It is clear that if $T = (ij \dots s)$ then $T^{-1} = (s \dots ji)$.

We now establish the **Lemma**. *If a subgroup U of the symmetric group on n letters ($n > 4$) contains every 3-cycle, and if u is a normal subgroup of U such that U/u is abelian, then u contains every 3-cycle.*

Proof: Let f be the natural homomorphism $f(U) = U/u$ and let $x = (ijk), y = (krs)$ be two elements of U , where i, j, k, r, s are 5 numbers. Then since U/u is abelian, setting $f(x) = x', f(y) = y'$ we have $f(x^{-1}y^{-1}xy) = x'^{-1}y'^{-1}x'y = 1$, so that $x^{-1}y^{-1}xy \in u$. But $x^{-1}y^{-1}xy = (kji) \cdot (srk) \cdot (ijk) \cdot (krs) = (kjs)$ and for each k, j, s we have $(kjs) \in u$. \square

THEOREM 33. *The symmetric group G on n letters is **not solvable** for $n > 4$.*

Proof: If there were a sequence exhibiting the solvability, since G contains every 3-cycle, so would each succeeding group, and the sequence could not end with the unit. \square

C. Solution of Equations by Radicals

The extension field \mathbb{E} over \mathbb{F} is called an extension by radicals if there exist intermediate fields $\mathbb{B}_1, \mathbb{B}_2, \dots, \mathbb{B}_r = \mathbb{E}$ and $\mathbb{B}_i = \mathbb{B}_{i-1}(a_i)$ where each a_i is a root of an equation of the form $x_{n_i} - a_i = 0$, $a_i \in \mathbb{B}_{i-1}$. A polynomial $f(x)$ in a field \mathbb{F} is said to be **solvable by radicals** if its splitting field lies in an extension by radicals. We assume unless otherwise specified that the base field has characteristic 0 and that \mathbb{F} contains as many roots of unity as are needed to make our subsequent statements valid.

Let us remark first that any extension of \mathbb{F} by radicals can always be extended to an extension of \mathbb{F} by radicals which is normal over \mathbb{F} . Indeed \mathbb{B}_1 is a normal extension of \mathbb{B}_0 since it contains not only a_1 , but ϵa_1 , where ϵ is any n_1 -root of unity, so that \mathbb{B}_1 is the splitting field of $x^{n_1} - a_1$. If $f_1(x) = \prod_{\sigma} (x^{n_2} - \sigma(a_2))$, where σ takes all values in the group of automorphisms of \mathbb{B}_1 over \mathbb{B}_0 , then f_1 is in \mathbb{B}_0 , and adjoining successively the roots of $x^{n_2} - \sigma(a_2)$ brings us to an extension of \mathbb{B}_2 which is normal over \mathbb{F} . Continuing in this way we arrive at an extension of \mathbb{E} by radicals which will be normal over \mathbb{F} . We now prove

THEOREM 34. *The polynomial $f(x)$ is solvable by radicals **if and only if** its group is solvable.*

Proof: Suppose $f(x)$ is solvable by radicals. Let \mathbb{E} be a normal extension of \mathbb{F} by radicals containing the splitting field \mathbb{B} of $f(x)$, and call G the group of \mathbb{E} over \mathbb{F} . Since for each i , \mathbb{B}_i is a Kummer extension of \mathbb{B}_{i-1} , the group of \mathbb{B}_i over \mathbb{B}_{i-1} is abelian. In the sequence of groups $G = G_{\mathbb{B}_0} \supset G_{\mathbb{B}_1} \supset \dots \supset G_{\mathbb{B}_r} = 1$ each is a normal subgroup of the preceding since $G_{\mathbb{B}_{i-1}}$ is the group of \mathbb{E} over \mathbb{B}_{i-1} and \mathbb{B}_{i-1} is a normal extension of \mathbb{B}_i . But $G_{\mathbb{B}_{i-1}}/G_{\mathbb{B}_i}$ is the group of \mathbb{B}_i over \mathbb{B}_{i-1} and hence is abelian. Thus G is solvable. However, $G_{\mathbb{B}}$ is a normal subgroup of G , and $G/G_{\mathbb{B}}$ is the group of \mathbb{B} over \mathbb{F} , and is therefore the group of the polynomial $f(x)$. But $G/G_{\mathbb{B}}$ is a homomorphism of the solvable group G and hence is itself solvable.

