GALOIS THEORY

GALOIS THEORY

AND

ITS APPLICATION TO THE PROBLEM OF SOLVABILITY BY RADICALS OF AN EQUATION OVER A FIELD OF PRIME OR ZERO CHARACTERISTIC

By

RUPERT GEORGE RONALD, B.A.

A Thesis

Submitted to the Faculty of Arts and Science

in Partial Fulfilment of the Requirements

for the Degree

Master of Arts

McMaster University

May 1954

MASTER OF ARTS (1954)
(Mathematics)

McMASTER UNIVERSITY
Hamilton, Ontario

TITLE: Galois Theory and its Application to the Problem of Solvability by Radicals of an Equation over a Field of Prime or Zero Characteristic

AUTHOR: Rupert George Ronald, B.A.
(McMaster University)

SUPERVISOR: Professor N.D. Lane

NUMBER OF PAGES: 119

SCOPE AND CONTENTS:

In Part I of the thesis an account is given of the basic algebra of extension fields which is required for the understanding of Galois theory. The fundamental theorem states the relationships of the subgroups of a permutation group of the root field of an equation to the subfields which are left invariant by these subgroups. Extensions of the basic theorem conclude Part I. In Part II the solvability of equations by radicals is discussed, for fields of characteristic zero. A discussion of finite fields and primitive roots leads to a criterion for the solvability by radicals of equations over fields of prime characteristic. Finally, a method for determining the Galois group of any equation is discussed. Most of the material in the introductory chapters is taken from Artin's: Galois Theory [cf. p. 120].

TABLE OF CONTENTS

PART I

FUNDAMENTALS OF GALOIS THEORY

PART I

FUNDAMENTALS OF GALOIS THEORY

CHAPTER I

LINEAR ALGEBRA

1.1 Fields and Vector Spaces.

In the notation (1.1.1), (2.3.11), etc., the first number will denote the chapter, the second number the article, and the third number the lemma or theorem as it occurs in the article. A similar notation will be used with equations.

Definition: A set of at least two elements forms a field with respect to two operations called addition and multiplication if (a) the set is closed with respect to addition and multiplication; (b) the set forms a commutative group with respect to addition whose identity is called the zero element; (c) the nonzero elements of the set form a group with respect to multiplication, whose identity is called the unity element; (d) the distributive laws hold: $a(b + c) = ab + ac$, $(a + b)c = ac + bc$. If multiplication in the field is commutative then we shall say the elements form a commutative field.

Definition: If V is an additive abelian group with elements $A, B, \ldots$, and F is a field with elements $a, b, \ldots$; and if for each a of F and A of V the product aA denotes an element of V, then V is called a left vector space over F if the following assumptions hold:

(1) $a(A + B) = aA + aB$,

(2) $(a + b)A = aA + bA$,

(3) $a(bA) = (ab)A$,

(4) $1A = A$.

Similarly when multiplication by field elements is from the right we shall call V a right vector space.

If o is the zero element of F and 0 the zero element of V then from these assumptions we see that $oA = 0$ and $a0 = 0$. The first relation follows from the equations: $aA = (a + o)A = aA + oA$. Similarly the second relation follows from: $aA = a(A + 0) = aA + a0$.

1.2 Linear Equations.

If we have a set of equations:

$$
(1.2.1) \qquad \begin{aligned} L_1 &\equiv a_{11}x_1 + a_{12}x_2 + \dots + a_{1n}x_n = o, \\ &\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots \\ L_m &\equiv a_{m1}x_1 + a_{m2}x_2 + \dots + a_{mn}x_n = o, \end{aligned}
$$

where the a_{ij}, $i = 1,2,\dots,m$, $j = 1,2,\dots,n$, are m.n elements belonging to F, a field, we will need to know conditions such that elements in F exist to satisfy the equations. Equations (1.2.1) are called linear homogeneous equations, and a set of elements, $x_1,x_2,\dots,x_n$ of F for which all the equations (1.2.1) are true is called a solution of the system. If all the elements $x_1,x_2,\dots,x_n$ are zero then the solution is trivial; otherwise it is called non-trivial.

THEOREM 1.2.1: *A system of linear homogeneous equa-*

<u>tions always has a non-trivial solution if the number of unknowns exceeds the number of equations</u>.

<u>Proof</u>: We see that one homogeneous equation $a_{11}x_1 + a_{12}x_2 + \ldots + a_{1n}x_n = o$, $n > 1$, has a non-trivial solution for if one of the a_{ij}'s is zero, say $a_{11} = o$, then $x_1 = 1$, $x_2 = x_3 = \ldots = x_n = o$ will serve as a solution. We continue using the induction method of proof. We assume that each system of equations, k in number, in more than k unknowns has a non-trivial solution when $k < m$. In the system of equations (1.2.1) we assume $n > m$. We wish to find elements $x_1, \ldots, x_n$ not all zero such that $L_1 = L_2 = \ldots = L_m = 0$. If $a_{ij} = o$ for each i and j then any choice of $x_1, \ldots, x_n$ will serve as a solution. If not all a_{ij} are zero, then we may assume $a_{11} \neq o$. We can find a non-trivial solution to equations (1.2.1), if and only if we can find a non-trivial solution to the following system:

$$
\begin{aligned}
&L_1 = 0, \\
&L_2 - \frac{a_{21}}{a_{11}} L_1 = 0, \\
&\ldots\ldots\ldots\ldots\ldots \\
&L_m - \frac{a_{m1}}{a_{11}} L_1 = 0.
\end{aligned} \tag{1.2.2}
$$

For, if $x_1, x_2, \ldots, x_n$ is a solution to (1.2.2) then, since $L_1 = 0$, the second term in each of the remaining equations is zero and hence, $L_2 = L_3 = \ldots = L_m = 0$. Conversely, if (1.2.1) is satisfied, then the new system is clearly satisfied. The new system was set up so as to eliminate x_1 from the last m - 1 equations. The last m - 1 equations have a non-trivial solution by our inductive assumption which proves the theorem.

Definition: In a vector space V over a field F the vectors $A_1,\ldots,A_n$ are called dependent if there exist elements $x_1,\ldots,x_n$ not all o of F such that $x_1A_1 + x_2A_2 + \ldots + x_nA_n = 0$. If the vectors $A_1,\ldots,A_n$ are not dependent, they are called independent.

Definition: The dimension of a vector space V over a field F is the maximum number of independent elements in V. Thus we see that the dimension of V is n if there are n independent elements in V and no set of more than n elements are independent.

Definition: A system $A_1,\ldots,A_m$ of elements in V is called a generating system of V if each element A of V can be expressed linearly in terms of $A_1,\ldots,A_m$, that is, $A = \sum_{i=1}^{m} a_i A_i$ for a suitable choice of a_i, $i = 1,\ldots,m$, in a field F.

THEOREM 1.2.2: In any generating system the maximum number of independent vectors is equal to the dimension of the vector space.

Proof: Let p be the maximum number of independent vectors in the generating system $S = (A_1,\ldots,A_q)$ of V and assume that $A_1,\ldots,A_p$ are p independent vectors of S. Since p is the maximum number of independent vectors then the p + 1 vectors $A_1,\ldots,A_p,A_k$, where $p < k \leq q$, are linearly dependent. Thus,

$$a_1A_1 + \dots + a_pA_p + a_kA_k = o,$$

where not all $a_i = o$, $i = 1,\dots,p,k$, and further, where $a_k \neq o$; for if $a_k = o$ then $A_1,\dots,A_p$ would be dependent. Therefore,

$$A_k = -\frac{1}{a_k}(a_1A_1 + \dots + a_pA_p).$$

Thus every $A_k \in S$ is then a linear combination of $A_1,\dots,A_p$. Since every vector B of V is a linear combination of $A_1,\dots,A_q$, B is also a linear combination of $A_1,\dots,A_p$. Conversely, since every linear combination of these p vectors also belongs to V, V consists of all linear combinations of $A_1,\dots,A_p$. Consider t vectors B_j of V, where $t > p$ and let $B_j = \sum_{i=1}^{p} a_{ij}A_i$, $j = 1,\dots,t$. Let $x_1,\dots,x_t$ be a non-trivial solution of the $p < t$ equations $\sum_{j=1}^{t} a_{ij}x_j = 0$, $i = 1,\dots,p$ (cf. Theorem 1.2.1). Then

$$\sum_{j=1}^{t} x_jB_j = \sum_{j=1}^{t} x_j\Big(\sum_{i=1}^{p} a_{ij}A_i\Big) = \sum_{i=1}^{p}\Big(\sum_{j=1}^{t} a_{ij}x_j\Big)A_i = 0.$$

Thus $B_1,\dots,B_t$ are linearly dependent whenever $t > p$. Since p linearly independent vectors of V do exist, for example $A_1,\dots,A_p$, we see that p is the dimension of V and that $A_1,\dots,A_p$ forms a generating system for the vector space V. This proves our theorem.

<u>Definition</u>: Any set of linearly independent vectors which generates V is called a basis.

<u>THEOREM 1.2.3</u>: <u>Let</u> $A_1,\dots,A_n$ <u>be a basis of a vector space V and let B be any element of V</u>. <u>Then the representation</u> $B = c_1A_1 + c_2A_2 + \dots + c_nA_n$ <u>is unique</u>.

Proof: If

$$B = c_1A_1 + \dots + c_nA_n = d_1A_1 + \dots + d_nA_n$$

where $c_i \neq d_i$, for some $i = 1,\dots,n$, then $\sum_{i=1}^{n}(c_i - d_i)A_i = 0$. Since A_i are independent, this is a contradiction, which proves the theorem.

THEOREM 1.2.4: Let $A_1,\dots,A_n$ be a basis of V and let $B_1,\dots,B_n$ be a set of n vectors such that $B_i = \sum_{j=1}^{n} a_{ij}A_j$, $i = 1,\dots,n$. Then the B_i form a basis if and only if $|a_{ij}| \neq 0$.

Proof: Let

$$\sum_{i=1}^{n} x_iB_i = \sum_{i=1}^{n} x_i \sum_{j=1}^{n} a_{ij}A_j = \sum_{j=1}^{n}\Big(\sum_{i=1}^{n} a_{ij}x_i\Big)A_j = 0.$$

Thus $\sum_{i=1}^{n} a_{ij}x_i = 0$, $j = 1,\dots,n$. These equations have a non-trivial solution[1] if and only if $|a_{ij}| = 0$, and thus B_i are independent if and only if $|a_{ij}| \neq 0$.

Definition: A subset of a vector space is called a subspace if it is a subgroup of the vector space and if the multiplication of any element in the subset by any element of the field is also in the subset. An s-tuple of elements $A = [a_1,\dots,a_s]$ in a field F will be called a row vector. All s-tuples will form a vector space if,

(1) $[a_1,\dots,a_s] = [b_1,\dots,b_s]$ if and only if $a_i = b_i$, $i = 1,\dots,s$,

(2) $[a_1,\dots,a_s] + [b_1,\dots,b_s] = [a_1 + b_1,\dots,a_s + b_s]$,

(3) $b[a_1,\dots,a_s] = [ba_1,\dots,ba_s]$, for b an element of F.

When the s-tuples are written vertically $\begin{bmatrix} a_1 \\ \cdot \\ \cdot \\ \cdot \\ a_s \end{bmatrix} = A^1$ they will

---

[1] A. A. Albert, Solid and Analytical Geometry, McGraw-Hill, 1949, p. 95.

be called column vectors.

THEOREM 1.2.5: The row (column) vector space F^n of all n-tuples from a field F is a vector space of dimension n over F.

Proof: The n elements,

$$\begin{aligned} e_1 &= (1,0,0,\ldots,0), \\ e_2 &= (0,1,0,\ldots,0), \\ &\ldots\ldots\ldots\ldots\ldots\ldots \\ e_n &= (0,0,0,\ldots,1), \end{aligned}$$

are independent and generate F^n. This is true since $(a_1,a_2,\ldots,a_n) = a_1e_1 + a_2e_2 + \ldots + a_ne_n = \sum_{i=1}^{n} a_ie_i$, $i = 1,2,\ldots,n$.

Definition: We call a rectangular array,

$$A_m^n = [a_{ij}] = \begin{bmatrix} a_{11}a_{12}\cdots a_{1n} \\ a_{21}a_{22}\cdots a_{2n} \\ \cdots\cdots\cdots\cdots \\ a_{m1}a_{m2}\cdots a_{mn} \end{bmatrix}$$

where $i = 1,2,\ldots,m$, $j = 1,2,\ldots,n$, of elements of a field F, a matrix. By the right row rank of a matrix, we mean the maximum number of independent row vectors among the rows $(a_{i1},\ldots,a_{in})$ 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 1.2.6: In any matrix with elements in a field the right (left) column rank equals the left (right) row rank.

Proof: We call the column vectors of the matrix $C^{(1)}$,

$\ldots, C^{(n)}$ and the row vectors $R_{(1)}, \ldots, R_{(m)}$. The column vector 0 is $\begin{bmatrix} 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ \cdot \\ \cdot \\ \cdot \\ 0 \end{bmatrix}$ and any right dependence $C^{(1)}x_1 + C^{(2)}x_2 + \ldots + C^{(n)}x_n = 0$ is equivalent to a solution of the equations

$$\begin{aligned} a_{11}x_1 + a_{12}x_2 + \ldots + a_{1n}x_n &= 0, \\ \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots \\ a_{m1}x_1 + a_{m2}x_2 + \ldots + a_{mn}x_n &= 0. \end{aligned} \tag{1.2.3}$$

Any change in the order in which the rows are written still gives us the same set of equations and 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. Let the right column rank be c and let the left row rank be r. We may assume the first r rows to be independent row vectors. The row vector space generated by all the rows of the matrix has, by Theorem 1.2.2, the dimension r and is generated by the first r rows. Thus, each row after the r-th is linearly expressible in terms of the first r rows. Thus, any solution of the first r equations in the set (1.2.3) will be a solution of the entire system since any of the remaining n - r equations can be represented as a linear combination of the first r. Conversely, any solution of equations (1.2.3) will also be a solution of the first r equations. Therefore the matrix,

$$(1.2.4)\qquad \begin{bmatrix} a_{11}a_{12}\cdots a_{1n} \\ \cdots\cdots\cdots\cdots \\ a_{r1}a_{r2}\cdots a_{rn} \end{bmatrix}$$

of the first r rows of the original matrix has the same right column rank as the original. It also has the same left row rank since the r rows chosen were independent. But the column rank of matrix (1.2.4) cannot exceed r by Theorem 1.2.5. Therefore $c \leq r$. Similarly, calling c' the left column rank and r' the right row rank, then $c' \leq r'$. If we form the transpose of the original matrix, that is, replace rows by columns and vice versa, then the left row rank of the transposed matrix equals the left column rank of the original. Now apply the above relations to the transposed matrix and we see that $r \leq c$ and $r' \leq c'$. Therefore $r = c$ and $r' = c'$ which was to be proved.

<u>Corollary</u>: <u>In a commutative field the row and column ranks are equal</u>.

<u>Definition</u>: The rank of a matrix over a commutative field is its row or column rank.

<u>THEOREM 1.2.7</u>: <u>The set of non-homogeneous linear equations</u>,

$$(1.2.5)\qquad \begin{aligned} a_{11}x_1 + a_{12}x_2 + \cdots + a_{1n}x_n &= a_{1,n+1}, \\ a_{21}x_1 + a_{22}x_2 + \cdots + a_{2n}x_n &= a_{2,n+1}, \\ \cdots\cdots\cdots\cdots\cdots\cdots&\cdots\cdots \\ a_{m1}x_1 + a_{m2}x_2 + \cdots + a_{mn}x_n &= a_{m,n+1}, \end{aligned}$$

<u>with coefficients in a field, has a solution if and only if</u>

<u>the left row rank of the augmented[1] matrix</u> A_m^{n+1} <u>is equal to the left row rank of the coefficient matrix</u> A_m^n.

<u>Proof</u>: The set (1.2.5) has a solution if and only if the column vector $A^{(n+1)} = \begin{bmatrix} a_{1,n+1} \\ \cdot \\ \cdot \\ \cdot \\ a_{m,n+1} \end{bmatrix}$ lies in the space generated by the vectors $A^{(1)} = \begin{bmatrix} a_{11} \\ \cdot \\ \cdot \\ \cdot \\ a_{m1} \end{bmatrix}$, $A^{(2)} = \begin{bmatrix} a_{12} \\ \cdot \\ \cdot \\ \cdot \\ a_{m2} \end{bmatrix}, \ldots,$ $A^{(n)} = \begin{bmatrix} a_{1n} \\ \cdot \\ \cdot \\ \cdot \\ a_{mn} \end{bmatrix}$. Since the vector space generated by the columns of A_m^n must be the same as the vector space generated by those of A_m^{n+1} there is a solution if and only if the right column rank of the matrix A_m^n is the same as the right column rank of the augmented matrix A_m^{n+1}, i.e., by Theorem 1.2.6, if and only if the left row ranks are equal. Conversely, if the left row rank of A_m^{n+1} is equal to the left row rank of A_m^n, the right column ranks will be equal and the equations will have a solution. If the equations (1.2.5) have a solution, then any relation among the rows of A_m^n exists among the rows of A_m^{n+1}. For equations (1.2.5) this means that like combinations of equals are equal. Conversely, if each relation which exists among the rows of A_m^{n+1} also exists among the rows of A_m^n, then the left <u>(right) row rank of</u> A_m^{n+1} <u>is the same as the left (right)</u>

[1] $A_m^{n+1} = \left[A_m^n A^{(n+1)}\right]$, (cf. p.7 and line 4:p.10)

row rank of A_m^n. This proves the theorem.

THEOREM 1.2.8: *If in equations (1.2.5) $m = n$, then there exists a unique solution to (1.2.5) if and only if the corresponding homogeneous equations,*

$$(1.2.6) \qquad \begin{array}{l} a_{11}x_1 + a_{12}x_2 + \dots + a_{1n}x_n = 0, \\ \dots\dots\dots\dots\dots\dots\dots\dots\dots \\ a_{n1}x_1 + a_{n2}x_2 + \dots + a_{nn}x_n = 0, \end{array}$$

have only the trivial solution.

Proof: (1) Assume that the equations (1.2.6) have only the trivial solution. Then the column vectors of A_n^n are independent and A_n^n has rank n. Thus the rank of A_n^{n+1} is equal to the rank of A_n^n and by Theorem 1.2.7 equations (1.2.5) have at least one solution. If $A^{(1)}x_1 + \dots + A^{(n)}x_n = A^{(n+1)}$ has two distinct solutions X_i and Y_i then

$$A^{(1)}(X_1 - Y_1) + \dots + A^{(n)}(X_n - Y_n) = 0,$$

and $X_i - Y_i$ is a non-trivial solution of equations (1.2.6) contrary to our assumption. Thus equations (1.2.5) have exactly one solution.

(2) Now suppose that equations (1.2.5) have a unique solution X_i. Then $\sum_{i=1}^{n} A^{(i)}X_i = A^{(n+1)}$. If Y_i is a solution of (1.2.6), then $\sum_{i=1}^{n} A^{(i)}Y_i = 0$. Thus $\sum_{i=1}^{n} A^{(i)}(X_i + Y_i) = A^{(n+1)}$. But (1.2.5) has only one solution and thus $Y_i = 0$. Therefore (1.2.6) has only a trivial solution which completes the proof.

CHAPTER II

FIELD THEORY

2.1 Extension Fields.

Definition: If E is a field and F a subset of E which is a subfield of E then we call E an extension of F, designated by $F \subset E$.

Definition: If $\alpha, \beta, \ldots$, are elements of E, let $F(\alpha, \beta, \ldots)$ be the set of elements in E which can be expressed as quotients of polynomials in $\alpha, \beta, \ldots$, with coefficients in F. $F(\alpha, \beta, \ldots)$ is called the field obtained after the adjunction of the elements $\alpha, \beta, \ldots$ to F, or the field generated out of F by the elements $\alpha, \beta, \ldots$.

Obviously $F(\alpha, \beta, \ldots)$ is a field and is the smallest extension of F which contains the elements $\alpha, \beta, \ldots$. Henceforth, all fields will be assumed to be commutative fields. If $F \subset E$, then ignoring the multiplication operation defined between the elements in E, we may consider E as a vector space over F.

Definition: The degree of E over F, written (E/F), is the dimension of the vector space E over F. If (E/F) is finite, E is called a finite extension.

THEOREM 2.1.1: If F, B, E are three fields such that $F \subset B \subset E$, then $(E/F) = (E/B)\cdot(B/F)$.

Proof: Let (E/B) be r and let (B/F) be s. Now let

$b_1, b_2, \ldots, b_s$ be a basis of B over F. Thus

$$b_i = f_{i1}b_1 + \ldots + f_{is}b_s = \sum_{j=1}^{s} f_{ij}b_j$$

where b_i is any element of B. Also let $e_1, e_2, \ldots, e_r$ be a basis of E over B, that is, for any e belonging to E,

$$e = b_1 e_1 + \ldots + b_r e_r = \sum_{i=1}^{r} b_i e_i.$$

Thus any e belonging to E has the representation

$$e = (\sum_{j=1}^{s} f_{1j}b_j)e_1 + \ldots + (\sum_{j=1}^{s} f_{rj}b_j)e_r = \sum_{j=1}^{s}\sum_{i=1}^{r} f_{ij}b_j e_i.$$

Therefore every element e of E can be expressed as a linear combination of the rs elements $b_j e_i$. Now let $\sum_{i=1}^{r}\sum_{j=1}^{s} f_{ij}b_j e_i = 0$, where $f_{ij} \in F$. Thus

$$(\sum_{j=1}^{s} f_{1j}b_j)e_1 + \ldots + (\sum_{j=1}^{s} f_{rj}b_j)e_s = 0.$$

Since the e are independent then $\sum_{j=1}^{s} f_{ij}b_j = 0$ where $i = 1, \ldots, r$. But the b_j are independent over F and therefore $f_{ij} = 0$. Therefore the rs elements $b_j e_i$ are independent over F and they form a basis of E over F. Thus $(E/F) = (E/B).(B/F)$ which was to be established.

<u>Corollary</u>: <u>If</u> $F \subset F_1 \subset F_2 \subset \ldots \subset F_n$, <u>then</u> $(F_n/F) = (F_n/F_{n-1}).(F_{n-1}/F_{n-2}) \ldots (F_2/F_1).(F_1/F)$.

<u>2.2 Polynomials</u>.

<u>Definition</u>: An expression of the form $a_o x^n + a_1 x^{n-1} + \ldots + a_n$ is called a polynomial in F of degree n if the coefficients $a_o, \ldots, a_n$ are elements of the field F and a_o is not zero.

<u>Definition</u>: A polynomial in F is called reducible in F if it is equal to the product of two polynomials in F each of degree at least one. Polynomials which are not re-

ducible in F are called irreducible in F.

Multiplication and addition of polynomials are performed in the same manner as with field elements. In the set of all polynomials of degree lower than n, we include the zero polynomials, although they have no degree.

<u>Definition</u>: If $f(x) = g(x).h(x)$ is a relation which holds between the polynomials $f(x)$, $g(x)$, $h(x)$ in a field F, then we say that $g(x)$ divides $f(x)$ in F.