On the other hand, suppose the group G of $f(x)$ to be solvable and let \mathbb{E} be the splitting field. Let $G = G_0 \supset G_1 \supset \dots \supset G_r = 1$ be a sequence with abelian factor groups. Call \mathbb{B}_i the fixed field for G_i .

Since G_{i-1} is the group of \mathbb{E} over B_{i-1} and G_i is a normal subgroup of G_{i-1} , then \mathbb{B}_i is normal over \mathbb{B}_{i-1} and the group G_{i-1}/G_i is abelian. Thus \mathbb{B}_i is a Kummer extension of \mathbb{B}_{i-1} , hence is splitting field of a polynomial of the form $(x^n - a_1)(x^n - a_2) \cdots (x^n - a_s)$ so that by forming the successive splitting fields of the $x^n - a_k$ we see that \mathbb{B}_i is an extension of \mathbb{B}_{i-1} by radicals, from which it follows that \mathbb{E} is an extension by radicals. \square

Remark. The assumption that \mathbb{F} contains roots of unity is not necessary in the above theorem. For if $f(x)$ has a solvable group G , then we may adjoin to \mathbb{F} a primitive n -th root of unity, where n is, say, equal to the order of G . The group of $f(x)$ when considered as lying in \mathbb{F}' is, by the theorem on **Natural Irrationalities**, a subgroup G' of G , and hence is solvable. Thus the splitting field over \mathbb{F}' of $f(x)$ can be obtained by radicals. Conversely, if the splitting field \mathbb{E} over \mathbb{F} of $f(x)$ can be obtained by radicals, then by adjoining a suitable root of unity \mathbb{E} is extended to \mathbb{E}' which is still normal over \mathbb{F}' . But \mathbb{E}' could be obtained by adjoining first the root of unity, and then the radicals, to \mathbb{F} ; \mathbb{F} would first be extended to \mathbb{F}' and then \mathbb{F}' would be extended to \mathbb{E}' . Calling G the group of \mathbb{E}' over \mathbb{F} and G' the group of \mathbb{E}' over \mathbb{F}' , we see that G' is solvable and G/G' is the group of \mathbb{F}' over \mathbb{F} and hence abelian. Thus G is solvable. The factor group $G/G_{\mathbb{E}}$ is the group of $f(x)$ and being a homomorphism of a solvable group is also solvable.

D. The General Equation of Degree n

If \mathbb{F} is a field, the collection of rational expressions in the variables u_1, u_2, \dots, u_n with coefficients in \mathbb{F} is a field $\mathbb{F}(u_1, u_2, \dots, u_n)$. By the general equation of degree n we mean the equation

$$(1) \quad f(x) = x^n - u_1 x^{n-1} + u_2 x^{n-2} - \cdots + (-1)^n u_n.$$

Let \mathbb{E} be the splitting field of $f(x)$ over $\mathbb{F}(u_1, u_2, \dots, u_n)$. If v_1, v_2, \dots, v_n are the roots of $f(x)$ in \mathbb{E} , then

$$\begin{aligned} u_1 &= v_1 + v_2 + \cdots + v_n \\ u_2 &= v_1 v_2 + v_1 v_3 + \cdots + v_{n-1} v_n \\ &\vdots \\ u_n &= v_1 v_2 \cdots v_n. \end{aligned}$$

We shall prove that the group of \mathbb{E} over $\mathbb{F}(u_1, u_2, \dots, u_n)$ is the symmetric group.

Let $\mathbb{F}(x_1, x_2, \dots, x_n)$ be the field generated from \mathbb{F} by the variables x_1, x_2, \dots, x_n . Let

$$\begin{aligned} a_1 &= x_1 + x_2 + \cdots + x_n \\ a_2 &= x_1 x_2 + x_1 x_3 + \cdots + x_{n-1} x_n \\ &\vdots \\ a_n &= x_1 x_2 \cdots x_n. \end{aligned}$$

be the elementary symmetric functions, i.e., $(x - x_1)(x - x_2) \cdots (x - x_n) = x^n - a_1 x^{n-1} + \cdots + (-1)^n a_n = f^*(x)$. If $g(a_1, a_2, \dots, a_n)$ is a polynomial in a_1, a_2, \dots, a_n then $g(a_1, a_2, \dots, a_n) = 0$ only if g is the zero

polynomial. For if $g(\sum x_i, \sum x_i x_k, \dots) = 0$, then this relation would hold also if the x_i were replaced by the v_i . Thus, $g(\sum v_i, \sum v_i v_k, \dots) = 0$ or $g(u_1, u_2, \dots, u_n) = 0$ from which it follows that g is identically zero.

Between the subfield $\mathbb{F}(a_1, \dots, a_n)$ of $\mathbb{F}(x_1, \dots, x_n)$ and $\mathbb{F}(u_1, \dots, u_n)$ we set up the following correspondence: Let $f(u_1, \dots, u_n)/g(u_1, \dots, u_n)$ be an element of $\mathbb{F}(u_1, \dots, u_n)$. We make this correspond to $f(a_1, \dots, a_n)/g(a_1, \dots, a_n)$. This is clearly a mapping of $\mathbb{F}(u_1, \dots, u_n)$ on all of $\mathbb{F}(a_1, \dots, a_n)$. Moreover, if $f(a_1, \dots, a_n)/g(a_1, \dots, a_n) = f_1(a_1, a_2, \dots, a_n)/g_1(a_1, a_2, \dots, a_n)$, then $f g_1 - g f_1 = 0$. But this implies by the above that

$$f(u_1, \dots, u_n) g_1(u_1, \dots, u_n) - g(u_1, \dots, u_n) f_1(u_1, \dots, u_n) = 0$$

so that $f(u_1, \dots, u_n)/g(u_1, \dots, u_n) = f_1(u_1, \dots, u_n)/g_1(u_1, \dots, u_n)$. It follows readily from this that the mapping of $\mathbb{F}(u_1, \dots, u_n)$ on $\mathbb{F}(a_1, a_2, \dots, a_n)$ is an isomorphism. But under this correspondence $f(x)$ corresponds to $f^*(x)$. Since \mathbb{E} and $\mathbb{F}(x_1, x_2, \dots, x_n)$ are respectively splitting fields of $f(x)$ and $f^*(x)$, by Theorem 10 the isomorphism can be extended to an isomorphism between \mathbb{E} and $\mathbb{F}(x_1, x_2, \dots, x_n)$. Therefore, the group of \mathbb{E} over $\mathbb{F}(u_1, u_2, \dots, u_n)$ is isomorphic to the group of $\mathbb{F}(x_1, x_2, \dots, x_n)$ over $\mathbb{F}(a_1, a_2, \dots, a_n)$.

Each permutation of x_1, x_2, \dots, x_n leaves a_1, a_2, \dots, a_n fixed and, therefore, induces an automorphism of $\mathbb{F}(x_1, x_2, \dots, x_n)$ which leaves $\mathbb{F}(a_1, a_2, \dots, a_n)$ fixed. Conversely, each automorphism of $\mathbb{F}(x_1, x_2, \dots, x_n)$ which leaves $\mathbb{F}(a_1, a_2, \dots, a_n)$ fixed must permute the roots x_1, x_2, \dots, x_n of $f^*(x)$ and is completely determined by the permutation it effects on x_1, x_2, \dots, x_n . Thus, the group of $\mathbb{F}(x_1, x_2, \dots, x_n)$ over $\mathbb{F}(a_1, a_2, \dots, a_n)$ is the symmetric group on n letters. Because of the isomorphism between $\mathbb{F}(x_1, x_2, \dots, x_n)$ and \mathbb{E} , the group for \mathbb{E} over $\mathbb{F}(u_1, u_2, \dots, u_n)$ is also the symmetric group. If we remark that the symmetric group for $n > 4$ is not solvable, we obtain from the theorem on solvability of equations the famous **theorem of Abel**:

THEOREM 35. *The group of the general equation of degree n is the symmetric group on n letters. The general equation of degree n is not solvable by radicals if $n > 4$.*

□

E. Solvable Equations of Prime Degree

The group of an equation can always be considered as a permutation group. If $f(x)$ is a polynomial in a field \mathbb{F} , let a_1, a_2, \dots, a_n be the roots of $f(x)$ in the splitting field $\mathbb{E} = \mathbb{F}(a_1, a_2, \dots, a_n)$. Then each automorphism of \mathbb{E} over \mathbb{F} maps each root of $f(x)$ into a root of $f(x)$, that is, permutes the roots. Since \mathbb{E} is generated by the roots of $f(x)$, different automorphisms must effect distinct permutations. Thus, the group of \mathbb{E} over \mathbb{F} is a permutation group acting on the roots a_1, a_2, \dots, a_n of $f(x)$.