We see that the degree of $f(x)$, in the relation $f(x) = g(x).h(x)$, is equal to the sum of the degrees of $g(x)$ and $h(x)$. If neither $g(x)$ nor $h(x)$ is a constant then each has a degree less than the degree of $f(x)$. The division algorithm[1] holds for any two polynomials $f(x)$ and $g(x)$, that is, $f(x) = q(x)g(x) + r(x)$, where $q(x)$ and $r(x)$ are unique[2] polynomials in F and the degree of $r(x)$ is less than that of $g(x)$. Also $r(x)$, the remainder of $f(x)$, is the uniquely determined polynomial of a degree less than that of $g(x)$ such that $f(x) - r(x)$ is divisible by $g(x)$. It follows from the identity $f(x) \equiv (x - a)q(x) + r(x)$ that if a is a root of the polynomial $f(x)$ in F then $r(x) \equiv 0$ and $x - a$ is a factor of $f(x)$. As a consequence a polynomial in a field <u>cannot have more roots in the field than its degree.</u>

[1]Marie J. Weiss, Higher Algebra for the Undergraduate, ed. John Wiley and Sons (New York:1949), pg. 70.

[2]If F is not commutative $f(x) = g(x)q_1(x) + r_1(x)$ and $q_1(x)$ and $r_1(x)$ need not equal $q(x)$ and $r(x)$, respectively.[3]

[3]A.A.Albert, University of Chicago Press, (Chicago) 1947, pg. 24.

Lemma 2.2.1: The set S: $r(x)f(x) + s(x)g(x)$ where $f(x)$, $g(x)$ are fixed, consists of multiples of a fixed polynomial $m(x)$.

Proof: Let $m(x)$ be a polynomial of least degree such that $r(x)f(x) + s(x)g(x) = m(x)$ for a suitable choice of $r(x)$ and $s(x)$. Let

$$r_1(x)f(x) + s_1(x)g(x) = p(x) = m(x)q(x) + r(x),$$

where $r(x)$ has degree less than the degree of $m(x)$. Then

$$\left[r_1(x) - r(x)q(x)\right]f(x) + \left[s_1(x) - s(x)q(x)\right]g(x) = r(x).$$

Thus $r(x) \equiv 0$, which proves the lemma.

Lemma 2.2.2: If $(f(x),g(x)) = d(x)$ there exist polynomials $r(x)$, $s(x)$ such that $r(x)f(x) + s(x)g(x) = d(x)$.

Proof: As in Lemma 2.2.1 there exist an $r(x)$ and $s(x)$ such that $r(x)f(x) + s(x)g(x) = m(x)$. The set S contains $f(x)$ and $g(x)$ and hence $m(x)$ divides $f(x)$ and $m(x)$ divides $g(x)$. Since $d(x)$ divides $f(x)$ and $d(x)$ divides $g(x)$, therefore $d(x)$ divides $m(x)$. Thus $d(x)$ equals $m(x)$ which completes the proof.

THEOREM 2.2.3: If $p(x)$ is an irreducible polynomial over a field F and if $p(x)$ divides the product $f(x).g(x)$ of two polynomials over F, then $p(x)$ divides $f(x)$ or $p(x)$ divides $g(x)$.

Proof: Suppose $p(x)$ does not divide $f(x)$. Since $p(x)$ is irreducible over F, its only divisors are its associates[1] and the units[2] of the field. Thus $(p(x),f(x)) = 1$. By Lemma 2.2.2 there exist polynomials $r(x)$, $s(x)$ such that

[1] Two elements of a ring are called associates if each divides the other.

[2] A unit is any associate of 1.

if 1 is the unity element of F then

$$(2.2.1) \qquad 1 = r(x)f(x) + s(x)p(x).$$

Multiply equation (2.2.1) by $g(x)$. Then

$$(2.2.2) \qquad g(x) = r(x)f(x)g(x) + s(x)p(x)g(x).$$

Since $p(x)$ divides the right side of equation (2.2.2), $p(x)$ divides $g(x)$. Similarly, if $p(x)$ does not divide $g(x)$ then $p(x)$ divides $f(x)$, which completes the proof.

We see that if $p(x)$ is an irreducible polynomial over F, then $p(x)$ does not divide the product of two polynomials over F, each of whose degree is less than the degree of $p(x)$, since the only divisors of $p(x)$ would be its associates and units of the field F.

<u>THEOREM 2.2.4</u>: <u>A polynomial $f(x)$ of positive degree over a field F can be expressed as an element of F times a product of monic[1] irreducible polynomials over F. This decomposition is unique except for the order in which the factors occur.</u>

<u>Proof</u>: If $f(x)$ is irreducible, the decomposition is accomplished. Now let $f(x) = g(x) \cdot h(x)$. Then $g(x)$ and $h(x)$ are polynomials of degree less than the degree of $f(x)$. We make the inductive assumption that the decomposition is possible for all polynomials of degree less than that of $f(x)$. Thus

$$g(x) = cp_1(x) \cdot p_2(x) \cdot \ \ldots \ \cdot p_r(x),$$

and

$$h(x) = dq_1(x) \cdot q_2(x) \cdot \ \ldots \ \cdot q_s(x),$$

---

[1] $a_n x^n + a_{n-1}x^{n-1} + \ldots + a_o$ is monic if $a_n = 1$.

where c,d are in F and where $p_i(x)$ and $q_j(x)$ are monic irreducible polynomials over F. We have then

$$f(x) = g(x)h(x) = cdp_1(x) \ \ldots \ p_r(x)q_1(x) \ \ldots \ q_s(x).$$

Thus the induction is completed and the decomposition is accomplished. Now to show that the decomposition is unique suppose there exists two decompositions

$$f(x) = cp_1(x) \ \ldots \ p_n(x) = dq_1(x) \ \ldots \ q_m(x).$$

Since the irreducible polynomials are monic then c equals d. Since $p_1(x)$ is irreducible it divides some $q_j(x)$. As both $p_1(x)$ and $q_j(x)$ are monic their quotient is the unity element of F, and hence $p_1(x) = q_j(x)$. Thus we obtain

$$f_1(x) = p_2(x)\ldots p_n(x) = q_1(x)\ldots q_{j-1}(x)\cdot q_{j+1}(x)\ldots q_m(x).$$

Now $f_1(x)$ is of degree less than the degree of f(x). We make the inductive assumption that all polynomials of degree less than that of f(x) have a unique decomposition. Thus $f_1(x)$ has a unique decomposition, m = n, and therefore f(x) has a unique decomposition into the product of irreducible polynomials which proves the theorem.

<u>Lemma 2.2.5</u>: <u>With regard to division by f(x), the remainder of the product of the remainders of two polynomials is the remainder of the product of these two polynomials</u>.

<u>Proof</u>: Let $g_1(x) = q_1(x)f(x) + r_1(x)$ and $g_2(x) = q_2(x)f(x) + r_2(x)$ be the two polynomials. Then

$$r_1(x)r_2(x) = \left[q_1(x)q_2(x)f(x) - g_1(x)q_2(x) - g_2(x)q_1(x)\right]f(x) + g_1(x)g_2(x).$$

Let $g_1(x)g_2(x) = q(x)f(x) + r(x)$. Thus

$$r_1(x)r_2(x) = \left[q_1(x)q_2(x)f(x) - g_1(x)q_2(x) - g_2(x)q_1(x) + q(x)\right]f(x) + r(x),$$

2.3 Algebraic Elements.

Definition: If α is an element of an extension field of F, and if there are polynomials with coefficients in F which have α as root then α is called algebraic with respect to F. If α is not algebraic it is called transcendental with respect to F.

Lemma 2.3.1: Let α be algebraic and select among all monic polynomials in F which have α as root, one, $f(x)$, of least degree. Then $f(x)$ is uniquely determined, is irreducible, and each polynomial in F with the root α is divisible by $f(x)$.

Proof: Let $g(x)$ be any polynomial in F with $g(\alpha) = 0$. We may divide $g(x)$ by $f(x)$, and write $g(x) = f(x)q(x) + r(x)$ where the degree of $r(x)$ is less than that of $f(x)$. Substituting $x = \alpha$ we get $r(\alpha) = 0$. Since the degree of $r(x)$ is less than the degree of $f(x)$, $r(x) \equiv 0$, and $g(x)$ is divisible by $f(x)$. This also shows that $f(x)$ is unique. If $f(x)$ were reducible, one of the factors would have to vanish for $x = \alpha$ contradicting again the choice of $f(x)$.

We consider now the subset E_0 of the following elements θ of E:

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

where $g(x)$ is a polynomial in F of degree less than n, the degree of $f(x)$. We note that the constants $c_0, c_1, \ldots, c_{n-1}$ are uniquely determined by the element θ, since two expressions for the same θ would lead after subtracting to an equation for α of lower degree than n.

<u>Lemma 2.3.2</u>: <u>E_0 is a field</u>.

<u>Proof</u>: Let $g(x)$ and $h(x)$ be two polynomials of degree less than n. Thus

$$g(\alpha) + h(\alpha) = (c_0 + c_1\alpha + \ldots + c_{n-1}\alpha^{n-1}) + (d_0 + d_1\alpha + \ldots + d_{n-1}\alpha^{n-1}) = b_0 + b_1\alpha + \ldots + b_{n-1}\alpha^{n-1} = k(\alpha)$$

which is also a polynomial of degree less than n. Thus E_0 is closed under addition. Now considering $g(x)$ and $h(x)$ again we put $g(x)h(x) = q(x)f(x) + r(x)$ and hence $g(\alpha)h(\alpha) = r(\alpha)$. Therefore E_0 is closed under multiplication. Now let $h(\alpha) \neq 0$ so that $(h(x), f(x)) = 1$. By Lemma 2.2.2 there exist polynomials $a(x)$, $b(x)$ such that $a(x)h(x) + b(x)f(x) = 1$. Thus $a(\alpha)h(\alpha) = 1$ and we may assume that the degree of $a(x)$ is less than n for we may replace $a(x)$ by its remainder after division by $f(x)$. Hence, $h(\alpha)$ has an inverse $a(\alpha)$. Thus E_0 is a field, which completes the proof.

Since the space $F(\alpha)$ is generated by the linearly independent $1, \alpha, \alpha^2, \ldots, \alpha^{n-1}$ the degree $[F(\alpha)/F]$ is n. We shall see that the internal structure of the field $E_0 = F(\alpha)$ depends not on the nature of α but only on the irreducible $f(x)$.

<u>THEOREM 2.3.3</u>: <u>(Kronecker) Given a polynomial</u>

<u>$p(x)$ with coefficients in a field F, there exists an extension field $E \supseteq F$ in which $p(x) = 0$ has a root</u>.

<u>Proof</u>: Let $f(x) = x^n + b_{n-1}x^{n-1} + \dots + b_o$ be an irreducible polynomial of $p(x)$. We select a symbol s and let E_1 be the set of all formal polynomials $g(s) = c_o + c_1 s + \dots + c_{n-1}s^{n-1}$ of a degree lower than n. This set forms a group under addition. Besides the ordinary multiplication we introduce a new multiplication $\otimes$ of two elements $g(s)$ and $h(s)$ of E_1 denoted by $g(s) \otimes h(s)$. It is defined as the remainder $r(s)$ of the ordinary product $g(s)h(s)$ under division by $f(s)$. Also the product of m terms $g_1(s), g_2(s), \dots, g_m(s)$ is again the remainder of the ordinary product $g_1(s) g_2(s) \dots g_m(s)$ by Lemma 2.2.5. This shows that our new product is associative and commutative and that the new product $g_1(s) \otimes g_2(s) \otimes \dots \otimes g_m(s)$ will coincide with the old product $g_1(s)g_2(s)\dots g_m(s)$ if the latter does not exceed n in degree.

The set E_1 contains our field F and our multiplication in E_1 has for F the meaning of the old multiplication. One of the polynomials of E_1 is s. The product of i factors each of which is s will lead to s^i if $i < n$. For $i = n$ this is not the case since it leads to the remainder of the polynomial s^n. This remainder is

$$s^n - f(s) = - b_{n-1}s^{n-1} - b_{n-2}s^{n-2} - \dots - b_o.$$

We now give up our old multiplication altogether and keep only the new one. We also change our notation, using the point as a symbol for the new multiplication. Computing in this sense we can construct the element

$$c_o + c_1 . s + c_2 . s^2 + \dots + . c_{n-1} . s^{n-1}$$

since all the degrees involved are below n. But

$$s^n = - b_{n-1} . s^{n-1} - b_{n-2} . s^{n-2} - \dots - b_o .$$

Transposing we see that $f(s) = 0$.

We thus have constructed a set E_1 and an addition and multiplication in E_1. Now E_1 contains F as subfield and s satisfies the equation $f(s) = 0$. We have to show that if $g(s) \neq 0$ and $h(s)$ are given elements of E_1, there is an element

$$X(s) = x_o + x_1 . s + \dots + x_{n-1} . s^{n-1}$$

in E_1 such that

$$g(s) . X(s) = h(s).$$

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

$$L_o = d_o, L_1 = d_1, \dots, L_{n-1} = d_{n-1}$$

where the d_i are the coefficients of $h(s)$. By Theorem 1.2.7 this system will be uniquely solvable if the corresponding homogeneous equations

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

have only the trivial solution.

The homogeneous problem would occur if we should ask for the set of elements $X(s)$ satisfying $g(s).X(s) = 0$. Considering the old multiplication this would mean that the product $g(s)X(s)$ had the remainder zero, and is thus divisible by $f(s)$. By Theorem 2.2.3 this is only possible for $X(s) = 0$. Therefore E_1 is a field. Thus we have constructed an extension field $E_1 = F(s)$ in which an irreducible factor $f(x)$ of $p(x)$ has a root. This completes the proof of our theorem.

Now consider our old extension E with a root α of $f(x)$, leading to the set E_o. We see that E_o has, in a certain sense, the same structure as E_1, if we map the element $g(s)$ of E_1 onto the element $g(\alpha)$ of E_o. This mapping will have the property that the image of a sum of elements is the sum of their images, and the image of a product is the product of their images.

2.4 Homomorphism, Isomorphism, Automorphism.

Definition: By a homomorphism of a multiplicative group we mean a (possibly many-to-one) mapping T such that for a,b any two elements of G, $T(a).T(b) = T(a.b)$.

Definition: A mapping T of one field on another which is one-to-one such that $T(a + b) = T(a) + T(b)$ and $T(a.b) = T(a).T(b)$ is called an isomorphism.

Definition: The isomorphism T of a field on itself is called an automorphism.

Definition: If not every element of the image field is the image under T of an element in the first field, then T is called an isomorphism of the first field *into* the second.

We will consistently use the term "mapping of F *on* F'" when every element of F' is the image of an element of F, and the term "mapping of F *into* F'" if at least one element of F' is not the image of an element of F.

THEOREM 2.4.1: *Let T be an isomorphism mapping a field F on a field F'. Let f(x) be an irreducible polynomial in F and f'(x) the corresponding polynomial in F'. If $E = F(\alpha)$ and $E' = F'(\alpha')$ are extensions of F and F', respectively, where $f(\alpha) = 0$ in E and $f'(\alpha') = 0$ in E', then T can be extended to an isomorphism between E and E'.*

Proof: Since isomorphisms are transitive and E and E' are both isomorphic to E_1, (cf. Theorem 2.3.3), therefore, E is isomorphic to E'.

CHAPTER III

GALOIS THEORY

3.1 Splitting Fields.

Definition: If F, B, E are three fields such that $F \subset B \subset E$, then we call B an intermediate field.

Definition: If E is an extension of a field F in which a polynomial $p(x)$ can be factored into linear factors, and if $p(x)$ can not be so factored in any intermediate field, then E is called a splitting field for $p(x)$.

Lemma 3.1.1: If E is a splitting field of $p(x)$, the roots of $p(x)$ generate E, where the coefficients of $p(x)$ belong to a field F.

Proof: If $p(x)$ of degree n splits in E then $p(x)$ splits into linear factors $(x - p_1)(x - p_2)\ldots(x - p_n)$. If only one root of $p(x)$, say p_1 lies outside F then $E = F(p_1)$ and thus p_1 would generate E. Similarly if $p_1, p_2, \ldots, p_n$ are outside F then $F(p_1, p_2, \ldots, p_n) = E$. Thus the roots of $p(x)$ generate E.

Lemma 3.1.2: A splitting field E is of finite degree.

Proof: Since E is constructed by a finite number of adjunctions of algebraic elements, each defining an extension field of finite degree, by the Corollary to Theorem 2.1.1, the total degree of E is finite.

THEOREM 3.1.3: If $p(x)$ is a polynomial in a field F, there exists a splitting field E of $p(x)$.

Proof: We factor $p(x)$ in F into irreducible factors $f_1(x) \cdot f_2(x) \cdot \ldots \cdot f_r(x) = p(x)$. If each of these factors is of the first degree then F itself is the required splitting field. Suppose then that $f_1(x)$ is of degree higher than the first. By Theorem 2.3.3 there is an extension F_1 of F in which $f_1(x)$ has a root. Factor each of the factors $f_1(x)$, $\ldots, f_r(x)$ into irreducible factors in 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 F by the roots of $p(x)$ is the required splitting field.

Lemma 3.1.4: If $f(x)$ is an irreducible factor of $p(x)$ in F, then E contains a root of $f(x)$.

Proof: Let $p(x) = (x - \alpha_1)(x - \alpha_2)\ldots(x - \alpha_s)$ be the splitting of $p(x)$ in E. Then $(x - \alpha_1)(x - \alpha_2)\ldots(x - \alpha_s) = f(x)g(x)$. We consider $f(x)$ as a polynomial in E and construct the extension field $B = E(\alpha)$ in which $f(\alpha) = 0$. Then $(\alpha - \alpha_1)(\alpha - \alpha_2)\ldots(\alpha - \alpha_s) = f(\alpha) \cdot g(\alpha) = 0$ and $\alpha - \alpha_i$ being elements of the field B can have a product equal to zero only if for one of the factors, say the first, we have $\alpha - \alpha_1 = 0$. Thus $\alpha = \alpha_1$, and α_1 is a root of $f(x)$.

THEOREM 3.1.5: Let T be an isomorphic mapping of the field F on the field F'. Let $p(x)$ be a polynomial in F and $p'(x)$ the polynomial in F' with coefficients corresponding to those of $p(x)$ under T. Finally, let E be a splitting *field of p(x) and E' a splitting field of p'(x). Under these conditions the isomorphism T can be extended to an isomorphism between E and E'.*

Proof: In case all roots of p(x) are in F, then $E = F$ and p(x) can be split in F. This factored form has an image in F' which is a splitting of p'(x), since the isomorphism T 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 F', we must have $F' = E'$. In this case, T itself is the required extension and the theorem is proved if all the roots of p(x) are in F. We proceed by induction. We suppose the theorem proved for all cases in which the number of roots of p(x) outside F is less than $n > 1$, and we also suppose that p(x) is a polynomial having n roots outside F. We factor p(x) into irreducible factors in F; $p(x) = f_1(x) \cdot f_2(x) \ldots f_m(x)$. Not all of these factors can be of degree 1, since in this case p(x) would split in F, contrary to our assumption. Hence, we may suppose the degree of $f_1(x)$ to be $r > 1$. Let $f_1'(x) \cdot f_2'(x) \ldots f_m'(x) = p'(x)$ be the factorization of p'(x) into the polynomials corresponding to $f_1(x), \ldots, f_m(x)$ under T. Now f'(x) is irreducible in F', for a factorization of f'(x) in F' would induce under T^{-1}, the inverse of T, a factorization of $f_1(x)$, which was taken to be irreducible. By Lemma 3.1.4, E contains a root α of $f_1(x)$ and E' contains a root α' of f'(x).

By Theorem 2.4.1, the isomorphism T can be extended to an isomorphism T_1, between the fields $F(\alpha)$ and $F'(\alpha')$. Since $F \subset F(\alpha)$, $p(x)$ is a polynomial in $F(\alpha)$ and E is a splitting field for $p(x)$ in $F(\alpha)$. Similarly for $p'(x)$. There are now less than n roots of $p(x)$ outside the new ground field $F(\alpha)$. Hence by our inductive assumption T_1 can be extended from an isomorphism between $F(\alpha)$ and $F'(\alpha')$ to an isomorphism T_2 between E and E'. Since T_1 is an extension of T, and T_2 is an extension of T_1, we conclude that T_2 is an extension of T and the theorem follows.

Corollary: If $p(x)$ is a polynomial in a field F, then any two splitting fields for $p(x)$ are isomorphic.

Proof: From Theorem 3.1.5 take $F = F'$ and T to be the identity mapping, that is, $T(x) = x$.

From this corollary we may use 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, it will have repeated roots in any other splitting field.

3.2 Finite Fields[1]

Definition: A field which has a finite number of elements is called a finite field.

Definition: The order of an element A of a finite group G is the least positive integer a such that $A^a = e$,

[1] A further discussion of the algebra of finite fields is to be found in Chapter VIII.

where e is the unity element of G.

<u>Lemma 3.2.1: Let A have order a, then $A^c = e$ implies $a \mid c$.</u>

<u>Proof</u>: Let $c = aq + r$, $0 \leq r < a$. Then $A^c = A^{aq+r} = (A^a)^q A^r = (e)^q A^r = A^r$. Thus if $A^c = e$, $r = 0$ and therefore $c = aq$.

<u>Lemma 3.2.2: If $(a,b) = 1$, and A has order a, B has order b, then AB has order ab.</u>

<u>Proof</u>: Let $AB = C$, have order c. Suppose $c = aq + r$, $0 \leq r < a$. Then $e^b = C^{cb} = C^{(aq+r)b} = A^{(aq+r)b}B^{(aq+r)b} = A^{rb}$. Thus by Lemma 3.2.1 $a \mid rb$. But, since $(a,b) = 1$, $a \mid r$. Therefore $r = 0$. Thus $a \mid c$. Similarly $b \mid c$ and therefore $ab \mid c$. But $(C)^{ab} = (AB)^{ab} = A^{ab}B^{ab} = (A^a)^b(B^b)^a = e$. Thus $c \mid ab$. Therefore $c = ab$.

<u>Lemma 3.2.3: 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.</u>

<u>Proof</u>: If d divides a, we have an element $A^{a/d}$ which is an element of order d in the group. Let $p_1, p_2, \ldots, p_r$ be the prime numbers dividing either a or b and let $a = p_1^{n_1} p_2^{n_2} \ldots p_r^{n_r}$, $b = p^{m_1} p^{m_2} \ldots p^{m_r}$. Now call t_i the larger of n_i and m_i. Then $c = p_1^{t_1} p_2^{t_2} \ldots p_r^{t_r}$. 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 $p_i^{t_i}$. Lemma 3.2.2 shows that the product of these elements will have the desired order c.

Lemma 3.2.4: If there is an element C in an abelian group whose order c is maximal then the order a of every element A in the group divides c. Hence $x^c = e$ is satisfied by each element in the group.

Proof: If a does not divide c, the greatest common multiple of a and c would be larger than c and by Lemma 3.2.3 we could find an element of that order, thus contradicting the choice of c.

THEOREM 3.2.5: If S is a finite subset ($\neq 0$) of a field F which is a group under multiplication in F, then S is a cyclic group.

Proof: Let n be the number of distinct elements of S and r the largest order occurring in S. Then $x^r - 1 = 0$ is satisfied for all elements of S. Since this polynomial of degree r in the field cannot have more than r roots, it follows that $r \geq n$. Each element of S generates a cyclic subgroup of S whose order divides n, and since the order of each element of the group divides n, $r \leq n$. Thus $r = n$. Therefore S is a cyclic group consisting of $1, a^1, a^2, \ldots, a^{n-1}$ where $a^n = 1$, which proves our theorem.

Corollary: The non-zero elements of a finite field F form a cyclic group.

Proof: Since the non-zero elements of a finite field F form a finite group under multiplication in F then by Theorem 3.2.5 they form a cyclic group.