For an irreducible equation this group is always transitive. For let a and a' be any two roots of $f(x)$, where $f(x)$ is assumed irreducible. $\mathbb{F}(a)$ and $\mathbb{F}(a')$ are isomorphic where the isomorphism is the identity on \mathbb{F} , and this isomorphism can be extended to an automorphism of \mathbb{E} (Theorem 10). Thus, there is an automorphism sending any given root into any other root, which establishes the *transitivity* of the group.

A permutation σ of the numbers $1, 2, \dots, q$ is called a linear substitution modulo q if there exists a number $b \neq 0$ modulo q such that $\sigma(i) \equiv bi + c \pmod{q}$, $i = 1, 2, \dots, q$.

THEOREM 36. *Let $f(x)$ be an irreducible equation of prime degree q in a field \mathbb{F} . The group G of $f(x)$ (which is a permutation group of the roots, or the numbers $1, 2, \dots, q$) is solvable **if and only if**, after a suitable change in the numbering of the roots, G is a group of linear substitutions modulo q , and in the group G all the substitutions with $b = 1$, $\sigma(i) \equiv c + 1$ ($c = 1, 2, \dots, q$) occur.*

Proof Let G be a transitive substitution group on the numbers $1, 2, \dots, q$ and let G_1 be a normal subgroup of G . Let $1, 2, \dots, k$ be the images of 1 under the permutations of G_1 ; we say: $1, 2, \dots, k$ is a domain of transitivity of G_1 . If $i \leq q$ is a number not belonging to this domain of transitivity, there is a $\sigma \in G$ which maps 1 on i . Then $\sigma(1, 2, \dots, k)$ is a domain of transitivity of $\sigma G_1 \sigma^{-1}$. Since G_1 is a normal subgroup of G , we have $G_1 = \sigma G_1 \sigma^{-1}$. Thus, $\sigma(1, 2, \dots, k)$ is again a domain of transitivity of G_1 which contains the integer i and has k elements. Since i was arbitrary, the domains of transitivity of G_1 all contain k elements. Thus, the numbers $1, 2, \dots, q$ are divided into a collection of mutually exclusive sets, each containing k elements, so that k is a divisor of q . Thus, in case q is a **prime**, either $k = 1$ (and then G_1 consists of the unit alone) or $k = q$ and G_1 is also transitive.

To prove the theorem, we consider the case in which G is solvable. Let $G = G_0 \supset G_1 \supset \dots \supset G_{s+1} = 1$ be a sequence exhibiting the solvability. Since G_s is abelian, choosing a cyclic subgroup of it would permit us to assume the term before the last to be cyclic, i.e., G_s is cyclic. If σ is a generator of G_s , σ must consist of a cycle containing all q of the numbers $1, 2, \dots, q$ since in any other case G_s would not be transitive [if $\sigma = (lij \dots m)(n \dots p) \dots$ then the powers of σ would map 1 only into $1, i, j, \dots, m$, contradicting the transitivity of G_s]. By a change in the number of the permutation letters, we may assume

$$\begin{aligned}\sigma(i) &\equiv i + 1 \pmod{q} \\ \sigma^c(i) &\equiv i + c \pmod{q}.\end{aligned}$$

Now let τ be any element of G_{s-1} . Since G_s is a normal subgroup of G_{s-1} , $\tau \sigma \tau^{-1}$ is an element of G_s , say $\tau \sigma \tau^{-1} = \sigma^b$. Let $\tau(i) = j$ or $\tau^{-1}(j) = i$, then $\tau \sigma \tau^{-1}(j) = \sigma^b(j) \equiv j + b \pmod{q}$. Therefore, $\tau \sigma(i) \equiv \tau(i) + b \pmod{q}$ or $\tau(i + 1) \equiv \tau(i) + b$ for each i . Thus, setting $\tau(0) = c$, we have $\tau(1) = c + b$, $\tau(2) = \tau(1) + b = c + 2b$ and in general $\tau(i) \equiv c + ib \pmod{q}$. Thus, each substitution in G_{s-1} is a linear substitution. Moreover, the only elements of G_{s-1} which leave no element fixed belong to G_s , since for each $a \neq 1$ there is an i such that $ai + b \equiv i \pmod{q}$ [take i such that $(a - 1)i \equiv -b$].

We prove by an induction that the elements of G are all linear substitutions, and that the only cycles of q letters belong to G_s . Suppose the assertion true of G_{s-n} . Let $\tau \in G_{s-n-1}$ and let v be a cycle which belongs to G_s (hence also to G_{s-n}). Since the transform of a cycle is a cycle, $\tau \sigma \tau^{-1}$ is a cycle in G_{s-n} , and hence belongs to G_n . Thus $\tau \sigma \tau^{-1} = \sigma^b$ for some b . By the argument in the preceding paragraph, τ is a linear substitution $bi + c$ and if τ itself does not belong to G_s , then τ leaves one integer fixed and hence is not a cycle of q elements.

We now prove the second half of the theorem. Suppose G is a group of linear substitutions which contains a subgroup N of the form $c(i) \equiv i + c$. Since the only linear substitutions which do not leave an integer fixed belong to N , and since the transform of a cycle of q elements is again a cycle of q elements, N is a normal subgroup of G . In each coset $N \cdot \tau$ where $\tau(i) \equiv bi + c$ the substitution $\sigma^{-1}\tau$ occurs, where $\sigma \equiv i + c$. But $\sigma^{-1}\tau(i) = (bi + c) - c \equiv bi$. Moreover, if $\tau(i) \equiv i$ and $\tau'(i) = b'i$ then $\tau\tau'(i) \equiv bb'i$. Thus, the factor group (G/N) is isomorphic to a multiplicative subgroup of the numbers $1, 2, \dots, q-1 \pmod q$ and is therefore abelian. Since (G/N) and N are both abelian, G is solvable. \square

Corollary 1. *If G is a solvable transitive substitution group on q letters (q prime), then the only substitution of G which leaves two or more letters fixed is the identity.*

Proof This follows from the fact that each substitution is linear modulo q and $bi + c \equiv i \pmod q$ has either no solution ($b \equiv 1, c \not\equiv 0$) or exactly one solution ($b \not\equiv 1$) unless $b \equiv 1, c \equiv 0$ in which case the substitution is the identity. \square

Corollary 2. *A solvable, irreducible equation of prime degree in a field which is a subset of the real numbers has either one real root or all its roots are real.*

Proof The group of the equation is a solvable transitive substitution group on q (prime) letters. In the splitting field (contained in the field of complex numbers) the automorphism which maps a number into its complex conjugate would leave fixed all the real numbers. By Corollary 1, if two roots are left fixed, then all the roots are left fixed, so that if the equation has two real roots all its roots are real. \square

F. Ruler and Compass Construction

Suppose there is given in the plane a finite number of elementary geometric figures, that is, *points*, *straight lines* and *circles*. We seek to construct others which satisfy certain conditions in terms of the given figures.

Permissible steps in the construction will entail the choice of an arbitrary point interior to a given region, drawing a line through two points and a circle with given center and radius, and finally intersecting pairs of lines, or circles, or a line and circle. Since a straight line, or a line segment, or a circle is determined by two points, we can consider ruler and compass constructions as constructions of points from given points, subject to certain conditions.

If we are given two points we may join them by a line, erect a perpendicular to this line at, say, one of the points and, taking the distance between the two points to be the unit, we can with the compass lay off any integer n on each of the lines. Moreover, by the usual method, we can draw parallels and can construct m/n . Using the two lines as axes of a cartesian coordinate system, we can with ruler and compass construct all points with rational coordinates.