Definition: If G is an additive abelian group (with group operation written $+$) then the elements $g_1,\ldots,g_k$ will be said to generate G if each element g of G can be written as sum of multiples of $g_1,\ldots,g_k$, $g = n_1g_1 + \ldots + n_kg_k$.

<u>Definition</u>: If no set of fewer than k elements generate G, then $g_1,\ldots,g_k$ is called a minimal generating system.

Any group which has a finite generating system will have a minimal generating system. A finite group always has a minimal generating system. Since

$$n_1g_1 + n_2g_2 = n_1(g_1 + mg_2) + (n_2 - n_1m)g_2$$

it follows that if $g_1,g_2,\ldots,g_k$ generate G, then also $g_1 + mg_2,g_2,\ldots,g_k$ generate G.

<u>Definition</u>: An equation $m_1g_1 + m_2g_2 + \ldots + m_kg_k = 0$ will be called a relation among the generators where $m_1,\ldots,m_k$ are called coefficients in the relation.

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

<u>THEOREM 3.2.6</u>: <u>Each abelian group having a finite number of generators is the direct product of cyclic subgroups</u> $G_1,\ldots,G_n$ <u>where n is the number of elements in a minimal generating system, and where</u> $O(G_i)$ <u>divides</u> $O(G_{i+1})$ <u>for</u> $i = 1,2,\ldots,r-1$, <u>if</u> $G_1,\ldots,G_r$, $2 \leq r \leq n$, <u>are finite</u>.

<u>Proof</u>: We assume the theorem true for all groups having minimal generating systems of k-1 elements. If

$n = 1$ the group is cyclic and the theorem is trivial. Now suppose G is an abelian group having a minimal generating system of k elements. If every minimal generating system satisfies only a trivial relation, then let $g_1, g_2, \ldots, g_k$ be a minimal generating system and let G_i, be the cyclic group generated by g_i. For each $g \in G$, $g = n_1 g_1 + \ldots + n_k g_k$ where the expression is unique; otherwise we should obtain a non-trivial relation. Moreover, the cyclic groups G are all infinite, since $ng_i = 0$ would yield a non-trivial relation. Thus the theorem would be true. We assume now that a non-trivial relation holds for some minimal generating system. Of all the relations belonging to minimal generating systems, let

(3.2.1) $$m_1 g_1 + \ldots + m_k g_k = 0$$

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

(3.2.2) $$n_1 g_1 + \ldots + n_k g_k = 0$$

we must have $m_1 | n_1$. Otherwise $n_1 = qm_1 + r$, $0 < r < m_1$, and q times relation (3.2.1) subtracted from relation (3.2.2) would give a relation with a positive coefficient $r < m_1$. Also in the relation (3.2.1) we must have $m_1 | m_i$, $i = 2, \ldots, k$. For if m_1 does not divide one coefficient, say m_2, then $m_2 = q_2 m_1 + r$, $0 < r < m_1$. In the generating system $g_1 + q_2 g_2, g_2, \ldots, g_k$ we would then have a relation

$m_1(g_1 + q_2g_2) + rg_2 + m_3g_3 + \dots + m_kg_k = 0$ where the coefficient r contradicts the choice of m_1. Hence $m_2 = q_2m_1$, $m_3 = q_3m_1, \dots, m_k = q_km_1$. The system

$$\bar{g}_1 = g_1 + q_2g_2 + \dots + q_kg_k, g_2, g_3, \dots, g_k$$

is minimal generating, and $m_1\bar{g}_1 = 0$. In any relation $0 = n_1\bar{g}_1 + n_2g_2 + \dots + n_kg_k$, since n_1 is a coefficient in a relation between $\bar{g}_1, g_2, \dots, g_k$, our previous argument gives $m_1 \mid n_1$, and hence $n_1\bar{g}_1 = 0$. Let G' be the subgroup of G generated by $g_2, \dots, g_k$ and G_1 the cyclic group of order m_1 generated by $\bar{g}_1$. Then G is the direct product of G_1 and G'. Each element g of G can be written

$$g = n_1\bar{g}_1 + n_2g_2 + \dots + n_kg_k = n_1\bar{g}_1 + g', \ 0 \leq n_1 < m_1.$$

This 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 $(n_1 - n_1')\bar{g}_1 = 0$, so that $n_1 - n_1' = 0$ and also $g' = g''$. By our induction assumption, G' is the direct product of k - 1 cyclic groups $\bar{G}_i$ generated by elements $\bar{g}_2, \bar{g}_3, \dots, \bar{g}_k$. Moreover, if $\bar{G}_2, \bar{G}_3, \dots, \bar{G}_r$ are finite, and $3 \leq r \leq k-1$, their respective orders $t_2, \dots, t_r$ satisfy $t_i \mid t_{i+1}$, $i = 2, \dots, r-1$. If $\bar{G}_2$ is finite the preceding argument applied to the generators $\bar{g}_1, \bar{g}_2, \dots, \bar{g}_k$ gives $m_1 \mid t_2$, from which the theorem follows.

<u>Definition</u>: If a is an element of a field F, we denote the n-fold of a, that is, the sum of n terms, each of which is a, by n.a.

Now n.(m.a) = (nm).a and (n.a)(m.b) = nm.ab. If for one element $a \neq 0$, there is an integer n such that $n.a = 0$ then $n.b = 0$ for each b in F, since $n.b = (n.a)(a^{-1}b) = 0(a^{-1}b) = 0$.

<u>Definition</u>: If there is a positive integer p such that $p.a = 0$ for each a in F, and if p is the smallest integer with this property, then F is said to have the characteristic p, but if no such positive integer p exists then we say F has the characteristic 0 or ∞.

<u>Lemma 3.2.7</u>: <u>The characteristic</u> p <u>of a finite field</u> F <u>is always a prime number which divides the order of any non-zero</u> a <u>of</u> F.

<u>Proof</u>: If $p = rs$ then $p.a = rs.a = r.(s.a)$. But $s.a = b \neq 0$ if $a \neq 0$ and $r.b \neq 0$ since r and s are less than p, so that $p.a \neq 0$ contrary to the definition of the characteristic. If $n.a = 0$ for $a \neq 0$, then p divides n, for $n = qp + r$ where $0 \leq r < p$ and $n.a = (qp + r).a = q.(p.a) + r.a$. Hence $n.a = 0$ implies $r.a = 0$, and since $r < p$, we must have $r = 0$.

<u>Lemma 3.2.8</u>: <u>If</u> F <u>is a finite field having</u> q <u>elements and</u> E <u>an extension of</u> F <u>such that</u> $(E/F) = n$, <u>then</u> E <u>has</u> q^n <u>elements</u>.

<u>Proof</u>: If $\omega_1, \omega_2, \ldots, \omega_n$ is a basis of E over F, each element of E can be uniquely represented as a linear combination

$$x_1\omega_1 + x_2\omega_2 + \ldots + x_n\omega_n,$$

where the x_i belong to F. Since each x_i can assume q values in F, there are q^n distinct possible choices of $x_1,\ldots,x_n$ and hence q^n distinct elements of E.

Lemma 3.2.9: If F is a finite field and $(E/F) = n$, there is an element α of E so that $E = F(\alpha)$.

Proof: Since E is finite, Theorem 3.2.5 shows that the non-zero elements of E form a cyclic group generated by some element α. This completes the proof.

Lemma 3.2.10: The order of any finite field F is a power of its characteristic.

Proof: Let $P \equiv [0,1,2,\ldots,p-1]$ denote the set of multiples of the unit element in a field F of characteristic p. Then P is a subfield of F having p distinct elements, and P is isomorphic to the field of integers reduced modulo p. Let $(F/P) = n$, then by Lemma 3.2.8 F contains p^n elements.

THEOREM 3.2.11: Two finite fields having the same number of elements are isomorphic.

Proof: If F and F' are two finite fields having the same order q, then by Lemma 3.2.10, they have the same characteristic since q is a power of the characteristic. The multiples of the units in F and F' form two fields P and P' which are isomorphic. The non-zero elements of F and F' form a group of order q-1 and, thus, satisfy $x^{q-1} - 1 = 0$. The fields F and F' are splitting fields of the equation $x^{q-1} = 1$ considered as lying in P and P' respectively. By Theorem 3.1.5 the isomorphism between P and P' can be extended to an isomorphism between F and F' which proves the theorem.

Definition: If $f(x) = a_0 + a_1x^1 + \ldots + a_nx^n$ is a polynomial in a field F, then the formal derivative of f is $f' = a_1 + 2.a_2x^1 + \ldots + n.a_nx^{n-1}$.[1]

For each pair of polynomials f and g we show that

(i) $(f + g)' = f' + g'$,

(ii) $(fg)' = fg' + gf'$,

(iii) $(f^n)' = nf^{n-1}f'$.

For (i) if $f = a_0 + a_1x^1 + \ldots + a_nx^n$ and $g = b_0 + b_1x^1 + \ldots + b_mx^m$ then if $n > m$ we have

$$(f + g) = \big[(a_0 + b_0) + (a_1 + b_1)x + \ldots + (a_m + b_m)x^m + a_{m+1}x^{m+1} + \ldots + a_nx^n\big].$$

Now

$$(f + g)' = (a_1 + b_1) + 2(a_2 + b_2)x + \ldots + m(a_m + b_m)x^{m-1} + \ldots + na_nx^{n-1} = a_1 + 2a_2 + \ldots + na_nx^{n-1} + b_1 + 2b_2x + \ldots + mb_mx^{m-1} = f' + g'.$$

For (ii) let $f = \sum_{i=0}^{m} a_ix^i$, $g = \sum_{j=0}^{n} b_jx^j$. Then $(fg) = \sum_{i=0}^{m}\sum_{j=0}^{n} a_ib_jx^{i+j}$. Now $(fg)' = (\sum_{i=0}^{m}\sum_{j=0}^{n} a_ib_jx^{i+j})' = \sum_{i=0}^{m}\sum_{j=0}^{n} (i + j)a_ib_jx^{i+j-1}$. Also $f'g + fg' = \sum_{i=0}^{m}\sum_{j=0}^{n} ia_ix^{i-1}b_jx^j + \sum_{i=0}^{m}\sum_{j=0}^{n} ja_ix^ib_jx^{j-1} = \sum_{i=0}^{m}\sum_{j=0}^{n}(i + j)a_ib_jx^{i+j-1}$. Therefore $(fg)' = f'g + fg'$.

For (iii) $(f^n)' = nf^{n-1}f'$ is true for $n = 1$. Proceeding by induction, we assume it is true for $n = k$, that is, $(f^k)' = kf^{k-1}f'$. We wish to show that (iii) holds for

[1]We will write na for n.a from now on.

$n = k + 1$. Now $(f^{k+1})' = (ff^k)' = f(f^k)' + f^k f' = fkf^{k-1}f' + f^k f' = (k+1)f^k f'$. Thus by induction $(f^n)' = nf^{n-1}f'$.

Definition: If $f(x)$ is a polynomial in F, then $f(x)$ is called separable if its irreducible factors do not have repeated roots.

Definition: If E is an extension of the field F, the element α of E is called separable if it is a root of a separable polynomial $f(x)$ in F, and E is called a separable extension if each element of E is separable.

THEOREM 3.2.12: The polynomial f has repeated roots if and only if in the splitting field E the polynomials f and f' have a common root; or equivalently, if and only if f and f' have a common factor of degree greater than zero in F.

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

$$f' = (x-\alpha)^k Q'(x) + k(x-\alpha)^{k-1}Q(x) = (x-\alpha)^{k-1}\left[(x-\alpha)Q'(x) + kQ(x)\right].$$

If $k > 1$, then α is a root of f' of multiplicity at least $k-1$. If $k = 1$, then $f'(x) = Q(x) + (x-\alpha)Q'(x)$ and $f'(\alpha) = Q(\alpha) \neq 0$. Thus, f and f' have a root α in common if and only if α is a root of f of multiplicity greater than 1. If f and f' have a root α in common then the irreducible polynomial in F having α 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' which proves the theorem.

Corollary: If F is a field of characteristic zero

<u>then each irreducible polynomial in F is separable.</u>

<u>Proof</u>: Suppose the irreducible polynomial $f(x)$ has a root α of multiplicity greater than 1. Then, $f'(x)$ is a polynomial which is not identically zero for its leading coefficient is a multiple of the leading coefficient of $f(x)$ and is not zero since the characteristic is 0. Also $f'(x)$ is of degree 1 less than the degree of $f(x)$. But α is also a root of $f'(x)$ which contradicts the irreducibility of $f(x)$.

<u>3.3 Group Characters</u>.

<u>Definition</u>: If G is a multiplicative group, F a field and T a homomorphism mapping G into F(i.e., $G \rightarrow G' \subset F$), then T is called a <u>character</u> of G in F.

Let $a \in G$, $a \neq 0$. If $T_1(a) = 0$, $T_1(e) = T_1(a)T_1(a^{-1}) = 0$. Therefore $T_1(g) = T_1(e)T_1(g) = 0$ for all g of G. We will assume $T_1(a) \neq 0$ in the following discussion, i.e., T_1 is a non-trivial mapping.

<u>Definition</u>: The characters $T_1, T_2, \ldots, T_n$ are called <u>dependent</u> if there exist elements $b_1, b_2, \ldots, b_n$, not all zero, in F such that

(3.3.1) $\quad b_1T_1(x) + b_2T_2(x) + \ldots + b_nT_n(x) = 0$

for each x belonging to G. The dependence relation (3.3.1) is called non-trivial. If the characters are not dependent they are called <u>independent</u>.

<u>THEOREM 3.3.1</u>: <u>If G is a group and</u> $T_1, T_2, \ldots, T_n$ <u>are n mutually distinct characters of G into F, the</u> $T_1, T_2, \ldots, T_n$ <u>are independent</u>.

Proof: One character cannot be dependent, since $b_1T_1(x) = 0$ implies $b_1 = 0$ due to the assumption that $T_1(a) \neq 0$. Suppose $n > 1$. We make the inductive assumption that no set of less than n distinct characters is dependent and we wish to show that n characters are independent. For each a in G, let

$$\sum_{i=1}^{n} b_i T_i(x) = 0 \tag{3.3.1}$$

where b_i and $T_i(x)$ belong to F. If $b_n = 0$ then by our inductive assumption $b_1 = b_2 = b_3 = \dots = b_{n-1} = b_n = 0$. In (3.3.1) if $b_n \neq 0$ we replace x by ax where a is any element of G such that $T_{n-1}(a) \neq T_n(a)$.

Then

$$b_1T_1(a)T_1(x) + \dots + b_{n-1}T_{n-1}(a)T_{n-1}(x) + b_nT_n(a)T_n(x) = 0$$

while

$$b_1T_n(a)T_1(x) + \dots + b_{n-1}T_n(a)T_{n-1}(x) + b_nT_n(a)T_n(x) = 0.$$

By our induction assumption, the coefficient of $T_{n-1}(x)$, i.e. $b_{n-1}\left[T_{n-1}(a) - T_n(a)\right]$, in the difference of these two equations will be zero. Thus $b_{n-1} = 0$. But then the relation $b_1T_1(x) + \dots + b_{n-2}T_{n-2}(x) + b_nT_n(x) = 0$ implies $b_1 = b_2 = \dots = b_{n-2} = b_n = 0$, too. Thus the T_i are independent, and the theorem is proved.

Corollary: If E and E' are two fields, and $T_1, T_2, \dots, T_n$ are n mutually distinct isomorphisms mapping E into E', then $T_1, T_2, \dots, T_n$ are independent.

Proof: This follows from Theorem 3.3.1, since E without the 0 is a group and the T's defined in this group are mutually distinct characters.

Definition: If $T_1, T_2, \ldots, T_n$ are isomorphisms of a field E into a field E', then each element a of E such that $T_1(a) = T_2(a) = \ldots = T_n(a)$ is called a fixed point of E under $T_1, T_2, \ldots, T_n$. When $E = E'$, the T's are automorphisms, and if T_1 is the identity, that is, $T_1(x) = x$, we have $T_i(x) = x$, $i = 1, \ldots, n$, for a fixed point.

Lemma 3.3.2: The set of fixed points of E under $T_1, \ldots, T_n$ is a subfield F of E.

Proof: If a and b are fixed points $a, b \in F$, then

$$T_i(a \pm b) = T_i(a) \pm T_i(b) = T_j(a) \pm T_j(b) = T_j(a \pm b)$$

and $a \pm b \in F$. Similarly,

$$T_i(a.b) = T_i(a).T_i(b) = T_j(a).T_j(b) = T_j(a.b).$$

Finally, we have

$$T_i(a^{-1}) = (T_i(a))^{-1} = (T_j(a))^{-1} = T_j(a^{-1}).$$

Thus, the sum and product of two fixed points is a fixed point and the inverse of a fixed point is a fixed point. Thus the set of fixed points of E is a field, which is a subfield F of E.

Definition: We call F the fixed field of E under $T_1, T_2, \ldots, T_n$.

THEOREM 3.3.3: If $T_1, T_2, \ldots, T_n$ are n mutually distinct isomorphisms of a field E into a field E', and if F is the fixed field of E, then $(E/F) \geq n$.

Proof: Assume $(E/F) = r$. Let $w_1, w_2, \ldots, w_r$ be a generating system of E over F. Consider the homogeneous linear equations,

$$
(3.3.2)\quad
\begin{aligned}
&T_1(w_1)x_1 + T_2(w_1)x_2 + \dots + T_n(w_1)x_n = 0,\\
&T_1(w_2)x_1 + T_2(w_2)x_2 + \dots + T_n(w_2)x_n = 0,\\
&\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots\\
&T_1(w_r)x_1 + T_2(w_r)x_2 + \dots + T_n(w_r)x_n = 0.
\end{aligned}
$$

For any element α in E there exist $b_1, b_2, \dots, b_r$ in F such that $\alpha = b_1w_1 + b_2w_2 + \dots + b_rw_r$. We multiply the first equation of (3.3.2) by $T_1(b_1)$, the second by $T_1(b_2)$ and so on. The b_i belong to F and hence $T_1(b_i) = T_j(b_i)$. Since also $T_j(b_i) \cdot T_j(w_i) = T_j(b_iw_i)$, we obtain,

$$
(3.3.3)\quad
\begin{aligned}
&T_1(b_1w_1)x_1 + \dots + T_n(b_1w_1)x_n = 0,\\
&\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots\\
&T_1(b_rw_r)x_1 + \dots + T_n(b_rw_r)x_n = 0.
\end{aligned}
$$

Adding equations (3.3.3) and using

$$T_i(b_1w_1) + T_i(b_2w_2) + \dots + T_i(b_rw_r) = T_i(b_1w_1 + \dots + b_rw_r) = T_i(\alpha)$$

we obtain

$$T_1(\alpha)x_1 + T_2(\alpha)x_2 + \dots + T_n(\alpha)x_n = 0.$$

Since the $T_1, T_2, \dots, T_n$ are independent, $x_i = 0$, thus (3.3.2) has only the trivial solution and so $r \geq n$.

Corollary: If $T_1, \dots, T_n$ are automorphisms of the field E, and F is the fixed field, then $(E/F) \geq n$.

Proof: Since the automorphism is an isomorphism of E into E, the proof is immediate.

If F is a subfield of the field E, and T an automorphism of E, we shall say that T leaves F fixed if for each element a of F, $T(a) = a$. If T and S are two automorphisms of E, then the mapping $x \rightarrow T(S(x))$ written as TS is an automorphism since $TS(x.y) = T(S(x.y)) = T(S(x).S(y)) = T(S(x)).T(S(y)) = TS(x).TS(y)$, and similarly, $TS(x \pm y) = TS(x) \pm TS(y)$. We call TS the product of T and S. If T is an automorphism $T(x) = y$, then we shall call T^{-1} the mapping of y into x, that is, $T^{-1}(y) = x$ the inverse of T. We show that T^{-1} is an automorphism. We have

$$T(x_1) = y_1,\ T(x_2) = y_2 \text{ and } T^{-1}(y_1) = x_1,\ T^{-1}(y_2) = x_2.$$

We wish to show that

$$T^{-1}(y_1y_2) = T^{-1}(y_1)T^{-1}(y_2) \text{ and } T^{-1}(y_1 \pm y_2) = T^{-1}(y_1) \pm T^{-1}(y_2).$$

Now

$$T^{-1}(y_1y_2) = T^{-1}\left[T(x_1).T(x_2)\right] = T^{-1}T(x_1x_2) = x_1x_2 = T^{-1}(y_1)T^{-1}(y_2).$$

Also

$$T^{-1}(y_1 \pm y_2) = T^{-1}\left[T(x_1) \pm T(x_2)\right] = T^{-1}\left[T(x_1 \pm x_2)\right] = x_1 \pm x_2 = T^{-1}(y_1) \pm T^{-1}(y_2).$$

Therefore T^{-1} is an automorphism. The automorphism $I(x) = x$ will be called the unit automorphism.

<u>Lemma 3.3.4</u>: <u>If E is an extension field of F, the set G of automorphisms which leave F fixed is a group</u>.

<u>Proof</u>: The product of two automorphisms which leave F fixed, leaves F fixed. The inverse of an automorphism in G is in G. Therefore the set G is a group.

In regard to Lemma 3.3.4 we may have an element of E not in F which is left fixed by G and therefore the fixed field of G may be larger than F.

<u>3.4 Normal Extensions</u>.

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

THEOREM 3.4.1: *If $T_1, T_2, \ldots, T_n$ is a group of automorphisms of a field E and if F is the fixed field of $T_1, T_2, \ldots, T_n$, then* $(E/F) = n$.

Proof: If $T_1, \ldots, T_n$ is a group, then there is an identity, say, $T_1 = I$. The fixed field consists of those elements x which are not moved by any of $T_1, \ldots, T_n$. Suppose $(E/F) > n$. Then there exist $n + 1$ elements $\alpha_1, \alpha_2, \ldots, \alpha_{n+1}$ of E which are linearly independent with respect to F. By Theorem 1.2.1 there exists a non-trivial solution in E to the system of equations

$$
(3.4.1)\quad
\begin{aligned}
x_1T_1(\alpha_1) + x_2T_1(\alpha_2) + \ldots + x_{n+1}T_1(\alpha_{n+1}) &= 0,\\
x_1T_2(\alpha_1) + x_2T_2(\alpha_2) + \ldots + x_{n+1}T_2(\alpha_{n+1}) &= 0,\\
\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots &\\
x_1T_n(\alpha_1) + x_2T_n(\alpha_2) + \ldots + x_{n+1}T_n(\alpha_{n+1}) &= 0.
\end{aligned}
$$

We note that the solution to (3.4.1) cannot lie in F, otherwise, since T_1 is the identity, the first equation would be a dependence between $\alpha_1, \ldots, \alpha_{n+1}$. Among all non-trivial solutions $x_1, \ldots, x_{n+1}$ we choose one which has the most number of elements zero. We may suppose this solution to be $b_1, \ldots, b_r, 0, \ldots, 0$, where the first r terms are non-zero. Also, $r \neq 1$ because $b_1T_1(\alpha_1) = 0$ implies $b_1 = 0$ since $T_1(\alpha_1) = \alpha_1 \neq 0$. Also, we may suppose $b_r = 1$, since if we multiply the given solution by b_r^{-1} we obtain a new solution in which the r-th term is 1. Thus, we have

(3.4.2) $b_1T_i(\alpha_1) + b_2T_i(\alpha_2) + \dots + b_{r-1}T_i(\alpha_{r-1}) + T_i(\alpha_r) = 0$

for $i = 1,2,\dots,n$. Since $b_1,\dots,b_{r-1}$ cannot all belong to F, one of these, say b_1, is in E but not in F. There is an automorphism T_k for which $T_k(b_1) \neq b_1$. If we use the fact that $T_1,\dots,T_n$ form a group, we see that $T_k \cdot T_1, T_k \cdot T_2, \dots, T_k \cdot T_n$ is a permutation of $T_1,\dots,T_n$. Applying T_k to the set (3.4.2) we obtain equation

(3.4.3) $T_k(b_1) \cdot T_kT_j(\alpha_1) + \dots$

$$+ T_k(b_{r-1}) \cdot T_kT_j(\alpha_{r-1}) + T_kT_j(\alpha_r) = 0$$

for $j = 1,2,\dots,n$ so that from $T_kT_j = T_i$, (3.4.3) becomes

(3.4.4) $T_k(b_1)T_i(\alpha_1) + \dots + T_k(b_{r-1})T_i(\alpha_{r-1}) + T_i(\alpha_r) = 0$

and if we subtract (3.4.4) from (3.4.2) we have

$$\left[b_1 - T_k(b_1)\right] \cdot T_i(\alpha_1) + \dots + \left[b_{r-1} - T_k(b_{r-1})\right]T_i(\alpha_{r-1}) = 0$$

which is a non-trivial solution to set (3.4.1) having fewer than r elements non-zero, contrary to the choice of r, which proves the theorem.