If a, b, c, \dots are numbers involved as coordinates of points which determine the figures given, then the sum, product, difference and quotient of any two of these numbers can be constructed. Thus, each element of the field $\mathbb{R}(a, b, c, \dots)$ which they generate out of the rational numbers can be constructed. It is required that an arbitrary point is any point of a given region. If a construction by ruler and compass is possible, we can always choose our arbitrary points as points having rational coordinates. If we join two

points with coefficients in $\mathbb{R}(a, b, c, \dots)$ by a line, its equation will have coefficients in $\mathbb{R}(a, b, c, \dots)$ and the intersection of two such lines will be a point with coordinates in $\mathbb{R}(a, b, c, \dots)$. The equation of a circle will have coefficients in the field if the circle passes through three points whose coordinates are in the field or if its center and one point have coordinates in the field. However, the coordinates of the intersection of two such circles, or a straight line and circle, will involve **square roots**. It follows that if a point can be constructed with a ruler and compass, its coordinates must be obtainable from $\mathbb{R}(a, b, c, \dots)$ by a formula only involving square roots, that is, its coordinates will lie in a field $\mathbb{R}_s \supset \mathbb{R}_{s-1} \supset \dots \supset \mathbb{R}_1 = \mathbb{R}(a, b, c, \dots)$ where each field \mathbb{R}_i is splitting field over \mathbb{R}_{i-1} of a quadratic equation $x^2 - a = 0$.

It follows (Theorem 6) since either $\mathbb{R}_i = \mathbb{R}_{i-1}$ or $(\mathbb{R}_i/\mathbb{R}_{i-1}) = 2$, that $(\mathbb{R}_s/\mathbb{R}_1)$ is a power of two. If x is the coordinate of a constructed point, then $(\mathbb{R}_1(x)/\mathbb{R}_1) \cdot (\mathbb{R}_s/\mathbb{R}_1(x)) = (\mathbb{R}_s/\mathbb{R}_1) = 2^\nu$ so that $\mathbb{R}_1(x)/\mathbb{R}_1$ must also be a power of two.

Conversely, if the coordinates of a point can be obtained from $\mathbb{R}(a, b, c, \dots)$ by a formula involving square roots only, then the point can be constructed by ruler and compass. For, the field operations of addition, subtraction, multiplication and division may be performed by ruler and compass constructions and, also, square roots using $1 : r = r : r_1$ to obtain $r = \sqrt{r_1}$ may be performed by means of ruler and compass instructions.

As an illustration of these considerations, let us show that it is impossible to trisect an angle of 60° . Suppose we have drawn the unit circle with center at the vertex of the angle, and set up our coordinate system with X -axis as a side of the angle and origin at the vertex. Trisection of the angle would be equivalent to the construction of the point $(\cos 20^\circ, \sin 20^\circ)$ on the unit circle. From the equation $\cos 3\theta = 4\cos^3 \theta - 3\cos \theta$, the abscissa would satisfy $4x^3 - 3x = 1/2$. The reader may readily verify that this equation has no rational roots, and is therefore irreducible in the field of rational numbers. But since we may assume only a straight line and unit length given, and since the 60° angle can be constructed, we may take $\mathbb{R}(a, b, c, \dots)$ to be the field \mathbb{R} of rational numbers. A root a of the irreducible equation $8x^3 - 6x - 1 = 0$ is such that $(\mathbb{R}(a)/\mathbb{R}) = 3$, and not a power of two.

Index

- character, [24](#)
- characteristic, [35](#)
- column vector, [9](#)
- commutative field, [6](#)

- domain of transitivity, [47](#)

- elementary symmetric functions, [27](#)

- field, [6](#)
- finite field, [34](#)
- Finite Fields, [32](#)
- Fundamental Theorem of Galois Theory, [31](#)

- kernel, [39](#)
- Kummer, extension, [38](#)
- Kummer, field, [38](#)

- left cosets, [31](#)
- left invariant, [32](#)
- linear substitution, [47](#)

- minimal generating system, [33](#)

- natural homomorphism, [43](#)
- Noether equations, [36](#)
- normal extension, [28](#)

- permutation, [43](#)
- polynomial, separable, [30](#)
- primitive, [40](#)

- rank, [10](#)
- roots of unity, [36](#)
- row vector, [9](#)

- separable extension, [30](#)
- solvable by radicals, [44](#)
- solvable group, [43](#)
- subspace, [9](#)
- symmetric group, [44](#)
- theorem of symmetric functions, [28](#)
- vector space over a field, [6](#)