<u>Corollary 1</u>: <u>If a subfield F of E is the fixed field for a finite group G of order n, of automorphisms of E, then each automorphism T that leaves F fixed must belong to G</u>.

<u>Proof</u>: By Theorem 3.4.1 (E/F) = order of G = n. We assume there is a T not in G which leaves F fixed. Then F would remain fixed under the n + 1 elements consisting of T and the elements of G, thus $(E/F) \geq n + 1$ by the Corollary to Theorem 3.3.3. This is a contradiction.

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

Proof: This follows from the above Corollary 2.

Corollary 3: E is a normal extension of F, if and only if the number of automorphisms of E which leave F fixed is (E/F).

Proof: If E is a normal extension of F, the number of distinct automorphisms of E which leave F fixed is (E/F), by Theorem 3.4.1.

Conversely, suppose that F' is the fixed field of all those automorphisms of E which leave F fixed. Then $F \subseteq F' \subseteq E$. By Theorem 3.4.1, the number of automorphisms of E leaving F' fixed is (E/F'). Assuming that (E/F) automorphisms of E leave F fixed, we have $(E/F') = (E/F)$. Since $(E/F) = (E/F')(F'/F)$, $(F'/F) = 1$ and $F' = F$. Thus E is a normal extension of F.

Lemma 3.4.2: If E is a normal extension of F, then any element of E is root of an irreducible, separable equation over F which splits completely in E.

Proof: Let $T_1, \ldots, T_s$ be the group G of automorphisms of E whose fixed field is F. Let $\alpha \in E$, $\alpha \notin F$, and let $\alpha = \alpha_1, \alpha_2, \alpha_3, \ldots, \alpha_r$ be the set of distinct elements in the sequence $T_1(\alpha), T_2(\alpha), \ldots, T_s(\alpha)$. Since G is a group,

$$T_j(\alpha_i) = T_j(T_k(\alpha)) = T_jT_k(\alpha) = T_m(\alpha) = \alpha_n,$$

where $n \leq r$. Since the mapping T_j is one-to-one, the elements $\alpha, \alpha_2, \alpha_3, \ldots, \alpha_r$ are permuted by each automorphism of G. The coefficients of the polynomial $f(x) = (x - \alpha)(x - \alpha_2)\ldots(x - \alpha_r)$ 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 E which are left fixed by all the automorphisms of $G \in F$, f(x) is a polynomial in F. If g(x) is any other polynomial in F which also has α as root, then applying the automorphisms of G to $g(\alpha) = 0$ we obtain $g(\alpha_i) = 0$, so that the degree of $g(x) \geq r$. Hence f(x) is irreducible, which proves the lemma.

<u>THEOREM 3.4.3</u>: E <u>is a normal extension of</u> F <u>if and only if</u> E <u>is the splitting field of a separable polynomial</u> p(x) <u>in</u> F.

<u>Proof</u>: <u>Sufficiency</u>: We assume that E splits p(x), and prove that E is a normal extension of F. If all the roots of p(x) are in F, then $E = F$ and only the unit automorphism leaves F fixed and our proposition would hold. Suppose p(x) has $n > 1$ roots in E but not in F. We make the inductive assumption that for all pairs of fields with fewer than n roots of p(x) outside F our proposition holds. Let $p(x) = p_1(x) \cdot \ldots \cdot p_r(x)$ be a factorization in F 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 F. Suppose deg. $p_1(x) = s > 1$. Let α_1 be a root of $p_1(x)$. Then $(F(\alpha_1)/F) = \text{deg. } p_1(x) = s$ (cf. paragraph after Lemma 2.3.2). If we consider $F(\alpha_1)$ as the new ground field, fewer roots of p(x) than n are outside. Since p(x)

lies in $F(\alpha_1)$ and E is a splitting field of $p(x)$ over $F(\alpha_1)$, then by our inductive assumption it follows that E is a normal extension of $F(\alpha_1)$. Thus, each element in E which is not in $F(\alpha_1)$ is moved by at least one automorphism which leaves $F(\alpha_1)$ fixed. Since $p(x)$ is separable, the roots $\alpha_1,\ldots,\alpha_s$ of $p_1(x)$ are s distinct elements of E. By Theorem 2.4.1 there exist isomorphisms $T_1,T_2,\ldots,T_s$ mapping $F(\alpha_1)$ on $F(\alpha_1),F(\alpha_2),\ldots,F(\alpha_s)$, respectively, which are each the identity on F and map α_1 on $\alpha_1,\alpha_2,\ldots,\alpha_s$ respectively. We now apply Theorem 3.1.5. E is a splitting field of $p(x)$ in $F(\alpha_1)$ and is also a splitting field of $p(x)$ in $F(\alpha_i)$. Hence the isomorphism T_i, which makes $p(x)$ in $F(\alpha_1)$ correspond to the same $p(x)$ in $F(\alpha_i)$, can be extended to an isomorphic mapping of E onto E, that is, to an automorphism of E that we denote again by T_i. Hence, $T_1,T_2,\ldots,T_s$ are automorphisms of E that leave F fixed and map α_1 onto $\alpha_1,\alpha_2,\ldots,\alpha_n$. Now let β be any element of E that remains fixed under all automorphisms of E that leave F fixed. Thus β remains fixed under the subset of all automorphisms of E that leave $F(\alpha_1)$ fixed. Since E is a normal extension of $F(\alpha_1)$, β must lie in $F(\alpha_1)$. Thus

(3.4.5) $\quad \beta = c_0 + c_1\alpha_1 + c_2\alpha_1^2 + \ldots + c_{s-1}\alpha_1^{s-1},$

where the c_i are in F. If we apply T_i to (3.4.5) we get, since $T_i(\beta) = \beta$,

$$\beta = c_0 + c_1\alpha_i + c_2\alpha_i^2 + \ldots + c_{s-1}\alpha_i^{s-1}.$$

The polynomial $c_{s-1}x^{s-1} + c_{s-2}x^{s-2} + \ldots + c_1x + (c_0 - \beta)$

has therefore the s distinct roots $\alpha_1, \alpha_2, \ldots, \alpha_s$. There are more than its degree. So all coefficients of it must vanish, among them $c_0 - \beta$, which shows β is in F. Thus E is a normal extension of F.

<u>Necessity</u>: If E is a normal extension of F, we wish to show that E is the splitting field of a separable polynomial p(x). Let $w_1, w_2, \ldots, w_t$ be a generating system for the vector space E over F. By Theorem 3.4.2 there exists an irreducible, separable polynomial $f_i(x)$ in F which splits in E and has w_i as a root. Then E is the splitting field of the separable polynomial $p(x) = f_1(x).f_2(x)\ldots f_t(x)$. This proves Theorem 3.4.3.

<u>Definition</u>: If f(x) is a polynomial in a field F, and E the splitting field of f(x), then we shall call the group of automorphisms of E over F the <u>group of the equation</u> $f(x) = 0$.

In the Theorems 3.4.4, 3.4.5, 3.4.8 and Lemmas 3.4.6, 3.4.7 we will assume that

(1) p(x) is a separable polynomial in a field F,

(2) E is the splitting field of p(x) and,

(3) G is the group of $p(x) = 0$ over F.

<u>THEOREM 3.4.4</u>: <u>Each intermediate field</u>, B, <u>i.e.</u>, $F \subset B \subset E$, <u>is the fixed field for a subgroup</u> G_B <u>of</u> G, <u>and distinct subgroups have distinct fixed fields</u>.

<u>Proof</u>: Consider p(x) as lying in some intermediate field B. E is still the splitting field of p(x) in B. Thus,

E is a normal extension of each field B, so that B is the fixed field of the subgroup G_B of G made up of those automorphisms of E which leave B fixed. By Corollary 2 of Theorem 3.4.1 distinct subgroups have distinct fixed fields.

Definition: If G is the group of automorphisms of E over F and G_B is the subgroup of automorphisms of G which have B for its fixed field then B and G_B are said to *belong to each other*.

THEOREM 3.4.5: *If* B *is an intermediate field,* $(F \subset B \subset E)$, *and* G_B *belongs to* B, *then* (1) $(E/B) =$ *order of* G_B, *and* (2) $(B/F) =$ *index of* G_B *in* G.

Proof: (1). Since $B \subset E$ is the fixed field of G_B, Theorem 3.4.1 implies that $(E/B) =$ order of $G_B = O(G_B)$.
(2). $(B/F)(E/B) = (E/F) = O(G) = i(G_B).O(G_B) = i(G_B)(E/B)$, where $i(G_B)$ is the index of G_B. Therefore $(B/F) = i(G_B)$.

Lemma 3.4.6: *The number of distinct isomorphisms of* B *which leave* F *fixed is equal to the number of cosets of* G_B *in* G.

Proof: By Theorem 3.4.5, (B/F) is equal to the number of cosets of $G_B = O(G)/O(G_B)$. Since the elements of G are automorphisms of E they map B isomorphically into some other subfield of E and are the identity on F. The elements of G in any one coset of G_B map B in the same way. For let $T.T_1$ and $T.T_2$, where $T \in G$, $T_1, T_2 \in G_B$, be two elements of the coset $T.G_B$. Since T_1 and T_2 leave B fixed, for each α of B we have $T.T_1(\alpha) = T(\alpha) = T.T_2(\alpha)$. Also elements of different cosets give different isomorphisms, for if T and S give the same isomorphism, $T(\alpha) = S(\alpha)$ for each α in B, then $T^{-1}S(\alpha) = \alpha$ for each α in B. Thus $T^{-1}S = T_1$, where T_1 is in G_B. But then $S = T.T_1$ and $S.G_B = T.T_1G_B = T.G_B$ so that T and S belong to the same coset. Also each isomorphism of B which is the identity on F is induced by an automorphism of G. For let T be an isomorphism mapping B on B' and the identity on F. Then under T, p(x) corresponds to p(x), and E is the splitting field of p(x) in B and of p(x) in B'. By Theorem 3.1.5, T can be extended to an automorphism T' of E, and since T' leaves F fixed it belongs to G. This proves the lemma.

Lemma 3.4.7: B *is a normal extension of* F *if and only if each isomorphism of* B *is an automorphism of* B *which leaves* F *fixed*.

Proof: By Lemma 3.4.5 and Lemma 3.4.6, the number of distinct isomorphisms of B $= i(G_B) = (B/F)$. By Theorem 3.4.1, Corollary 3, B is normal over F, if and only if the number of distinct automorphisms of B which leave F fixed is also (B/F), i.e. if and only if the number of distinct isomorphisms of B is equal to the number of distinct automorphisms of B which leave F fixed. Since each automorphism of B is an isomorphism of B, our lemma is proved.

THEOREM 3.4.8: *An intermediate field* B, $(F \subset B \subset E)$, *is a normal extension of* F *if and only if the subgroup* G_B *is a normal subgroup of* G.

<u>Proof</u>: This theorem is an immediate consequence of Lemma 3.4.7 once we have proved that: G_B <u>is normal in</u> G <u>if and only if each isomorphism of</u> B <u>is an automorphism of</u> B, <u>which leaves</u> F <u>fixed</u>.

Now, if T is any automorphism of E, TG_BT^{-1} is a subgroup of G, and $TG_BT^{-1}[T(B)] = TG_B[T^{-1}T(B)] = TG_B(B) = T(B)$. Then, if $TG_BT^{-1}(\alpha) = \alpha$, $G_B[T^{-1}(\alpha)] = T^{-1}(\alpha)$, $T^{-1}(\alpha) \subset B$ and so $\alpha \subset T(B)$. Thus T(B) is the fixed field for TG_BT^{-1}. If G_B is normal in G, then $TG_BT^{-1} = G_B$, hence $T(B) = B$, and every isomorphism of B is an automorphism of B.

Conversely, if $T(B) = B$, for every isomorphism T of B, then $T^{-1}G_BT = G_B$, and G_B is normal in G.

<u>Theorems 3.4.4, 3.4.5, and 3.4.8 are the Fundamental theorems of the Galois theory</u>.

In Lemma 3.4.7, when B is normal over F, and each isomorphism of B is an automorphism of B which leaves F fixed, the cosets of G_B, each of which describes an isomorphism of B (cf. Lemma 3.4.6), are elements of the factor group (G/G_B). Thus each automorphism of B corresponds uniquely to an element of (G/G_B) and conversely. Since multiplication in (G/G_B) is obtained by repeating the mappings, the correspondence is an isomorphism between (G/G_B) and the group of automorphisms of B which leave F fixed.

CHAPTER IV

ROOTS OF UNITY

4.1 Roots of Unity in the Complex Field.

The n n-th roots of unity are found solving the equation $Z^n = 1$. If we let $U = p(\cos\theta + i\sin\theta)$ and $1 = r(\cos\phi + i\sin\phi)$. Suppose $U^n = p^n(\cos n\theta + i\sin n\theta) = 1$. Thus $p = r^{1/n}$; $\theta = \phi/n + 2k\pi/n$, where $k = 0,1,\ldots,n-1$. We have $r = 1$, and $\phi = 0$ and therefore $p = 1$, and $\theta = 2k\pi/n$. Thus the n n-th roots of unity can be represented by $R, R^2, \ldots, R^n$ where $R = \cos 2\pi/n + i\sin 2\pi/n$.

<u>Definition</u>: An n-th root U of 1 is a <u>primitive n-th root</u> of 1 if $U^n = 1$ and $U^m \neq 1$, when $0 < m < n$.

<u>THEOREM 4.1.1</u>: <u>Let</u> $R = \cos 2\pi/n + i\sin 2\pi/n$. <u>If</u> $(k,n) = d$, <u>then</u> R^k <u>is a primitive</u> (n/d)-th <u>root of unity</u>.

<u>Proof</u>: Let $k = k_1 d$, $n = n_1 d$ so that $(k_1,n_1) = 1$. Then $R^k = \cos 2k_1 d\pi/n_1 d + i\sin 2k_1 d\pi/n_1 d = \cos 2k_1\pi/n + i\sin 2k_1\pi/n_1$. Thus $(R^k)^{n_1} = \cos 2k_1\pi + i\sin 2k_1\pi = 1$ so that R^k is an $n_1 = (n/d)$-th root of unity. Also, R^k is a primitive (n/d)-th root of unity, for if $(R^k)^m = 1 = \cos 2k_1 m\pi/n_1 + i\sin 2k_1 m\pi/n_1$, $k_1 m/n_1$ is an integer. Since $(n_1,k_1) = 1$, n_1 divides m, but the least positive multiple of n_1 is n_1 itself.

<u>Corollary 1</u>: <u>Those and only those</u> n-th <u>roots of unity</u> $R, R^2, \ldots, R^n$ <u>are primitive</u> n-th <u>roots of unity whose</u>

<u>exponents are relatively prime to n</u>.

<u>Proof</u>: From Theorem 4.1.1 R^k is a primitive n-th root of unity if and only if $(n,k) = d = 1$.

<u>Corollary 2: If</u> U <u>is any primitive</u> n-th <u>root of unity and</u> $(k,n) = d$, <u>then</u> U^k <u>is a primitive</u> n/d-th <u>root of unity</u>.

<u>Proof</u>: Let $U = R^t$, where $(t,n) = 1$. Hence $U^k = R^{tk}$ and $(tk,n) = d$. Thus we may apply Theorem 4.1.1 to R^{tk} from which the proof is immediate.

<u>Corollary 3</u>: <u>The</u> n n-th <u>roots of unity include all the</u> m-th <u>roots of unity if and only if</u> m <u>divides</u> n.

<u>Proof</u>: If m divides n, $n = mk$, and $(n,k) = k$. Then by Corollary 2 above R^k is a primitive $n/k = m$-th root of unity and hence all the m-th roots of unity are included among the powers of (R^k) which are also n-th roots. If all the m-th roots of unity are included among the n-th roots, then the primitive m-th root $\cos 2\pi/m + i \sin 2\pi/m = R^v$. Again by Corollary 2, if $(v,n) = d$, R^v is a primitive n/d-th root of unity. Hence $n/d = m$ and $n = md$, which completes the proof.

<u>4.2 Roots of unity in fields of prime characteristic</u>.

If a field F has characteristic p, and E is the splitting field of the polynomial $x^n - 1$ where p does not divide n, then E is the field generated out of F by the adjunction of a primitive n-th root of unity. The polynomial $x^n - 1$ does not have repeated roots in E, since its derivative, nx^{n-1}, has only the root 0 and has, thus, no roots in common with $x^n - 1$. Therefore, <u>E is a normal extension of F</u> by Theorem 3.4.3. If $e_1, e_2, \ldots, e_n$ are the roots of $x^n - 1$ in E, they form a group under multiplication and by Theorem 3.2.5 this group will be cyclic. Let e be a generator of the group so that $1, e, e^2, \ldots, e^{n-1}$ are the elements of the group. Since the smallest power of e which is 1 is the n-th, we see that e is a primitive n-th root of unity. The order of any n-th root of unity is a divisor of n, since each n-th root of unity generates a cyclic subgroup of the group of all the roots. If e is a primitive n-th root of unity, evidently $e^{n/r}$ is a primitive r-th root of unity.

<u>THEOREM 4.2.1</u>: <u>If</u> E <u>is the field generated from</u> F <u>by a primitive</u> n-th <u>root of unity, then the group</u> G <u>of</u> E <u>over</u> F <u>is abelian for any</u> n <u>and cyclic if</u> n <u>is prime</u>.

<u>Proof</u>: We have $E = F(e)$, since the roots of $x^n - 1$ are powers of e. Thus, if S and T are distinct elements of G, $S(e) \neq T(e)$. But S(e) is a root of $x^n - 1$ and, thus, a power of e. Thus, $S(e) = e^{n_S}$ where n_S is an integer $1 \leq n_S < n$. Also, $TS(e) = T(e^{n_S}) = (T(e))^{n_S} = e^{n_T \cdot n_S} = ST(e) = e^{n_{ST}}$. Thus G is abelian, and $n_{ST} \equiv n_S n_T (\text{mod } n)$. Hence, the mapping of S on n_S is a homomorphism of G into a multiplicative subgroup of the intergers mod n. Since $T \neq S$ implies $T(e) \neq S(e)$, it follows that $T \neq S$ implies $n_S \not\equiv n_T (\text{mod } n)$. Hence, the homomorphism is an isomorphism. If n is prime, the multiplicative group of integers mod n

forms a cyclic group.

4.3 Noether Equations.

Definition: If E is a field, and $G = (S, T, \ldots)$ any group of automorphisms of E, any set of elements $x_S, x_T, \ldots$ in E will be said to provide a solution of Noether's equations if $x_S . S(x_T) = x_{ST}$ for each S and T in G.

As T traces G, ST assumes all values in G, and in the equation $x_S . S(x_T) = x_{ST}$, $x_{ST} = 0$ when $x_S = 0$. Thus, in any solution of the Noether equations no element $x_S = 0$ unless the solution is completely trivial. In the following we assume the trivial solution has been excluded.

THEOREM 4.3.1: The system $x_S, x_T, \ldots$ is a solution of Noether's equations if and only if there exists an element α in E, such that $x_S = \alpha / S(\alpha)$ for each S.

Proof: If $x_S = \alpha/S(\alpha)$, for some α, then x_S is a solution of the equations, since $x_S . S(x_T) = [\alpha/S(\alpha)] . [S(\alpha/T(\alpha))]$ $= [\alpha/S(\alpha)] . [S(\alpha)/ST(\alpha)] = \alpha/ST(\alpha) = x_{ST}$.

Conversely, we let $x_S, x_T, \ldots$ be a non-trivial solution. Since the automorphisms $S, T, \ldots$ are distinct they are linearly independent by Theorem 3.3.1, and the equation $x_S . S(z) + x_T T(z) + \ldots = 0$ does not hold identically. Hence, there is an element a in E such that $x_S S(a) + x_T T(a) + \ldots = \alpha \neq 0$. Applying S to α gives

$$S(\alpha) = \sum_{T \in G} S(x_T) . ST(a). \qquad (4.3.1)$$

Multiplying (4.3.1) by x_S gives

(4.3.2) $$x_S.S(\alpha) = \sum_{T\in G} x_S S(x_T).ST(a).$$

Replacing $x_S.S(x_T)$ by x_{ST} in (4.3.2) and observing that ST assumes all values in G when T does, then (4.3.2) becomes

$$x_S.S(\alpha) = \sum_{T\in G} x_T T(a) = \alpha$$

so that

$$x_S = \alpha/S(\alpha),$$

completing the proof.

THEOREM 4.3.2: If G is the group of the normal field E over F, then for each character C of G into F there exists an element α in E such that $C(S) = \alpha/S(\alpha)$ and, conversely, if $\alpha/S(\alpha)$ is in F for each S, then $C(S) = \alpha/S(\alpha)$ is a character of G. If r is the least common multiple of the orders of elements of G, then $\alpha^r \in F$.

Proof: Let $x_S = \alpha/S(\alpha)$. By Theorem 4.2.1, x_S is a solution of the Noether equations and yields a mapping C of G into E, namely $C(S) = x_S$. If F is the fixed field of G, and the elements x_S lie in F, then C is a character of G, for

$$C(ST) = x_{ST} = x_S.S(x_T) = x_S x_T = C(S).C(T)$$

since $S(x_T) = x_T$ if $x_T \in F$. Conversely, each character C of G into F provides a solution of the Noether equations, for if we call $C(S) = x_S$, then, since $x_T \in F$, we have $S(x_T) = x_T$. Thus,

$$x_S.S(x_T) = x_S.x_T = C(S).C(T) = C(ST) = x_{ST}.$$

For the last part of the theorem we need only show that $S(\alpha^r) = \alpha^r$ for each $S \in G$. Now,

$$\alpha^r/S(\alpha^r) = (\alpha/S(\alpha))^r = (x_S)^r = (C(S))^r = C(S^r) = C(I) = 1,$$

which proves the theorem.

4.4 Kummer's Fields.

Definition: If F contains a primitive n-th root of unity, any splitting field E of a polynomial $(x^n - a_1)\cdot(x^n - a_2)\cdot \ldots \cdot(x^n - a_r)$ where $a_i \in F$ for $i = 1,2,\ldots,r$ will be called a Kummer extension of F, or a Kummer field.

THEOREM 4.4.1: If E is a Kummer field then: (i) E is a normal extension of F, (ii) the group G of E over F is abelian, (iii) the least common multiple of the orders of the elements of G is a divisor of n, where n is the order of the primitive root of unity in F.

Proof: If F contains a primitive n-th root of unity, we prove that n is not divisible by the characteristic of F. For, suppose 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 thus is equal to zero. Thus

$$x^n - 1 = (x^q)^p - 1 = (x^q - 1)^p$$

and $x^n - 1$ cannot have more than q distinct roots. But we assumed that F has a primitive n-th root of unity and so $1, e, e^2, \ldots, e^{n-1}$ are n distinct roots of $x^n - 1$. It follows that n is not divisible by the characteristic of F. For a Kummer field 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 $x^n - a_i$. Thus, the irreducible factors of $x^n - a_i$ are separable, so that E is a normal extension of F.

Let α_i be a root of $x^n - a_i$ in E. If $e_1, e_2, \dots, e_n$ are the n distinct n-th roots of unity in F, then $\alpha_i e_1, \alpha_i e_2, \dots, \alpha_i e_n$ will be n distinct roots of $x^n - a_i$, and hence will be the roots of $x^n - a_i$, so that $E = F(\alpha_1, \alpha_2, \dots, \alpha_r)$. Let S and T be two automorphisms in the group G of E over F. For each α_i, both S and T map α_i on some other root of $x^n - a_i$. Thus $T(\alpha_i) = e_{iT}\alpha_i$ and $S(\alpha_i) = e_{iS}\cdot\alpha_i$ where e_{iS} and e_{iT} are n-th roots of unity in the basic field F. It follows that

$$T(S(\alpha_i)) = T(e_{iS}\alpha_i) = e_{iS}T(\alpha_i) = e_{iS}e_{iT}\alpha_i = S(T(\alpha_i)).$$

Since S and T are commutative over the generators of E, they commute over each element of E. Hence, G is abelian.

If $S \in G$ then $S(\alpha_i) = e_{iS}\alpha_i$, $S^2(\alpha_i) = e_{iS}^2\alpha_i$, ... Thus, $S^{n_i}(\alpha_i) = \alpha_i$ for n_i such that $e_{iS}^{n} = 1$. 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 $S^m(\alpha_i) = \alpha_i$ for $i = 1, 2, \dots, r$ it follows that m is the order of S. Hence, the order of each element of G is a divisor of n, and thus, the least common multiple of the orders of the elements of G is a divisor of n. This proves (iii).

<u>Corollary</u>: <u>If</u> E <u>is the splitting field of</u> $x^p - a$, <u>where</u> p <u>is a prime, and</u> F <u>contains a primitive</u> p-<u>th root of unity, then either</u> $E = F$ <u>and</u> $x^p - a$ <u>splits in</u> F, <u>or</u> $x^p - a$ <u>is irreducible over</u> F <u>and the group of</u> E <u>over</u> F <u>is</u>

<u>cyclic of order</u> p.

<u>Proof</u>: The order of each element of G is, by Theorem 4.4.1, a divisor of p and, hence, if the element is not the identity its order must be p. If α is a root of $x^p - a$, then $\alpha, e\alpha, \ldots, e^{p-1}\alpha$ are all roots of $x^p - a$ so that $F(\alpha) = E$ and $(E/F) \leq p$. 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 α, then α must have p distinct images. Hence, the irreducible equation in F for α must be of degree p and is therefore $x^p - a = 0$. This completes the proof.

<u>Definition</u>: Let C_1 and C_2 be characters mapping a group G <u>into</u> a field E. If C_1 maps S on a_S and C_2 maps S on b_S, then C_1C_2 is the character which maps S on a_Sb_S.

<u>Lemma 4.4.2</u>: <u>If</u> E <u>is a normal extension of a field</u> F, <u>whose group</u> G <u>over</u> F <u>is abelian, and</u> F <u>contains a primitive</u> r-<u>th root of unity where</u> r <u>is the least common multiple of the orders of elements of</u> G, <u>then the group of characters</u> X <u>of</u> G <u>into the group of</u> r-<u>th roots of unity is isomorphic to</u> G, <u>and to each</u> S <u>of</u> G, <u>if</u> $S \neq I$, <u>there exists a character</u> C <u>of</u> X <u>such that</u> $C(S) \neq 1$.

<u>Proof</u>: As in Theorem 3.2.6 we may express G as the direct product of the cyclic groups $G_1, G_2, \ldots, G_t$ of orders $m_1, m_2, \ldots, m_t$ such that $m_1 | m_2 | \ldots | m_t$. Each S of G may be written $S = S_1^{v_1} S_2^{v_2} \ldots S_t^{v_t}$ where S_i is a generator of G_i.

We will denote by C_i the character which sends S_i into e_i, a primitive m_i-th root of unity, and S_j into 1 for j not equal to i. Let C be any character. Now

$$[C(S_i)]^{m_i} = C(S_i^{m_i}) = C(I) = 1,$$

hence $C(S_i) = e_i^{w_i}$, and we have $C = C_1^{w_1}.C_2^{w_2}. \ldots .C_t^{w_t}$. Conversely, $C_1^{w_1}\ldots C_t^{w_t}$ defines a character. Since the order of C_i is m_i, the character group X of G is isomorphic to G. If S is not equal to I, then in $S = S_1^{v_1}S_2^{v_2}\ldots S_t^{v_t}$ at least one v_i, say v_1, is not divisible by m_1. Thus $C_1(S) = e_1^{v_1} \neq 1$, which proves the lemma.

Now suppose we have the conditions of Lemma 4.4.1. Let A denote the set of those non-zero elements α of E for which $\alpha^r \in F$ and let F_1 denote the non-zero elements of F. We see that A is a multiplicative group and 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. With these conditions we have in the following theorem a method for computing G.

<u>THEOREM 4.4.3</u>: <u>The factor groups</u> (A/F_1) <u>and</u> (A^r/F_1^r) <u>are isomorphic to each other and to the groups</u> G <u>and</u> X.

<u>Proof</u>: We map A on A^r by making α of A correspond to α^r of A^r. If $a^r \in A^r$, where $a \in A$, then $b \in A$ is mapped on a^r if and only if b^r equals a^r, that is, if b is a solution to the equation $x^r - a^r = 0$. But $a, ea, e^2a, \ldots, e^{r-1}a$ are distinct solutions to this equation and since $e \in F_1$ and a belong to A, it follows that b must be one of these

elements and must belong to the coset aF_1. Thus, the set of elements of A which map onto the subgroup F_1^r of A^r is F_1, so that the factor groups (A/F_1) and (A^r/F_1^r) are isomorphic.

If α is an element of A, then

$$\left[\alpha/T(\alpha)\right]^r = \alpha^r/T(\alpha^r) = \alpha^r/\alpha^r = 1,$$

for every automorphism T of G. Hence, $\alpha/T(\alpha)$ is an r-th root of unity and is in F_1. By Theorem 4.3.2, α defines a character C_α of G into F such that $C_\alpha(T) = \alpha/T(\alpha)$. We map α on the corresponding character C_α. Each character C is, by Theorem 4.3.2, the image of some α. Also, $\alpha.\alpha'$ defines the character $C_{\alpha\alpha'}$ such that $C_{\alpha\alpha'}(T) = \alpha\alpha'/T(\alpha.\alpha') = \alpha.\alpha'/T(\alpha).T(\alpha')$. By definition, $C_{\alpha\alpha'}(T) = C_\alpha(T).C_{\alpha'}(T)$, so that the mapping is a homomorphism. The kernel of this homomorphism is the set of those elements α for which $\alpha/T(\alpha) = 1$ for each T, hence is F_1. Thus, (A/F_1) is isomorphic to X under the mapping of the coset αF_1, of (A/F_1) on the character C_α defined by $C_\alpha(T) = \alpha/T(\alpha)$. By Lemma 4.4.2 X is isomorphic to G. This proves the theorem.

<u>THEOREM 4.4.4</u>: <u>If</u> E <u>is an extension field over</u> F, <u>then</u> E <u>is a Kummer field if and only if</u> E <u>is normal, its group</u> G <u>is abelian and</u> F <u>contains a primitive</u> r-<u>th root</u> e <u>of unity where</u> r <u>is the least common multiple of the orders of the elements of</u> G.

<u>Proof</u>: The necessity is proved in Theorem 4.4.1. We prove the sufficiency. Relative to the group A, let $\alpha_1 F_1, \alpha_2 F_1, \ldots, \alpha_t F_1$ be the cosets of F_1. Since α_i belong

to A, we have $\alpha_i^r = a_i \in F$. Thus, α_i is a root of the equation $x^r - a_i = 0$ and since $e\alpha_i, e^2\alpha_i, \ldots, e^{r-1}\alpha_i$ are also roots, $x^r - a_i$ must split in E. We prove that E is the splitting field of $(x^r - a_1)(x^r - a_2)\ldots(x^r - a_t)$, that is, we must show that $F(\alpha_1, \alpha_2, \ldots, \alpha_t) = E$. Suppose that $F(\alpha_1, \alpha_2, \ldots, \alpha_t) \neq E$. Then $F(\alpha_1, \ldots, \alpha_t)$ is an intermediate field between F and E, and since E is normal over $F(\alpha_1, \ldots, \alpha_t)$ where $[E/F(\alpha_1, \ldots, \alpha_t)] > 1$, there exists an automorphism T of G, $T \neq I$, which leaves $F(\alpha_1, \ldots, \alpha_t)$ fixed. By Lemma 4.4.2 there exists a character C of X corresponding to an element $T \in G$ for which $C(T) \neq 1$. Finally, there exists an element α in E such that $C(T) = \alpha/T(\alpha) \neq 1$. But α^r belongs to F_1 by Theorem 4.3.2, hence α belongs to A. Also, A is contained in $F(\alpha_1, \ldots, \alpha_t)$ since all the cosets $\alpha_i F_1$ are contained in $F(\alpha_1, \ldots, \alpha_t)$. Since $F(\alpha_1, \ldots, \alpha_t)$ is by assumption left fixed by T, $T(\alpha) = \alpha$ which contradicts $\alpha/T(\alpha) \neq 1$. Thus, $F(\alpha_1, \ldots, \alpha_t) = E$ which completes the proof.

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

Proof: E is generated by elements $\alpha_1, \ldots, \alpha_n$ where α_i^p belong to F. Let α_1 be not in F. Then $x^p - a$ is irreducible, for otherwise $F(\alpha_1)$ would be an intermediate field between F and E of degree less than p, and by Theorem 2.1.1, p would not be a prime number, contrary to assumption. Thus, $E = F(\alpha_1)$ is the splitting field of $x^p - a$.

CHAPTER V

EXTENSIONS AND INTERSECTIONS OF FIELDS

5.1 Primitive Extensions.

Definition: If an extension E of F is generated by a single element, it is called a primitive extension.

THEOREM 5.1.1: A finite extension E of F is primitive over F if and only if there are only a finite number of intermediate fields.

Proof: (a) Let $E = F(\alpha)$ and let $f(x) = 0$ be the irreducible equation for α in F. Let B be an intermediate field and $g(x)$ the irreducible equation for α in B. The coefficients of $g(x)$ adjoined to F will generate a field B' between F and B. Since $g(x)$ is irreducible in B it is also irreducible in B'. Since $E = B'(\alpha)$ we see that $(E/B) = (E/B')$. Thus $B = B'$, so that B is uniquely determined by the polynomial $g(x)$. But $g(x)$ is a divisor of $f(x)$ in E, and there are only a finite number of possible divisors of $f(x)$ in E. Thus, there are only a finite number of possible B's.

(b) Now we assume there are only a finite number of fields between E and F. If F consists only of a finite number of elements, then E is generated by one element (cf. Corollary to Theorem 3.2.5). Thus, we may assume F has an infinity of elements. We prove: To any two elements α, β

in E there is a γ in E such that $F(\alpha,\beta) = F(\gamma)$. Let $\gamma = \alpha + a\beta$ with a in F. Consider all the fields $F(\gamma)$ obtained in this way. Since we have an infinity of a's, there exist two, say a_1 and a_2, such that the corresponding γ's, $\gamma_1 = \alpha + a_1\beta$ and $\gamma_2 = \alpha + a_2\beta$, give the same field $F(\gamma_1) = F(\gamma_2)$. Since both γ_1 and γ_2 are in $F(\gamma_1)$, their difference is in the field $F(\gamma_1)$ and thus β is in the same field. Therefore $\gamma_1 - a_1\beta = \alpha$ lies in $F(\gamma_1)$. So $F(\alpha,\beta)$ is contained in $F(\gamma_1)$. But $F(\gamma_1)$ is contained in $F(\alpha,\beta)$ and therefore $F(\alpha,\beta) = F(\gamma_1)$. Select now η in E in such a way that $[F(\eta)/F]$ is as large as possible. Every element λ of E must be in $F(\eta)$ or else we could find an element δ such that $F(\delta) = F(\eta,\lambda)$ contains both η and λ and $[F(\delta)/F] = [F(\delta)/F(\eta)]\,[F(\eta)/F] > [F(\eta)/F]$. Thus, $E = F(\eta)$ which proves the theorem.

<u>THEOREM 5.1.2</u>: <u>If</u> $E = F(\alpha_1,\alpha_2,\ldots,\alpha_n)$ <u>is a finite extension of the field</u> F, <u>and</u> $\alpha_1,\ldots,\alpha_n$ <u>are separable elements in</u> E <u>then there exists a primitive</u> Θ <u>of</u> E <u>such that</u> $E = F(\Theta)$.

<u>Proof</u>: Let $f_i(x)$ be the irreducible equation of α_i in F and let B be an extension of E that splits $f_1(x)f_2(x)\ldots f_n(x)$. Then by Theorem 3.4.3 B is normal over F and contains only a finite number of intermediate fields. So the subfield E contains only a finite number of intermediate fields. Theorem 5.1.1 now completes the proof.

<u>THEOREM 5.1.3</u>: <u>If</u> E <u>is a normal extension of</u> F <u>and</u> $T_1,T_2,\ldots,T_n$ <u>are the elements of its group</u> G, <u>there is an</u>

<u>element</u> β <u>in</u> E <u>such that the</u> n <u>elements</u> $T_1(\beta), T_2(\beta), \ldots,$ $T_n(\beta)$ <u>are linearly independent with respect to</u> F.

<u>Proof</u>: Since E is normal over F, E is a finite extension of F, and by Theorem 5.1.2 there is an α such that $E = F(\alpha)$. Let $f(x)$ be the separable equation for α, put $T_i(\alpha) = \alpha_i$, where $\alpha_i \neq \alpha_j$ when $i \neq j$. Let $f(x) = (x - \alpha)h(x)$. Then $f'(x) = (x - \alpha)h'(x) + h(x)$ and $f'(\alpha) = h(\alpha) \neq 0$. Let $g(x) = f(x)/(x - \alpha)f'(\alpha)$ and $g_i(x) = T_i\left[g(x)\right] = f(x)/(x - \alpha_i)f'(\alpha_i)$. Now $g_i(x)$ is a polynomial in E having α_k as root for $k \neq i$ and thus

(5.1.1) $$g_i(x)g_k(x) \equiv 0\left[\text{mod } f(x)\right]$$

for $i \neq k$. In the equation

(5.1.2) $$g_1(x) + g_2(x) + \ldots + g_n(x) - 1 = 0$$

the left side is of degree at most $n - 1$. If equation (5.1.2) is true for n different values of x, the left side must be identically 0. Such n values are $\alpha_1, \alpha_2, \ldots, \alpha_n$, since $g_i(\alpha_i) = 1$ and $g_k(\alpha_i) = 0$ for $k \neq i$. Multiplying (5.1.2) by $g_i(x)$, and using (5.1.1), we see that

(5.1.3) $$\left[g_i(x)\right]^2 \equiv g_i(x)\left[\text{mod } f(x)\right].$$

We next compute the determinant

(5.1.4) $$D(x) = \left|T_iT_k\left[g(x)\right]\right|, \quad i,k = 1,2,\ldots n,$$

and prove that $D(x) \neq 0$. If we square $D(x)$ by multiplying column by column and compute its value $\left[\text{mod } f(x)\right]$ we get from (5.1.1),(5.1.2),(5.1.3) a determinant that has 1 in the diagonal and 0 elsewhere. Therefore $\left[D(x)\right]^2 \equiv 1(\text{mod } f(x))$. $D(x)$ can have only a finite number of roots in F. Avoiding these finite roots in F we can find a value a for x such that $D(a) \neq 0$. Now set $\beta = g(a)$. Then the determinant

(5.1.5) $$\left|T_i T_k(\beta)\right| = \left|T_i T_k[g(a)]\right| = D(a) \neq 0.$$

Consider any linear relation $x_1T_1(\beta) + x_2T_2(\beta) + \ldots + x_nT_n(\beta) = 0$ where the x_i are in F. Applying the automorphisms T_i to it would lead to n homogeneous equations for the n unknowns x_i. Equation (5.1.5) shows that $x_i = 0$ and our theorem is proved.

5.2 Intersections of Fields.

Let F be a field, p(x) a polynomial in F whose irreducible factors are separable, and let E be a splitting field for p(x). Let B be an arbitrary extension of F, and let E_B be the splitting field of p(x) when p(x) is taken to lie in B. If $\alpha_1, \alpha_2, \ldots, \alpha_s$ are the roots of p(x) in E_B, then $F(\alpha_1, \ldots, \alpha_s)$ is a subfield of E_B which is a splitting field for p(x) in F. By Theorem 3.1.5, E and $F(\alpha_1, \ldots, \alpha_s)$ are isomorphic. In the following work we take $E = F(\alpha_1, \ldots, \alpha_s)$ and assume that E is a subfield of E_B. Also, $E_B = B(\alpha_1, \ldots, \alpha_s)$.

<u>Definition</u>: $E \cap B$ denotes the intersection of the fields E and B.

Now $E \cap B$ forms a field, for if a,b belong to E and to B then ab belongs to E and ab belongs to B and thus belongs to $E \cap B$. Also if a,b belong to E,B then a^{-1}, b^{-1} belong to E,B and therefore belong to $E \cap B$. Thus $E \cap B$ is a field which is intermediate to E and F.

<u>THEOREM 5.2.1</u>: <u>If</u> G <u>is the group of automorphisms</u>

of E *over* F, *and* H *the group of* E_B *over* B, *then* H *is isomorphic to the subgroup of* G *having* $E \cap B$ *as its fixed field*.

Proof: Each automorphism of E_B over B simply permutes $\alpha_1, \ldots, \alpha_s$ in some way and leaves B fixed, and thus also $F \subset B$ fixed. Since the elements of E_B are quotients of polynomial expressions in $\alpha_1, \ldots, \alpha_s$ with coefficients in B, the automorphism is completely determined by the permutation it effects on $\alpha_1, \ldots, \alpha_s$. Thus, each automorphism of E_B over B defines an automorphism of $E = F(\alpha_1, \ldots, \alpha_s)$ which leaves F fixed. Distinct automorphisms, since $\alpha_1, \ldots, \alpha_s$ belong to E, have different effects on E. Thus, the group H of E_B over B can be considered as a subgroup of the group G of E over F. Each element of H leaves $E \cap B$ fixed since it leaves even all of B fixed. But, any element of E which is not in $E \cap B$ is not in B, and hence would be moved by at least one automorphism of H. Therefore $E \cap B$ is the fixed field of H, which proves the theorem.

Corollary: *If, under the conditions of Theorem 5.1.2, the group* G *is of prime order* p, *then either* $H = G$ *or* H *consists of the unit element alone*.

Proof: Since the order of H divides the order of G which is of prime order, then the order of H must be p or 1.

PART II

APPLICATIONS OF THE GALOIS THEORY

CHAPTER VI

A CRITERION FOR SOLVABILITY BY RADICALS IN FIELDS OF CHARACTERISTIC 0

6.1 Solvable Groups.

For our discussion on solvability we need the following group theoretic results.

THEOREM 6.1.1: *If* N *is a normal subgroup of the group* G, *then the mapping* $g \to gN$ *is a homomorphism of* G *on the factor group* G/N *called the natural homomorphism.*

Proof: If N is a normal subgroup of G, then $gN = Ng$ for all g in G. Let $g, h \in G$. If $g \to gN$ and $h \to hN$, then $gh \to (gN)(hN) = g(Nh)N = (gh)N$. Thus $g \to gN$ is a homomorphism of G on the factor group G/N. If N is a proper subgroup of G, the mapping is a many-to-one mapping.

THEOREM 6.1.2: *The image and the inverse image of a normal subgroup under a group homomorphism* $G \to G'$ *is a normal subgroup.*

Proof: Let $g \in G$ where G is a group, and let $n \in N$ where N is a normal subgroup of G. Then $gN = Ng$ or $gNg^{-1} = N$. Let $g \to g'$, where $g \in G$ and $g' \in G'$. Since the mapping is homomorphic, $g'(g^{-1})' = (gg^{-1})' = (e)' = e'$, and hence $(g^{-1})' = (g')^{-1}$, i.e., $g^{-1} \to g'^{-1}$. In particular, $N \to N'$, where N' is a subgroup of G'. Now $gN \to g'N'$. But $gN = Ng \to N'g'$. Therefore $g'N' = N'g'$ and N' is a normal subgroup of

G'. Conversely, if N' is a normal subgroup of G', we wish to show that N is a normal subgroup of G. Let N be the set of elements which map on N'. Now e, the identity of G is mapped on e'. But $e' \in N'$, thus e is in N. If n is in N, then $n^{-1} \to (n^{-1})' = (n')^{-1} \in N'$, so that $n^{-1} \in N$. Thus N is a group of G. Let g be any element of G. Then $gNg^{-1} \to g'N'g'^{-1} = N'$. Thus $gNg^{-1} \leq N$. Similarly, $g^{-1}Ng \leq N$, and this implies that $N \leq gNg^{-1}$. Thus $gNg^{-1} = N$ and N is a normal subgroup of G.

<u>THEOREM 6.1.3</u>: <u>If</u> $g \to g'$ <u>is a homomorphism of the group</u> G <u>on</u> G', N <u>is any normal subgroup of</u> G, $N \to N'$, <u>and</u> T <u>is the mapping</u>: $gN \to g'N'$, <u>where</u> $g \in G$, $g' \in G'$, <u>then</u> T <u>is a homomorphism of the factor group</u> G/N <u>on the factor group</u> G'/N'.

<u>Proof</u>: If $gN \to g'N'$, $hN \to h'N'$, then

$$(gN)(hN) = ghN \to (gh)'N' = g'h'N' = (g'N')(h'N').$$

Thus the factor group G/N is mapped homomorphically on the factor group G'/N'.

<u>Corollary</u>: <u>If the inverse image of</u> N' <u>is</u> N, <u>the homomorphism</u> $G/N \to G'/N'$ <u>is an isomorphism</u>.

<u>Proof</u>: Let $gN \to g'N'$, $hN \to h'N' = g'N'$. Then $(g')^{-1}h'N' = N'$ and $(g')^{-1}h'$ lies in N'. Thus $g^{-1}h$ is in N, and h is in gN. Therefore $gN = hN$.

<u>Definition</u>: If U and V are subgroups of G, UV is the set of all products uv, with $u \in U$ and $v \in V$.

<u>Definition</u>: By $(U \wedge V)$ we denote the distinct

elements of U which also belong to V.

<u>THEOREM 6.1.4</u>: <u>If</u> U <u>and</u> V <u>are subgroups of a group</u> G, U_1 <u>and</u> V_1 <u>normal subgroups of</u> U <u>and</u> V, <u>respectively, then the following three factor groups are isomorphic:</u> $U_1(U\cap V)/U_1(U\cap V_1), V_1(U\cap V)/V_1(U_1\cap V), (U\cap V)/(U_1\cap V)(V_1\cap U)$.

<u>Proof</u>: If $a \in U\cap V$, then $a(U\cap V_1)a^{-1} \subseteq U\cap V_1$. But $a^{-1}(U\cap V_1)a \subseteq U\cap V_1$ implies that $(U\cap V_1) \subseteq a(U\cap V_1)a^{-1}$. Thus $a^{-1}(U\cap V_1)a = U\cap V_1$, and $U\cap V_1$ is a normal subgroup of $U\cap V$. Let S map U on U/U_1. We call $S(U\cap V) = H$ and $S(U\cap V_1) = K$. Then $S^{-1}(H) = U_1(U\cap V)$ ① and $S^{-1}(K) = U_1(U\cap V_1)$ from which it follows from the Corollary to Theorem 6.1.3 that $U_1(U\cap V)/U_1(U\cap V_1)$ is isomorphic to H/K. But if S is defined only over $U\cap V$, then (cf. ①) $S^{-1}(K) = (U_1\cap V)(U\cap V_1)$ so that $[(U\cap V)/(U_1\cap V)(U\cap V_1)]$ is also isomorphic to H/K. Thus the first and third factor groups above are isomorphic to each other. Similarly, the second and third factor groups are isomorphic.

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

<u>Proof</u>: Set $G = U$, $N = U_1$, $H = V$ and the identity $e = V_1$ in Theorem 6.1.4 and the proof is immediate.

<u>Corollary 2</u>: <u>Under the conditions of Corollary 1, if G/N is abelian, so also is</u> $H/H\cap N$.

①Suppose $u \to uU_1 \subset H$. Thus $uU_1 = u_vU_1$, where $u_v \subset (U\cap V)$. Since $uU_1 \supset u$, $u = u_vu_1$, where $u_1 \subset U_1$, and thus $u \subset U_1[U\cap V]$.

Proof: By Corollary 1, if G/N is abelian so is HN/N, a subgroup of G/N. But $H/H \cap N$ is isomorphic to HN/N, so then also is $H/H \cap N$ abelian.

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

THEOREM 6.1.5: Any subgroup H of a solvable group G is solvable.

Proof: Let $H_i = H \cap G_i$. If $G_{i-1} = G$, $G_i = N$, $H_{i-1} = H$ of Corollary 2, Theorem 6.1.4 then H_{i-1}/H_i is abelian.

THEOREM 6.1.6: The homomorphic image of a solvable group is solvable.

Proof: Let $S(G) = G'$, and define $S(G_i) = G'_i$ where G_i belongs to a sequence exhibiting the solvability of G. By Theorem 6.1.3 there exists a homorphism 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' which completes the proof.

Definition: Any one-to-one mapping of a set of n objects on itself is called a permutation where the product of such permutations is a successive application of the mappings.

Definition: The set of all such mappings of n elements forms a group, called the symmetric group of degree n.

We will let the n objects be the numbers $1, 2, \ldots, n$.

We will let $(123\ldots n)$ be the mapping S such that $S(i) \equiv i + 1 \pmod{n}$ and generally $(ij\ldots m)$ is the mapping T such that $T(i) = j, \ldots, T(m) = i$. If $(ij\ldots m)$ has k numbers, then we call $(ij\ldots m)$ a k-cycle. If $T = (ij\ldots s)$ then we see that $T^{-1} = (s\ldots ji)$.

Lemma 6.1.7: *If a subgroup U of the symmetric group of degree $n > 4$ contains every 3-cycle of the symmetric group of degree n, and if U_1 is a normal subgroup of U such that U/U_1 is abelian, then U_1 contains every 3-cycle.*

Proof: Consider the natural homomorphism $U \to U/U_1 = U'$, and let $u = (ijk)$ and $v = (krs)$ be two elements of U where i,j,k,r,s are five distinct integers $\leq n$. If $u \to u'$, $v \to v'$, then $u^{-1}v^{-1}uv \to u'^{-1}v'^{-1}u'v' = e'$, since U' is abelian. Thus $u^{-1}v^{-1}uv$ belongs to U_1. But

$$u^{-1}v^{-1}uv = (kji)(srk)(ijk)(krs) = (kri)$$

and for each k,r,i, we have (kri) belongs to U_1.

THEOREM 6.1.8: *The symmetric group G of degree n is not solvable for $n > 4$.*

Proof: If there were a sequence exhibiting the solvability of G, since G contains every 3-cycle so would each succeeding group, by Lemma 6.1.7, and the sequence could not end with the unit.

6.2 Solution of equations by Radicals.

Definition: The extension field E over F is called an extension by radicals if there exist intermediate fields $F = B_0 \subset B_1 \subset B_2 \subset \cdots \subset B_r = E$ and $B_i = B_{i-1}(\alpha_i)$ where each α_i is a root of an equation[1] of the form $x^{n_i} - a_{i-1} = 0$, where a_{i-1} is in B_{i-1}, $i = 1,2,\ldots,r$.

<u>Definition</u>: A polynomial f(x) in a field F is said to be solvable by radicals if its splitting field lies in an extension of F by radicals.

In the remainder of this article <u>we assume</u>, unless stated otherwise, <u>that the base field</u> F <u>has characteristic zero</u>, and that F <u>contains</u> as many <u>roots of unity</u> as are needed.

<u>Lemma 6.2.1</u>: <u>Any extension of</u> F <u>by radicals can always be extended to an extension of</u> F <u>by radicals which is normal over</u> F.

<u>Proof</u>: Let $E = B_r \supset B_{r-1} \supset \cdots \supset B_1 = F(\alpha_1) \supset B_0 = F$. B_1 contains α_1 and also $e\alpha_1, e^2\alpha_1, \ldots, e^{n_1-1}\alpha_1$, where e is any n_1-th root of unity. Thus B_1 is the splitting field of $x^{n_1} - a_0$, $a_0 \in F$ and by Theorem 3.4.3 is therefore a normal extension of B . If $f_1(x) = \prod_T \left[x^{n_2} - T(a_1)\right]$, $(a_1 \in B_1)$, where T takes all values of the group of automorphisms of B_1 over B_0, then f_1 is in B_0, and if we adjoin successively to B_1 the roots of $x^{n_2} - T(a_1)$ for each T we get an extension of B_2 which is normal over F. Continuing in this way we arrive at an extension of E by radicals which will be normal over F.

<u>THEOREM 6.2.2</u>: <u>The polynomial</u> f(x) <u>is solvable by radicals if and only if its group is solvable</u>.

<u>Proof: Suppose f(x) is solvable by radicals. Let</u>

[1]We say that B_i is a pure extension of B_{i-1} if $x^{n_i} - a_{i-1} = 0$ is irreducible.

E be a normal extension of F by radicals containing the splitting field B of f(x), and call G the group of E over F. Since for each i, B_i is a Kummer extension of B_{i-1}, the group of B_i over B_{i-1} is abelian by Theorem 4.4.1. Since $G_{B_{i-1}}$ is the group of E over B_{i-1} and B_i is a normal extension of B_{i-1} then in the sequence of groups $G = G_{B_o} \supset G_{B_1} \supset \ldots \supset G_{B_r} = 1$ each is a normal subgroup of the preceding. But $G_{B_{i-1}}/G_{B_i}$ is isomorphic to the group of B_i over B_{i-1} and hence is abelian. Thus G is solvable. Now G_B is a normal subgroup of G, and G/G_B is isomorphic to the group of B over F, and is therefore the group of the polynomial f(x). But G/G_B is a homomorphic image of the solvable group G and hence is itself solvable.

Conversely, let the group G of f(x) be solvable, and E be the splitting field of f(x). Let $G = G_o \supset G_1 \supset \ldots \supset G_r = 1$ be a sequence with abelian factor groups. Let B_i be the fixed field for G_i. Since G_{i-1} is the group of E over B_{i-1} and G_i is a normal subgroup of G_{i-1}, then B_i by Theorem 3.4.8 is normal over B_{i-1} and the group G_{i-1}/G_i is abelian. By Theorem 4.4.4 B_i is a Kummer extension of B_{i-1}, and by definition it is a splitting field of a polynomial of the form $(x^n - a_1)(x^n - a_2)\ldots(x^n - a_s)$. By forming the successive splitting fields of the $x^n - a_k$ we see that B_i is an extension of B_{i-1} by radicals. Therefore E is an extension by radicals of F which completes the proof.

6.3 The General Equation of Degree n.

If F is a field, the totality of rational expressions in the indeterminates $u_1, u_2, \ldots, u_n$ with coefficients in F is a field $F(u_1, u_2, \ldots, u_n)$. That is, every element in $F(u_1, \ldots, u_n)$ is the quotient $Q(u_1, \ldots, u_n)$ of two polynomials $R(u_1, \ldots, u_n)/S(u_1, \ldots, u_n)$ with coefficients in F.

Definition: We define the general polynomial of degree n as

$$f(x) = x^n - u_1 x^{n-1} + \ldots + (-1)^n u_n. \tag{6.3.1}$$

THEOREM 6.3.1: If E is the splitting field of the polynomial $f(x)$ in (6.3.1) over $F(u_1, u_2, \ldots, u_n)$ then the group of E over $F(u_1, u_2, \ldots, u_n)$ is the symmetric group.

Proof: If $v_1, \ldots, v_n$ are the roots of $f(x)$ in E, then $u_1 = v_1 + v_2 + \ldots + v_n$, $u_2 = v_1 v_2 + v_1 v_3 + \ldots + v_{n-1} v_n$, $\ldots$, $u_n = v_1 v_2 \ldots v_n$. We let $F(x_1, \ldots, x_n)$ be the field generated from F by the variables $x_1, \ldots, x_n$. Also we let $\alpha_1 = x_1 + \ldots + x_n$, $\alpha_2 = x_1 x_2 + x_1 x_3 + \ldots + x_{n-1} x_n, \ldots,$ $\alpha_n = x_1 x_2 \ldots x_n$ be the elementary symmetric functions, that is, $(x - x_1)(x - x_2)\ldots(x - x_n) = x^n - \alpha_1 x^{n-1} + \ldots + (-1)^n \alpha_n = f^*(x)$. If $g(\alpha_1, \ldots, \alpha_n)$ is a polynomial in $\alpha_1, \alpha_2, \ldots, \alpha_n$ and if we have

$$h(x_1, \ldots, x_n) = g\left(\sum_i^n x_i, \sum_{i<k}^n x_i x_k, \ldots\right) = 0, \tag{6.3.2}$$

then relation (6.3.2) would still hold if the x_i were replaced by the v_i. That is, $g\left(\sum_i^n v_i, \sum_{i<k}^n v_i v_k, \ldots\right)$ would equal zero or $g(u_1, u_2, \ldots, u_n)$ would equal zero which implies g is identically zero. Thus $g(\alpha_1, \alpha_2, \ldots, \alpha_n) = 0$ only if g is the zero polynomial.

We set up the following correspondence between $F(\alpha_1,\ldots,\alpha_n)$ and $F(u_1,u_2,\ldots,u_n)$. Let $f(u_1,\ldots,u_n)/g(u_1,\ldots,u_n)$, an element of $F(u_1,u_2,\ldots,u_n)$, correspond to $f(\alpha_1,\ldots,\alpha_n)/g(\alpha_1,\ldots,\alpha_n)$. This correspondence is a mapping of $F(u_1,u_2,\ldots,u_n)$ on all of $F(\alpha_1,\ldots,\alpha_n)$. Now if

(6.3.3) $f(\alpha_1,\ldots,\alpha_n)/g(\alpha_1,\ldots,\alpha_n)=f_1(\alpha_1,\ldots,\alpha_n)/g_1(\alpha_1,\ldots,\alpha_n)$,

then $fg_1 - gf_1 = 0$. But, by the above discussion, equation (6.3.3) implies that

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

so that

$$f(u_1,\ldots,u_n)/g(u_1,\ldots,u_n) = f_1(u_1,\ldots,u_n)/g_1(u_1,\ldots,u_n).$$

Thus we have a one-to-one correspondence and thus the mapping of $F(u_1,\ldots,u_n)$ onto $F(\alpha_1,\ldots,\alpha_n)$ is an isomorphism. But under this correspondence $f(x)$ corresponds to $f^*(x)$. Since E and $F(x_1,\ldots,x_n)$ are respectively splitting fields of $f(x)$ and $f^*(x)$, by Theorem 3.1.5 the isomorphism between $F(u_1,u_2,\ldots,u_n)$ and $F(\alpha_1,\alpha_2,\ldots,\alpha_n)$ can be extended to an isomorphism between E and $F(x_1,\ldots,x_n)$. Therefore, the group of E over $F(u_1,\ldots,u_n)$ is isomorphic to the group of $F(x_1,\ldots,x_n)$ over $F(\alpha_1,\ldots,\alpha_n)$.

Each permutation of $x_1,\ldots,x_n$ leaves $\alpha_1,\ldots,\alpha_n$ fixed and, thus, induces an automorphism of $F(x_1,\ldots,x_n)$ which leaves $F(\alpha_1,\ldots,\alpha_n)$ fixed. Conversely, each automorphism of $F(x_1,\ldots,x_n)$ which leaves $F(\alpha_1,\ldots,\alpha_n)$ fixed must permute the roots $x_1,\ldots,x_n$ of $f^*(x)$ and is completely determined by the permutation it effects on $x_1,\ldots,x_n$.

Thus, the group of $F(x_1,\ldots,x_n)$ over $F(\alpha_1,\ldots,\alpha_n)$ is the symmetric group on n letters. But the group of $F(x_1,\ldots,x_n)$ over $F(\alpha_1,\ldots,\alpha_n)$ is isomorphic to the group of E over $F(u_1,\ldots,u_n)$. Therefore the group of E over $F(u_1,\ldots,u_n)$ is the symmetric group which was to be proved.

Corollary: The general equation of degree n is not solvable by radicals if $n > 4$.

Proof: By Theorem 6.1.8 the symmetric group for $n > 4$ is not solvable. Then by Theorem 6.3.1 above, the general equation of degree n is not solvable by radicals if $n > 4$. This completes the proof.

6.4 Solvable Equations of Prime Degree.

If f(x) is a polynomial in a field F, let $\alpha_1,\ldots,\alpha_n$ be the roots of f(x) in the splitting field $E = F(\alpha_1,\ldots,\alpha_n)$. Then each automorphism of E over F maps each root of f(x) into a root of f(x), that is, permutes the roots. Since E is generated by the roots of f(x), different automorphisms must effect distinct permutations. Therefore the group of an equation or the group of E over F is a permutation group acting on the roots $\alpha_1,\alpha_2,\ldots\alpha_n$ of f(x).

Definition: A transformation group G acting on a set S is said to be transitive in S if for $s_1, s_2 \in S$, there is an element $g \in G$ such that $gs_1 = s_2$.

For an irreducible equation p(x) the group of automorphisms is always transitive in the roots. For let α and α' be any two roots of p(x), then $F(\alpha)$ and $F(\alpha')$ are isomorphic where the isomorphism is the identity on F. This isomorphism can be extended to an automorphism of E by Theorem 3.1.5. Thus, there is an automorphism sending any given root into any other root, which establishes the transitivity of the group.

Definition: A permutation T of the numbers $1,2,\ldots,q$ is called a linear substitution modulo q if there exist fixed numbers $b,c,(b \not\equiv 0 \bmod q)$, such that $T(i) \equiv bi + c (\bmod q)$, $i = 1,2,\ldots,q$.

Suppose we let G be a transitive substitution group on the numbers $1,2,\ldots,q$ and let G_1 be a normal subgroup of G. Also let $1,2,\ldots,k$ be the images of one of the numbers, say, 1, under the permutations of G_1. We say that $D_1 = (1,2,\ldots,k)$ is a domain of transitivity of G_1 relative to 1. If $i \leq q$ is any number not in this domain of transitivity, there is a T of G which maps 1 on i. Then $TG_1T^{-1}(i) = TG_1(1) = T(D_1)$. Thus $T(D_1) = T(1,2,\ldots,k)$ is a domain of transitivity of TG_1T^{-1} relative to i. Since G_1 is a normal subgroup of G, we have $G_1 = TG_1T^{-1}$. Thus $G_1(i) = T(D_1)$ 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. Suppose $g_1(1) = h_1(i)$, where $g_1, h_1 \in G_1$. Then $h_1^{-1}g_1(1) = i$, which contradicts our assumption that no element of G_1 maps 1 on i. Thus the numbers $1,2,\ldots,q$ are divided into a collection of mutually exclusive sets, each containing k elements, so that k is a divisor of q. Therefore if q is a prime, either $k = 1$ and G_1 consists of the identity element alone, or $k = q$ and G_1 is also transitive.

THEOREM 6.4.1: Let $p(x)$ be an irreducible equation of prime degree q in a field F. The group G of $p(x)$ which is a permutation group of the roots, or the integers $1,2,\ldots,q$, is solvable if and only if, after a suitable change in the numbering of the roots, G is a group of linear substitutions T, where $T(i) \equiv bi + c \pmod q$, $i = 1,2,\ldots,q$, and in the group G all the substitutions with $b = 1$, $T(i) \equiv i + c$, $(c = 1,2,\ldots,q)$ occur.

Proof: First we let G be solvable and let

$$G = G_o \supset G_1 \supset \ldots \supset G_r \supset G_{r\,1} = 1$$

be a sequence exhibiting the solvability of G. If G_r is not cyclic, we can choose a cyclic subgroup of the abelian group $G_r \equiv G_r/G_{r\,1}$, and then we can insert this new cyclic subgroup into the original sequence. We then consider the new sequence in which this cyclic group is the term before the last. Thus there is no loss in generality if we assume that the penultimate term G_r is cyclic.

If T is a generator of G_r, we can show that T consists of a cycle containing all q of the numbers $1,2,\ldots,q$. For if $T = (1ij\ldots m)(n\ldots p)$ then the powers of T would map 1 into only $1,i,j,\ldots,m$, contradicting the transitivity of G_r. We can number the permutation letters in such a fashion that $T(i) \equiv i + 1 \pmod q$ and $T^c(i) \equiv i + c \pmod q$. Now let

S be any element of G_{r-1}. Since G_r is a normal subgroup of G_{r-1}, STS^{-1} is an element of G_r, say, $STS^{-1} = T^b$. Let $S(i) = j$ or $S^{-1}(j) = i$. Then

$$ST(i) = STS^{-1}(j) = T^b(j) \equiv j + b(\text{mod } q).$$

Therefore $ST(i) \equiv S(i) + b(\text{mod } q)$, or $S(i + 1) \equiv S(i) + b(\text{mod } q)$ for each i. Thus, setting $S(o) = c$, we have $S(1) \equiv c + b$, $S(2) \equiv S(1) + b = c + 2b$, and, in general, $S(i) \equiv c + ib(\text{mod } q)$. Thus each substitution in G_{r-1} is a linear substitution. Also, the only elements of G_{r-1} which leave no i fixed, $i = 1,\ldots,q$ are in G_r, since for each $b \neq 1$, we can take i such that $(b - 1)i \equiv -c(\text{mod } q)$, and this implies that $bi + c \equiv i(\text{mod } q)$, and i is left fixed by S. Thus if no i is feft fixed $b \equiv 1$ and thus the element S of G_{r-1} must be in G_r. By induction, we prove that the elements of G are all linear substitutions, and that the only cycles of q letters are in G_r. Suppose the assertion is true of G_{r-n}. Let S be in G_{r-n-1} and let T be a cycle in G_r and hence in G_{r-n}. Since the transform of a cycle is a cycle,[1] STS^{-1} is a cycle in G_{r-n} and is even in G_r since G_r is a normal subgroup of G. Thus $STS^{-1} = T^b$ for some b. By the preceding argument, S is a linear substitution $bi + c$ and if S itself is not in G_r, then S leaves one integer fixed and hence is not a cycle of q elements.

[1]If $T = (i,j,\ldots,m)$, $STS^{-1}\left[S(i)\right] = ST(i) = S(j)$, while if $k \neq i,j,\ldots,m$, $STS^{-1}\left[S(k)\right] = ST(h) = S(k)$. Thus STS^{-1} is the cycle $\left[S(i),S(j),\ldots,S(m)\right]$.

Conversely, let G be a group of linear substitutions which contains a subgroup N of the form $T(i) \equiv i + c \pmod{q}$. Since the only linear substitutions which do not leave an integer fixed are in 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 NS where $S(i) \equiv bi + c \pmod{q}$ the substitution $T^{-1}S$ occurs where $T(i) \equiv i + c \pmod{q}$. But $T^{-1}S(i) \equiv (bi + c) - c = bi \pmod{q}$. Also, if $S(i) \equiv bi \pmod{q}$ and $S'(i) \equiv b'i \pmod{q}$ then $SS'(i) \equiv bb'i \pmod{q}$. Thus, the factor group (G/N) is isomorphic to a multiplicative subgroup of the numbers $1, 2, \ldots, q-1 \pmod{q}$ and is therefore abelian. Since (G/N) and N are both abelian, G is solvable which completes the proof.

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

Proof: Each substitution is linear modulo q. Now the congruence $bi + c \equiv i \pmod{q}$ has no solution in the case $b \equiv 1$, $c \not\equiv 0$ and it has exactly one solution in the case $b \equiv 1$. Finally, if $b \equiv 1$, $c \equiv 0$ the substitution is the identity and thus Corollary 1 is proved.

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: By Theorem 6.4.1 the group of the equation, G, is a solvable, transitive, substitution group on q letters where q is prime. In the splitting field, E, of the equation, which is 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. This proves Corollary 2.

CHAPTER VII

A METHOD OF DETERMINING THE GALOIS GROUP[1]

7.1 Finding the Galois Group of an Equation.

We will show how to find the Galois group of a polynomial, after a finite number of operations, which consist of finding the rational roots of certain induced equations. We determine successively whether the Galois group is, or is not, contained in each of the subgroups of the symmetric group, S_n, of degree equal to the degree of the given equation.

In this chapter we will assume that the equation under consideration is of the form

$$p(x) = x^n + a_1 x^{n-1} + \dots + a_n = 0$$

where the coefficients belong to a separable field F of characteristic 0. We let G denote the group of p(x) relative to F, and we let H, of order m, denote any fixed subgroup of the symmetric group S_n of degree n. G and H can be considered to be permutation subgroups on n symbols. We let $\alpha_1, \alpha_2, \dots, \alpha_n$ be the roots of $p(x) = 0$. We construct a function, $f_1(x_1, x_2, \dots, x_n)$, of the n indeterminants $x_1, x_2, \dots, x_n$, which is invariant under the permutations of H. We first define q_1 to be the function

[1]Cf. Wilson, R.L., A Method for the Determination of the Galois Group. Duke Math. Journal, Vol.17(1950),p.403-8.

$$(7.1.1) \qquad q_1(x_1,x_2,\ldots,x_n) = x_1^{n-1}x_2^{n-2}\ldots x_{n-1}.$$

We next define $q_i(x_1,x_2,\ldots,x_n)$, $i = 1,2,\ldots,m$, to be the functions

$$q_i(x_1,x_2,\ldots,x_n) = q_1\left[h_i(x_1),h_i(x_2),\ldots,h_i(x_n)\right]$$

where h_i are the permutations of H. We finally define $f_1(x_1,x_2,\ldots,x_n)$ to be the function

$$(7.1.2) \qquad f_1(x_1,\ldots,x_n) = \sum_{i=1}^{m} q_i(x_1,x_2,\ldots,x_n).$$

Since the m permutations of H form a group, any permutation of H applied to $f_1(x_1,\ldots,x_n)$ will simply permute the $q_i(x_1,\ldots,x_n)$. Thus f_1 is left invariant under the permutations of H. But any permutation of S_n not in H will not leave f_1 invariant, for such a permutation will carry q_1 into some function not contained in f_1. Upon permuting the indeterminants by a permutation not in H, we obtain a second function $f_2(x_1,\ldots,x_n)$ which is distinct from $f_1(x_1,\ldots,x_n)$. By using all of the permutations s_i of S_n we obtain, say, k distinct polynomials

$$(7.1.3) \quad f_j(x_1,\ldots,x_n) = s_i\left[f_1(x_1,\ldots,x_n)\right], \; j = 1,2,\ldots,k.$$

If s_1 and s_2 are two distinct elements of the same coset of H in S_n, then $s_1 = s_2h$, where $h \in H$. Since $s_1\left[f_1\right] = s_2h\left[f_1\right] = s_2\left[f_1\right]$, s_1 and s_2 map f_1 in the same way. Conversely, if $s_1\left[f_1\right] = s_2\left[f_1\right]$, $s_1^{-1}s_2\left[f_1\right] = f_2$ and $s_1^{-1}s_2 \in H$. Thus $s_2 \in s_1H$. Finally, $k = n!/m$, the index of k in S_n.

<u>Definition</u>: We define the equation

$$(7.1.4) \qquad \Phi(y) = \prod_{j=1}^{k}\left[y - f_i(\alpha_1,\alpha_2,\ldots,\alpha_n)\right] = 0$$

to be the <u>induced equation of</u> H. Since the coefficients of $\Phi(y)$ are symmetric in the roots of $p(x) = 0$, they are in F. Since the functions f_j are not necessarily the only functions of n indeterminates which are invariant under H, $\Phi(x)$ is not necessarily unique. We can easily determine if any of the roots of $\Phi(y) = 0$ lie in F.

THEOREM 7.1.1: The Galois group G relative to the coefficient field F of a separable equation $p(x) = 0$ is uniquely defined by the following properties: (1) Every rational function, with coefficients in F, of the roots of $p(x) = 0$ which is invariant under G is equal to an element of F, (2) Every rational function with coefficients in F of the roots of $p(x) = 0$ which is equal to a number in F is invariant under G.

Proof: The rational functions, with coefficients in F, of the roots of $p(x) = 0$ are elements of the splitting field E of $p(x) = 0$. The elements of F are precisely those elements of E which are invariant under the Galois group of E relative to F.

If none of the roots of $\Phi(y)$ is in F, then $f_1(\alpha_1, \alpha_2, \ldots, \alpha_n)$ is a rational function of the roots of $p(x) = 0$ with coefficients in F, invariant under H, which is not equal to an element in F. By Theorem 7.1.1, part (1), G is not contained in H. Also, if at least one non-repeated root of $\Phi(y)$ belongs to F, then this root is invariant under G, by Theorem 7.1.1, part (2). Since this is a non-repeated root, it is invariant under precisely the permutations of

H, for permutations not in H do not leave a particular f_j invariant. Therefore in this latter case G must be contained in H. Thus we have established the following theorem:

THEOREM 7.1.2: <u>If the equation induced by</u> H <u>has no roots in</u> F, <u>then the Galois group</u> G <u>is not contained in</u> H. <u>If the equation induced by</u> H <u>has at least one non-repeated root in</u> F, <u>then</u> G <u>is either</u> H, <u>or a proper subgroup of</u> H.

If $\Phi(y) = 0$ has only multiple roots in F, conclusions similar to those above can not be drawn, since the functions f_j are then invariant under H and also under permutations which are not in H. In this case, we consider the n! functions,

$$q_1^{(j)} = \alpha_1^{r_1}\alpha_2^{r_2}\cdots\alpha_{n-1}^{r_{n-1}},\ 0 \leq r_i \leq n-i,$$

where the r_i are integers and $j = 1,2,\ldots,n!$ is some labeling of these functions. Since the r_i are such that $0 \leq r_i \leq n-i$, this will give n! functions $q_1^{(j)}$. Now α_1 is a root of $p(x)$ of degree n; α_2 is a root of $p(x)/(x - \alpha_1)$ of degree $n-1$; α_i is a root of $p(x)/(x - \alpha_1)(x - \alpha_2)\ldots(x - \alpha_{i-1})$ of degree $n-i+1$, etc. Therefore, $\alpha_1^{k_1}$ can be reduced to $\alpha_1^{r_1}$, $0 \leq r_1 \leq n-1$; $\alpha_2^{k_2}$ can be reduced to $\alpha_2^{r_2}$, $0 \leq r_2 \leq n-2$; and so on. Thus all the elements of the field E can be expressed rationally in terms of the n! elements $q_1^{(j)}$. The $q_1^{(j)}$ therefore form a generating system for the root field E. Since the $q_1^{(j)}$ are not necessarily distinct, they do not necessarily form a minimal generating system. If H is contained in G, there is an intermediate field B belonging to the group H, such that F is contained in B by Theorem 3.4.4. Since B is a subfield of the splitting field, E, of $p(x) = 0$, any element b_1 of B is of the form

$$b_1 = \sum_{j=1}^{n!} c_j q_1^{(j)}, \quad c_j \in F.$$

Let

$$q_i^{(j)} = h_i\left[q_1^{(j)}\right], \quad i = 1,2,\ldots,m; \; h_i \in H,$$

denote the m elements we obtain from $q_1^{(j)}$ by applying the m permutations h_i of H to the α_i, and denote by

$$b_i = \sum_{j=1}^{n!} c_j q_i^{(j)}, \quad i = 1,2,\ldots m,$$

the m functions which we obtain from b_1 by applying these m permutations to b_1. Since B is the fixed field for H, $b_1 = b_2 = \ldots = b_m$ and hence

$$b_1 = \frac{1}{m}\sum_{i=1}^{m} b_i = \frac{1}{m}\sum_{i=1}^{m}\sum_{j=1}^{n!} c_j q_i^{(j)} = \sum_{j=1}^{n!} c_j \left\{\frac{1}{m}\sum_{i=1}^{m} q_i^{(j)}\right\}.$$

We define

$$f_1^{(j)} = \frac{1}{m}\sum_{i=1}^{m} q_i^{(j)}, \quad j = 1,2,\ldots,n!.$$

Now $f_1^{(j)}$ is invariant under H, since the $q_i^{(j)}$ are permuted by the elements of H. Hence the $f_1^{(j)}$ belong to B, the fixed field of H. Thus the $f_1^{(j)}$ form a generating system for B. If F is properly contained in B, at least one of the $f_1^{(j)}$ is not in F.

(7.1.5) $$f_1(a) = \sum_{j=1}^{n!} a^{j-1} f_1^{(j)}$$

where a is a parameter. Since the $f_1^{(j)}$ are invariant under the permutations of H, then $f_1(a)$ is invariant under H. Now using (7.1.5), instead of (7.1.2), we form the induced equation $\Phi(y,a) = 0$, as in (7.1.4):

$$\Phi(y,a) = \prod_{i=1}^{K}\left[y - f_i(a)\right],$$

where $f_i(a) = s_i\left[f_1(a)\right] = \sum_{j}^{n!} a^{j-1}\left\{s_i\left[f_1^{(j)}\right]\right\}$, $s_i \in S_n$. The induced equation now depends upon the parameter a. If we choose $\left[c(n! - 1) + 1\right]$ distinct values of a in F, we have $\left[c(n! - 1) + 1\right]$ induced equations, one for each value of the parameter if each of these induced equations has a root in F, then one of the $f_i(a)$ must belong to F for at least n! distinct values of a in F. If we denote these values of a by a_t, $t = 1,2,\ldots,n$, and the corresponding values of $f_i(a)$ by d_t, we have, from (7.1.5), the system of equations

(7.1.6) $\quad \sum_{j=1}^{n!} a_t^{j-1} f_i^{(j)} = d_t, \ (t = 1,2,\ldots,n\ ).$

Cramer's rule gives each of the $f_i^{(j)}$ in F, since the coefficients of (7.1.6) are in F, and the determinant of the coefficients of the $f_i^{(j)}$ is the Vandermonde determinant, and hence non-vanishing. But if $H \subset G$, $B \supset F$, and at least one $f_i^{(j)}$ is not in F. Therefore if $H \subset G$ there are only a finite number of values of a such that $\Phi(y,a) = 0$ has roots in F. Also, any such equation having roots in F will have only multiple roots in F by Theorem 7.1.2. Now, if $G \subseteq H$, at least one $f_i(a)$ will be in F for every value of a in F, by Theorem 7.1.2. If $f_u(a) = f_v(a)$ for n! distinct values of a, we will have the system of equations

$$\sum_{j=1}^{n!} a_t^{j-1}\left[f_u^{(j)} - f_v^{(j)}\right] = 0, \ t = 1,2,\ldots,n!.$$

Since, as before, the Vandermonde determinant is not equal to zero, we have $f_u^{(j)} = f_v^{(j)}$, $j = 1,2,\ldots,n!$. But this implies that s_u and s_v belong to the same coset of H in S_n, and even in H the hypothesis (compare with the discussion following equation (7.1.3)) that $s_u H \neq s_v H$. Thus no two $f_i(a)$ can be equal for more than $(n! - 1)$ distinct values of a. Therefore, there are only a finite number of a in F such that $\Phi(y,a) = 0$ has multiple roots in F. Hence by a suitable choice of a, it will be possible in every case to apply Theorem 7.1.2. This proves the following theorem.

THEOREM 7.1.3: For any given polynomial equation and an arbitrary group H, which is a subgroup of the symmetric group S_n of degree n, it is possible to obtain after a finite number of steps an induced equation which has either no roots in F or has non-repeated roots in F.

By using Theorem 7.1.2 we have a means for sifting the possible choices of H for a given equation. If, for a given H, $G \subseteq H$, but G is contained in no subgroup of H, then $G = H$. If G is in no subgroup of the symmetric group of degree n, then G is the symmetric group of degree n.

7.2 An Example of the Method of 7.1.

As an illustration of Theorem 7.1.3 we consider the polynomial

$$p(x) = x^3 - a_1x^2 + a_2x - a_1 = x^3 - x^2 + x - 1 = 0.$$

Now $q_1 = x_1^2x_2$ (cf.(7.1.1)). Let H_1 be (1)(2)(3), (123), (132). Then by applying each permutation of H_1 in turn to q_1 we get $f_1 = x_1^2x_2 + x_2^2x_3 + x_3^2x_1$. Now apply the permutation (12), which is not in H_1, to each element of f_1. Thus we get $f_2 = x_2^2x_1 + x_1^2x_3 + x_3^2x_1$. Replace x_i by α_i. Our induced equation is

$$\Phi(y) = (y - f_1)(y - f_2)$$
$$= y^2 - (a_1a_2 - 3a_3)y + (a_2^3 + a_1^3a_3 + 9a_3^2 - 6a_1a_2a_3)$$
$$= y^2 + 2y + 5 = 0.$$

But this equation has no roots in F, thus G is not contained in H_1.

Next, let $H_2 = (1)(2)(3), (13)$. Then we get

$$f_1 = x_1^2x_2 + x_3^2x_2$$
$$f_2 = x_2^2x_1 + x_3^2x_1$$
$$f_3 = x_1^2x_2 + x_2^2x_3.$$

Replace x_i by α_i. Now

$$\Phi(y_1) = y_1^3 - (f_1 + f_2 + f_3)y_1^2 + (f_1f_2 + f_2f_3 + f_3f_1)y_1 - f_1f_2f_3$$
$$= y_1^3 + 2y_1^2$$

after simplification. Since this equation has a multiple root in F, no conclusions can be drawn.

Let us consider $H_3 = (1)(2)(3), (12)$. Then we get

$$f_1 = x_1^2x_2 + x_2^2x_1$$
$$f_2 = x_3^2x_1 + x_2^2x_3$$
$$f_3 = x_1^2x_3 + x_3^2x_1.$$

Replacing x_i by α_i,

$$\Phi(y_2) = y_2^3 - (f_1 + f_2 + f_3)y_2^2 + (f_1f_2 + f_2f_3 + f_3f_1)y_2 - f_1f_2f_3$$
$$= y_2^3 + 2y_2^2 + 2y_2$$

after simplification. This equation has a non-repeated root in F. But H_3 has no proper subgroups. Therefore H_3 is the Galois group of our equation.

CHAPTER VIII

GALOIS FIELDS

8.1 Further Discussion of Finite Fields.

We will discuss further some general properties of finite fields (cf. 3.2) with particular attention to the cyclotomic polynomial. It was shown in Lemma 2.2.2 that if $F(x)$ and $P(x)$ are relatively prime polynomials over a field K, there exist polynomials $A(x)$ and $B(x)$ such that

$$A(x)F(x) + B(x)P(x) = 1.$$

This holds, in particular, for a Galois field $G.F.(p^n)$, i.e. a finite field of characteristic p containing p^n elements. When $n = 1$ this means

$$A(x)F(x) + B(x)P(x) \equiv 1 (\mathrm{mod}\ p),$$

which can also be expressed in the form

$$A(x)F(x) \equiv 1 [\mathrm{mod}\ p, P(x)].$$

Definition: A polynomial $F(x)$ of degree m belonging to and irreducible in the $G.F.(p^n)$ will be denoted by $I.Q.(m,p^n)$.

THEOREM 8.1.1: Every $I.Q.(m,p^n)$ divides

$$x^{p^{nm}} - x.$$

Proof: Upon dividing any polynomial $G(x)$ belonging to the $G.F.(p^n)$ by $F(x)$ we obtain a remainder of the form

$$a_0 + a_1 x + \dots + a_{m-1} x^{m-1},$$

where the a's are elements of the G.F.(p^n). We denote the p^{nm} distinct residues of the above form by

(8.1.1) $$Y_i,\ i = 0,1,\ldots,p^{nm} - 1,$$

and in particular, by Y_o, the residue 0. Consider the products by a fixed residue $Y_j \neq Y_o$,

(8.1.2) $$Y_j Y_i \quad (i = 1,\ldots,p^{nm} - 1).$$

If $Y_j Y_i \equiv Y_j Y_k \left[\text{mod } F(x)\right]$, then $Y_j(Y_i - Y_k) \equiv 0\left[\text{mod } F(x)\right]$. By Theorem 2.2.3 $Y_i = Y_k$, and hence the products (8.1.2) are all distinct and different from Y_o. Thus the residues obtained on dividing them by F(x) must coincide, apart from their order, with the non-zero residues in (8.1.1). We form the products of the non-zero residues in (8.1.1) and (8.1.2),

$$\prod_{i=1}^{p^{nm}-1} (Y_j Y_i) \equiv \prod_{i=1}^{p^{nm}-1} Y_i \ \left[\text{mod } F(x)\right].$$

Since $\prod_{i=1}^{p^{nm}-1} Y_i \not\equiv 0\left[\text{mod } F(x)\right]$, by Theorem 2.2.3 we have

(8.1.3) $$Y_j^{p^{nm}-1} - 1 \equiv 0\left[\text{mod } F(x)\right].$$

In particular, this is true when Y_j is the residue x.

<u>THEOREM 8.1.2</u>: <u>If</u> f(x) <u>is a polynomial in</u> G.F.(p^n) <u>and</u> t <u>is a non-negative integer</u>,

$$f(x^{p^{nt}}) = \left[f(x)\right]^{p^{nt}}.$$

<u>Proof</u>: Let

$$f(x) = c_o + c_1 x + \ldots + c_k x^k$$

where the c's belong to the G.F.(p^n). From the Corollary to Theorem 3.2.5,

$$c_i^{p^n} = c_i \quad (i = 0,1,\ldots,k). \tag{8.1.4}$$

Raising f(x) to the power p, and noting that the multinomial coefficients of those product terms which are not p-th powers are multiples of p, and hence equal to zero, in G.F.(p^n), we have

$$[f(x)]^p = c_0^p + c_1^p x^p + \ldots + c_k^p x^p.$$

By induction, we obtain

$$[f(x)]^{p^s} = c_0^{p^s} + c_1^{p^s} x^{p^s} + \ldots + c_k^{p^s} x^{p^s}.$$

Applying (8.1.4) we get, for $s = n$,

$$[f(x)]^{p^n} = c_0 + c_1 x^{p^n} + \ldots + c_k x^{p^n}.$$

Theorem 8.1.2 now follows from a simple induction argument.

<u>THEOREM 8.1.3</u>: <u>An</u> I.Q.(m,p^n) <u>divides</u> $x^{p^{nt}} - x$ <u>in the field if and only if</u> t <u>is a multiple of</u> m.

<u>Proof</u>: If $t = ms$, a multiple of m, it follows directly from Theorem 8.1.1 that if F(x) is an I.Q.(m,p^n),

$$x^{p^{nt}} = x^{p^{nms}} = x^{p^{nm\,p^{nm}\cdots p^{nm}}} \equiv x\,[\bmod F(x)]. \tag{8.1.5}$$

Next, suppose that $t = ms + r$, where $0 \leq r < m$. By (8.1.5),

$$x^{p^{nt}} - x = \left[x^{p^{nms}}\right]^{p^{nr}} - x \equiv x^{p^{nr}} - x\,[\bmod F(x)].$$

Hence if $x^{p^{nt}} - x$ is divisible by F(x) in the G.F.(p^n)

$$x^{p^{nr}} \equiv x\,[\bmod F(x)]. \tag{8.1.6}$$

By f(x) we denote any one of the p^{nm} expressions

$$c_0 + c_1x + \dots + c_{m-1}x^{m-1}$$

where the c's are elements of the G.F.(p^n). If (8.1.6) holds, then by Theorem 8.1.2,

$$\left[f(x)\right]^{p^{nr}} = f(x^{p^{nr}}) \equiv f(x)\left[\text{mod } F(x)\right],$$

in other words, the equation

$$(8.1.7) \qquad Y^{p^{nr}} - Y \equiv 0\left[\text{mod } F(x)\right]$$

has p^{nm} distinct solutions $\left[\text{mod } F(x)\right]$. However, an algebraic equation cannot have more distinct solutions than its degree, (compare with the discussion on pg. 14) and hence (8.1.7) is an identity and $r = 0$.

<u>THEOREM 8.1.4</u>: <u>If</u> $F(x)$ <u>is an</u> I.Q.(m,p^n) <u>and</u> $M(x)$ <u>is an</u> I.Q.(h,p^n), <u>where</u> k <u>divides</u> m, <u>then the roots of</u>

$$(8.1.8) \qquad M(Y) \equiv 0\left[\text{mod } F(x)\right]$$

<u>are</u>

$$(8.1.9) \qquad Y_1, Y_1^{p^n}, \dots, Y_1^{p^{n(h-1)}}$$

<u>where</u> Y_1 <u>is any root of</u> (8.1.8) <u>necessarily belonging to a</u> G.F.(p^{nm}).

<u>Proof</u>: By Theorem 8.1.2,

$$M(Y^{p^{nr}}) = \left[M(Y)\right]^{p^{nr}}.$$

Hence if Y_1 is a root of (8.1.8), so is $Y_1^{p^{nr}}$. Since $M(x)$ is an I.Q.(h,p^n), we have by Theorem 8.1.1, with $x = Y_1$,

$$Y_1^{p^{nh}} - Y_1 \equiv M(Y_1).Q(Y_1) \equiv 0\left[\text{mod } F(x)\right].$$

Since m is a multiple of h (cf. (8.1.5)), (8.1.10) $$Y_1^{p^{nm}} \equiv Y_1 \left[\bmod F(x)\right].$$

If

(8.1.11) $$Y_1^{p^{na}} \equiv Y_1^{p^{nb}} \left[\bmod F(x)\right],$$

for $a < b < h$, we would have from (8.1.10), after raising (8.1.11) to the power $p^{n(m-a)}$,

$$Y_1^{p^{nm}} \equiv Y_1 \equiv Y_1^{p^{n(m-a+b)}} \left[\bmod F(x)\right],$$

and by Theorem 8.1.3 m-a+b would be divisible by m. Finally $b-a = 0$, so that any two of the roots (8.1.9) are incongruent mod F(x).

<u>Corollary</u>: <u>In a</u> G.F.(p^{nm}), M(Y) <u>has the decomposition</u>

$$M(Y) = (Y - Y_1)(Y - Y_1^{p^n})\ldots(Y - Y_1^{p^{(h-1)n}}).$$

<u>In particular (cf. Theorem 2.3.3, with</u> x <u>for</u> s), $F(Y) = 0$ <u>has the distinct roots</u>

$$x, x^{p^n}, \ldots, x^{p^{(m-1)n}}.$$

<u>THEOREM 8.1.5</u>: <u>An</u> I.Q.(m,p^n) <u>remains irreducible in the</u> G.F.(p^{nk}) <u>if</u> k <u>is prime to</u> m.

<u>Proof</u>: The roots of an equation $F(Y) = 0$ of degree m in a G.F.(p^n) are

$$x, x^{p^n}, x^{p^{2n}}, \ldots, x^{p^{(m-1)n}}$$

all belonging to the G.F.(p^{nm}). If F(Y) is reducible in the G.F.(p^{kn}), the root x will satisfy an I.Q.(t,p^{kn}), $t < m$, of the form

$$(8.1.12)\quad (Y - x)(Y - x^{p^{kn}})\ldots(Y - x^{p^{kn(t-1)}}) = 0.$$

The constant term of (8.1.12) must be an element of the G.F.(p^{kn}) so that by the Corollary to Theorem 3.2.5

$$\left[x^{1+p^{kn}+p^{2kn}+\cdots+p^{(t-1)kn}}\right](p^{kn}-1) = x^{p^{tkn}-1} = 1$$

in the G.F.(p^{kn}). By Theorem 8.1.3, tk is a multiple of m, and therefore t is a multiple of m which contradicts $t < m$.

<u>THEOREM 8.1.6</u>: <u>An</u> I.Q.(m,p^n) <u>decomposes in the</u> G.F.(p^{nk}) <u>into</u> d <u>factors each of which is an</u> I.Q.($m/d,p^{nk}$), <u>where</u> $(m,k) = d$.

<u>Proof</u>: Given F(x), the roots of F(Y) = 0 in the G.F.(p^{nm}) are

$$x, x^{p^n}, x^{p^{2n}}, \ldots, x^{p^{(m-1)n}}, \left[x^{p^{nm}} = x \text{ in the G.F.}(p^{nm})\right].$$

They may be separated into d sets of m/d roots each,

$$x^{p^{ni}}, x^{p^{n(d+i)}}, x^{p^{n(2d+i)}}, \ldots, x^{p^{n[(m/d-1)+i]}},$$

for $i = 0,1,\ldots,d-1$. From Theorem 8.1.2 a symmetric function of the roots in one set is unaltered upon being raised to the power p^{nd} and therefore belongs to the G.F.(p^{nd}). The roots of the general set therefore satisfy an equation

$$F_i(Y) = (Y - x^{p^{ni}})(Y - x^{p^{n(d+i)}})\ldots = 0.$$

Let $x = \alpha_1, x^{p^{nd}} = \alpha_2, \ldots, x^{p^{n(\frac{m}{d}-1)d}} = \alpha_{\frac{m}{d}},$

with coefficients belonging to the G.F.(p^{nd}) and thus to the G.F.(p^{nk}). If

$$(8.1.13)\quad F_o(Y) = (Y-\alpha_1)(Y-\alpha_2)\dots(Y-\alpha_{\frac{m}{d}}) = Y^{\frac{m}{d}} - a_1 Y^{\frac{m}{d}-1} + \dots + (-1)^{m/d} a_{\frac{m}{d}}$$

then

$$a_1 = \sum \alpha_r, a_2 = \sum \alpha_r\alpha_s, \dots .$$

Let

$$F_i(Y) = (Y-\alpha_1^{p^{ni}})(Y-\alpha_2^{p^{ni}})\dots(Y-\alpha_{\frac{m}{d}}^{p^{ni}}) = Y^{\frac{m}{d}} - a_1^{(i)} Y^{\frac{m}{d}-1} + \dots + (-1)^{\frac{m}{d}} a_{\frac{m}{d}}^{(i)},$$

so that

$$a_1^{(i)} = \sum \alpha_r^{p^{ni}}, a_2^{(i)} = \sum \alpha_r^{p^{ni}}\alpha_s^{p^{ni}}, \dots .$$

Now

$$a_1^{(i)} = \sum \alpha_r^{p^{ni}} = (\sum \alpha_r)^{p^{ni}} = a_1^{p^{ni}},$$

$$a_2^{(i)} = \sum \alpha_r^{p^{ni}}\alpha_s^{p^{ni}} = (\sum \alpha_r\alpha_s)^{p^{ni}} = a_2^{p^{ni}}, \dots .$$

Thus

$$(8.1.14)\quad F_i(Y) \equiv Y^{\frac{m}{d}} - a_1^{p^{ni}} Y^{\frac{m}{d}-1} + \dots + (-1)^{\frac{m}{d}} a_{m/d}^{p^{ni}}.$$

We next prove that the $F_i(Y)$ are irreducible in the G.F.(p^{nd}). Suppose on the contrary, that in the latter field

$$F_o(Y) = f_o(Y)M_o(Y).$$

Then

$$F_i(Y) = f_i(Y)M_i(Y),$$

each coefficient of $f_{i+1}(Y)$ being the power p^n of the corresponding one of $f_i(Y)$, and each coefficient of f_o

being the power p^n of the corresponding one of f_{d-1}. The coefficients of the product $f_o f_1 \dots f_{d-1}$ are consequently unchanged when we replace the coefficients of each f_i by their p^n-th powers. Therefore the coefficients of the product $f_o f_1 \dots f_{d-1}$ are unaltered upon being raised to the power p^n. Hence that product belongs to the G.F.(p^n), so that $F(x)$ would be reducible in that field, contrary to our hypothesis. Since the degree, m/d, of $F_i(Y)$, an I.Q.$(m/d, p^{nd})$, is relatively prime to k/d, $F_i(Y)$, is irreducible in the G.F.(p^{nk}) by Theorem 8.1.5. This completes the proof.

8.2 Primitive roots of Unity.

Let F be a G.F.(m), $m = p^n$, and let s be an indeterminate. We consider the field $K = F(s)$, of all rational functions of s with coefficients in F. By the Corollary to Theorem 3.2.5, the non-zero elements of $F =$ G.F.(p^n) form a cyclic group of order $m-1 = p^n-1$, generated by some element a.

Let q be a prime number. Let e be a primitive q-th root of unity, so that

$$e^q - 1 = 0. \tag{8.2.1}$$

Let $K_q = K(e)$. If $q = p$, $x^p - 1 = (x - 1)^p$, and all the roots of $x^q - 1 = 0$ are equal to e. In the following, we consider the case $q \neq p$. Any primitive q-th root e of unity satisfies the cyclotomic equation

$$C(x) = (x^q - 1)/(x - 1) = x^{q-1} + x^{q-2} + \dots + 1 = 0. \tag{8.2.2}$$

The remaining roots of (8.2.2) are $e^2, e^3, \ldots, e^{q-1}$.

THEOREM 8.2.1: All the primitive q-th roots of unity belong to K if and only if $q \neq p$ is a divisor of $m - 1 = p^n - 1$.

Proof: The problem of determining the primitive q-th roots of unity in K is equivalent to that of determining the reducibility of $C(x)$ in K. Consider any polynomial $f(x)$ whose coefficients lie in F and hence in K also. Suppose we have a decomposition of $f(x)$ into irreducible factors in F. Then, a further decomposition of $f(x)$ in K is not possible. For if $Q(x)$, with coefficients in F is irreducible in F, while $Q(x) = Q_1(x)Q_2(x)$ in K, then at least one of the factors $Q_1(x), Q_2(x)$ must contain s. But then their product $Q_1(x)Q_2(x)$ contains s. Thus all the questions relative to the reducibility of $f(x)$ in K reduce to those in F.

Now, $f(x)$ is completely reducible in F (and hence also in K) if and only if one (and hence every) primitive q-th root of unity e exists in F.

We determine the condition under which (8.2.1) has a root $e \neq 1$ in F. Now $x = a^t$ is a solution of $x^q - 1 = 0$, if and only if $a^{tq} = 1$, i.e., $tq \equiv 0 (\mathrm{mod}\ m-1)$. If $(q, m-1) = 1$, then $t \equiv 0 (\mathrm{mod}\ m-1)$ is the only solution of this congruence, and accordingly $x = 1$ is the only root of (8.2.1). On the other hand, if $(q, m-1) = q$, the congruence has a non-trivial solution $t \equiv 0(\mathrm{mod}\ m-1/q)$, and we can take $x = a^{m-1/q}$ as a primitive root of (8.2.1). This proves Theorem 8.2.1.

In general, the question of the reducibility of $C(x)$ is answered by the following theorem.

THEOREM 8.2.2: If k is the smallest exponent for which $m^k \equiv 1 \pmod q$, then $C(x)$ in (8.2.2) decomposes in $F = G.F.(m)$ (and hence in K also) into irreducible factors of degree k.

Proof: Let

$$f(x) = x^k - a_1 x^{k-1} + \dots + (-1)^k a_k \tag{8.2.3}$$
$$= (x-\alpha_1)(x-\alpha_2)\dots(x-\alpha_k)$$

be any polynomial with coefficients in F. As in (8.1.13) and (8.1.14)

$$f^*(x) = (x-\alpha_1^{m^t})(x-\alpha_2^{m^t})\dots(x-\alpha_k^{m^t})$$
$$= x^k - a_1^{m^t} x^{k-1} + \dots + (-1)^k a_k^{m^t}.$$

As in (8.1.4) $c^{m^t} = c^{p^{nt}} = c$ for every element c in F. In particular, $a_1^{m^t} = a_1, a_2^{m^t} = a_2, \dots$ and hence

$$f^*(x) = f(x). \tag{8.2.4}$$

Thus if α is any root of $f(x) = 0$, then $\alpha^m, \alpha^{m^2}, \dots$ are also roots. Let $f(x)$ be an irreducible factor of $C(x)$. If $e \neq 1$ is a root of $f(x)$, then e is automatically a primitive q-th root of unity, and, from (8.2.4), $e^m, e^{m^2}, \dots$, are also roots of $f(x)$. Since $f(x)$ has degree $\leq q-1$, $f(x)$ has at most $q-1$ roots. If the residues $m, m^2, \dots, m^{q-1} \equiv 1 \pmod q$ are all distinct, $e^m, e^{m^2}, \dots, e^{m^{q-1}} = e$ are $q-1$

distinct primitive q-th roots of unity which are also roots of $f(x)$. Hence $f(x)$ is divisible by the linear factors corresponding to all the primitive q-th roots of unity. Thus $f(x) = C(x)$, that is, $C(x)$ is irreducible.

However, if $k < q-1$ is the least integer, for which

$$m^k \equiv 1 \pmod q$$

then $f(x)$ is divisible by the product

$$\begin{aligned} f_1(x) &= (x - e)(x - e^m)\dots(x - e^{m^{k-1}}) \\ &= x^k - b_1 x^{k-1} + \dots + (-1)^k b_k, \text{ say.} \end{aligned}$$

Since the b's are elementary symmetric functions of the roots,

$$\begin{aligned} b_i^m &= \left[b_i(e, e^m, e^{m^2}, \dots, e^{m^{k-1}})\right]^m \\ &= b_i(e^m, e^{m^2}, \dots, e) \\ &= b_i(e, e^m, e^{m^2}, \dots, e^{m^{k-1}}) \\ &= b_i. \end{aligned}$$

Thus the b_i are all roots of the equation

$$Y^m - Y = 0.$$

Every element of F satisfies this equation and the $m = p^n$ elements of F are its only roots, since an equation of degree m cannot have more than m roots. Thus every b_i is an element of F. Since $f_1(x)$ is a factor of the irreducible polynomial $f(x)$, we have

$$f_1(x) = f(x).$$

Thus every irreducible factor of $f(x)$ is of degree k, and so k is a divisor of q-1, say $kh = q-1$. All the primitive roots of unity can be arranged in h rows; each containing k conjugate roots:

$$e_1, e_1^m, \ldots, e_1^{m^{k-1}}$$
$$\ldots\ldots\ldots\ldots$$
$$e_h, e_h^m, \ldots, e_h^{m^{k-1}}.$$

This proves Theorem 8.2.2.

Let $(r,p) = 1$. To K adjoin an r-th root of unity, e_r, and let $K_r = K(e_r)$. Thus e_r satisfies the equation $x^r - 1 = 0$. Let

$$C_r(x) = x^{r-1} + x^{r-2} + \ldots + 1.$$

<u>THEOREM 8.2.3</u>: <u>If</u> $F = G.F.(p^n)$, <u>then</u> $C_r(x)$ <u>factors in</u> F (<u>and also in</u> $K = F(s)$) <u>into irreducible factors of degree</u> k, <u>where</u> k <u>is the least positive integer for which</u>

(8.2.5) $$m^k \equiv 1 \pmod r.$$

<u>Proof</u>: Let

$$f(x) = x^h + a_1x^{h-1} + \ldots + a_h$$

be an irreducible factor of $C_r(x)$ in F and let e_r be any root of $f(x) = 0$. After raising $f(x)$ to the power m^t, we have (cf.(8.1.4))

$$[f(x)]^{m^t} = x^{hm^t} + a_1x^{(h-1)m^t} + \ldots + a_h.$$

This implies that along with e_r, we have $e_r^m, e_r^{m^2}, \ldots, e_r^{m^{k-1}}$ also as roots of $f(x) = 0$. Thus $f(x)$ is divisible by the product

$$g(x) = (x - e_r)(x - e_r^m)\ldots(x - e_r^{m^{k-1}}).$$

The $e_r, e_r^m, e_r^{m^2}, \ldots, e_r^{m^{k-1}}$ are distinct primitive r-th roots of unity. Letting

$$g(x) = x^k + a_1 x^{k-1} + \ldots + a_k$$

it follows that the a's are symmetric functions of

$e_r, e_r^m, \ldots, e_r^{m^{k-1}}$, and hence

$$\begin{aligned} a_i^m &= \left[a_i(e_r, e_r^m, \ldots, e_r^{m^{k-1}})\right]^m \\ &= a_i(e_r^m, e_r^{m^2}, \ldots, e_r) \\ &= a_i(e_r, e_r^m, \ldots, e_r^{m^{k-1}}) = a_i. \end{aligned}$$

Thus the a_i is a root of the equation

$$Y^m = Y$$

of degree m whose roots are precisely the m elements of F. Thus the a's belong to F and, consequently, $g(x) = f(x)$. Therefore $h = k$, and the theorem is proved.

CHAPTER IX

A CRITERION FOR SOLVABILITY BY RADICALS IN A FIELD OF PRIME CHARACTERISTIC[1]

The Galois criterion for solvability by radicals given in Chapter VI is valid for fields of characteristic zero, but not in those of prime characteristic. The criterion which we now consider is valid in any field and emphasizes further the importance of primitive roots of unity and the cyclotomic polynomial in the theory of solvability by radicals.

9.1 Absolutely Algebraic Fields.

Definition: A field which has no proper subfields is called a prime field P.

P is either isomorphic to the field of rational numbers or to a field of residues(mod p), where p is a prime.[2]

When we are considering a simple extension F(x) of a field F, we have two cases to consider. The first corresponds to the assumption that two elements $\sum a_k x^k$, $\sum b_k x^k$ of F(x) are equal only when for every k, $a_k = b_k$, while in the second case the two elements may be equal when $a_k \neq b_k$ for some k. In the first case, the element x is called transcendental over F, while in the second

[1] R.L.Brewer, Amer. Jl. of Math. vol. 63, 1941 p.119-126.

[2] C.C.Macduffee, An Introduction to Abstract Algebra, p.157.

case it is called algebraic over F (cf. 2.3). When an element α of a field E is algebraic over a subfield F, it is naturally also algebraic over every intermediate field between E and F. In particular, if α is algebraic over the prime field P contained in E, then α is algebraic over every subfield of E. Such an element is called absolutely algebraic. Similarly, we call a field absolutely algebraic when it is algebraic over its prime field P, or, in other words, when all its elements are absolutely algebraic.

Definition: The absolute degree of a field E is its degree over its prime field P. Thus, if the absolute degree of a field E is m, then $(E/P) = m$.

9.2 G-adic Numbers[1].

Suppose p is any fixed prime number. We consider the absolutely algebraic fields of prime characteristic p. These include all the finite extensions of P, i.e., every finite extension of P is an absolutely algebraic field, for example G.F.(p^n).

Consider all the prime numbers q_i in their natural order:

$$q_1 = 2, q_2 = 3, q_3 = 5, \ldots .$$

Then every positive integer can be represented as an infinite product

$$m = \prod_{i=1}^{\infty} q_i^{x_i} \tag{9.2.1}$$

where the exponents x_i are positive integers, and only a

[1]German: Grad = degree.

finite number of them are different from zero. More generally, we now consider, symbolically, all expressions of the form (9.2.1) in which every exponent x_i is a fixed non-negative integer, or ∞. We call this expression a G-number.

The class of all G-numbers includes the natural numbers, and in agreement with the laws of integers, we postulate the following laws: Two G-numbers

$$m = \prod q_i^{x_i}, n = \prod q_i^{y_i}$$

are <u>equal</u> if and only if $x_i = y_i$ for every i. Also m is <u>divisible</u> by n if and only if for every i, $y_i \leq x_i$. If m is divisible by n, we define the <u>quotient</u>

$$m/n = \prod q_i^{x_i - y_i}$$

where $x_i - y_i$ is set equal to zero when $x_i = \infty$, $y_i = \infty$, and $x_i - y_i$ is set equal to ∞ when $x_i = \infty$ and y_i is finite. Thus all G-numbers are divisible by 1, and all divide that G-number which has the general exponent $x_i = \infty$.

Every(finite or infinite) set of G-numbers has always a greatest common divisor d, which contains all the common divisors, and a least common multiple v which is contained in all the common multiples. The exponent of q_i in d is the same as the least exponent of q_i which occurs in any G-number of the set, and the exponent of q_i in v, is the same as the greatest of these exponents. Now, in case the latter does not exist(consider, for example, the set of positive even integers), the exponent of q_i is taken to be ∞.

If m is any G-number, then the set S of natural numbers which are contained in m have the following properties:

(1) If n is a number of S, then every divisor of n belongs to S.

(2) If n_1, n_2 are numbers of S, then their least common multiple is also a number in S.

Thus in every case, the G-number m is the least common multiple of all the numbers of S, and is therefore entirely determined by the system S. Conversely, if any system S of natural numbers has the properties (1) and (2), above, and if m is the least common multiple of all the numbers of S, then S is the set of positive integers which are contained in m.

Now let E be any absolutely algebraic field of characteristic p. The degree of any finite field which is contained in E belongs to a system S of natural numbers which has the properties (1) and (2) above. Let m be the least common multiple of the numbers of S. If m is a natural number, then E is a finite field of degree m. Conversely, if E is a finite field, then S represents the set of degrees of the subfields of E. We shall denote by m the absolute degree of E in cases where E is not finite and m is not a natural number. Thus every absolutely algebraic field E of characteristic p has a determined degree m which is a G-number, and which is called the absolute degree of E.

We shall denote by $A(p,n)$ the absolutely algebraic field of prime characteristic p and absolute degree n. Thus when n is finite $A(p,n) = G.F.(p^n)$, is the Galois field containing p^n elements.

THEOREM 9.2.1: An irreducible polynomial $F(x)$ of degree m in the $A(p,n)$ factors in the $A(p,nk)$ into d distinct irreducible factors each of degree m/d where $(m,k) = d$.

Proof: The coefficients of $F(x)$ are all algebraic over the prime field $P = G.F.(p)$, and hence they belong to some $G.F.(p^h)$, where h is a divisor of n. Since d is a divisor of k, $G.F.(p^{hd}) \subseteq A(p,nk)$. By Theorem 8.1.6 $F(x)$ factors in the $G.F.(p^{hd})$ into d distinct irreducible factors

$$(9.2.1) \qquad F(x) = F_0(x)F_1(x)\ldots F_{d-1}(x)$$

each of degree m/d. We wish to show that these are the irreducible factors of $F(x)$ in the $A(p,nk)$. Let

$$(9.2.2) \qquad F(x) = f_0(x)f_1(x)\ldots f_{s-1}(x)$$

where the $f_i(x)$ are irreducible in the $A(p,nk)$. The coefficients of the $f_i(x)$ belong to some $G.F.(p^c) \subseteq A(p,nk)$. Thus c is a divisor of nk. Let $c = ab$, where a is a divisor of n and b is a divisor of k; let v_1h be the l.c.m. of a and h, and let v_2d be the l.c.m. of b and d. Since n is a common multiple of a and h, v_1h divides n. Since k is a common multiple of b and d, $v_2 d$ divides k. Thus

$$G.F.(p^c) = G.F.(p^{ab}) \subseteq G.F.(p^{v_1 h v_2 d}) \subseteq A(p,nk).$$

Therefore G.F.(p^h) and G.F.(p^{hv_1}) are subfields of A(p,n), F(x) is irreducible in these fields, and by Theorem 8.1.6 $(v_1,m) = 1$. Since v_2 is a factor of k/d, and $(k/d,m) = 1$, $(v_2,m) = 1$. Finally, $(v_1 v_2,m) = 1$. Applying Theorem 8.1.5, to the $F_i(x)$ in (9.2.1) which are irreducible in the G.F.(p^{dh}), we conclude that they are irreducible in the G.F.$(p^{dhv_1 v_2})$. Thus F(x) has at most d distinct irreducible factors in the subfield G.F.(p^c) of G.F.$(p^{dhv_1 v_2})$. Thus the factorization (9.2.2) in the A(p,nk) is the same as the factorization (9.2.1) in the G.F.(p^{dh}).

9.3 The Solvability Criterion.

We shall first prove that the set of all absolutely algebraic elements of a field E of prime characteristic is an absolutely algebraic field. Let G.F.(p) = P, and let α and β be any two absolutely algebraic elements of E. Now $1/\alpha$ and $\alpha\beta$ belong to the finite extension $P(\alpha,\beta)$ of P, and hence $1/\alpha$ and $\alpha\beta$ satisfy equations(of degrees $(P(\alpha,\beta):P)$) with coefficients in P. Thus $1/\alpha$ and $\alpha\beta$ are absolutely algebraic(cf. Theorem 1.2.2, and p.12).

__Definition__: The field of all absolutely algebraic elements of a field F of prime characteristic p is called the __maximal absolutely algebraic subfield of__ F and will be denoted by M.A.(p,m), where m is its absolute degree.

__Definition__: The number of residue classes prime to n is denoted by $\phi(n)$ and is called the <u>euler Φ-function</u>[1].

Let $\phi(n) = k$, and let $r_1, \ldots, r_k$ be the set of distinct residues prime to n. If $(p,n) = 1$, then $(pr_i, n) = 1$. Since $pr_i \not\equiv pr_j \pmod n$, if $r_i \not\equiv r_j \pmod n$, then $pr_1, \ldots, pr_k$ is also a set of distinct residues prime to n. Hence $\prod(pr_i) \equiv \prod r_i \pmod n$ from which we get

(9.3.1) $\qquad p^{\phi(n)} \equiv 1 \pmod n$ (Euler's Theorem).

If $n \equiv 0 \pmod p$, say $n = pq$, then

$$x^n - 1 = (x^q)^p - 1 = (x^q - 1)^p,$$

(as in the discussion in Theorem 4.4.1) and no root of unity has an order greater than q. In particular, <u>there are no primitive n-th roots of unity</u>.

If $n \not\equiv 0 \pmod p$ the polynomial $x^n - 1$ is separable, since the only root of its formal derivative function nx^{n-1} is $x = 0$ (cf. Theorem 3.2.12); consequently, as in the introductory remarks in 4.2, there exists a primitive n-th root of unity e, and $e, e^2, e^3, \ldots, e^{n-1}, e^n = 1$, are the n distinct n-th roots of unity.

Let e^k have the order r, $r \leq n$, so that r is the least integer for which $e^{kr} = 1$. Since e has order n, $n \mid kr$ by Lemma 3.2.1. Thus $r = n$ if and only if $(k,n) = 1$. Hence the cyclotomic polynomial

$$C_n(x) = x^{n-1} + x^{n-2} + \ldots + 1$$

has precisely $\phi(n)$ distinct primitive n-th roots of unity, <u>if n is not a multiple of p.</u>

[1] Cf. MacDuffee, Intro. to Abstract Alg., p.32-35.

We shall assume in the following discussion that n is not a multiple of p, and we shall denote by E_n the splitting field of $C_n(x)$ over F.

THEOREM 9.2.2: Let F be a field of characteristic p and let $F \supseteq$ M.A.(p,m). Let $n \not\equiv 0 (\mathrm{mod}\ p)$. Then

$$C_n(x) = x^{n-1} + x^{n-2} + \dots + 1$$

factors in F into $\phi(n)/a$ distinct irreducible(separable) factors each of degree a, where $(\phi(n),m) = d$ and a is the least exponent for which $p^{da} \equiv 1 (\mathrm{mod}\ n)$. Further, the Galois group of $C_n(x)$ over F is cyclic of order a.

Proof: Since d is a divisor of m, the G.F.$(p^d) \subseteq$ A(p,m). By Theorem 8.2.3, $C_n(x)$ factors in the G.F.(p^d) into irreducible factors of degree a. Letting $\phi(n) = dr$ and $m = dk$, we have $(r,k) = 1$. By (9.3.1) $p^{\phi(n)} = p^{dr} \equiv 1 (\mathrm{mod}\ n)$, and since a is the least integer for which $p^{da} \equiv 1 (\mathrm{mod}\ n)$, we have $a \mid r$. Thus $(a,k) = 1$. By Theorem 9.2.1, the irreducible factors of degree a of $C_n(x)$ in the G.F.$(p^d) =$ A(p,d) remain irreducible in the A$(p,kd) =$ A(p,m). Now these are the irreducible factors of $C_n(x)$ in F, since the coefficients of the irreducible factors of $C_n(x)$ in F are symmetric functions of certain of the primitive n-th roots of unity(which are themselves absolutely algebraic) and hence elements of the A$(p,m) \subseteq F$. Since the Galois group H of $C_n(x)$ relative to the G.F.(p^d) is cyclic(cf. the discussion in Theorem 4.2.1) and of order a, and the common degree of the irreducible factors of $C_n(x)$ in F is a, it follows from the properties of the cyclotomic polynomial that H is the Galois group of $C_n(x)$ relative to F, which proves the theorem.

From Theorem 9.2.2 we have the following:

Corollary: Let F be a field of prime characteristic p, $A_F = A(p,m) \subseteq F$. Then $C_n(x)$, $n \not\equiv 0 \pmod p$, is irreducible in F, if and only if $(\phi(n),m) = 1$, and $\phi(n)$ is the least exponent for which $p^{\phi(n)} \equiv 1 \pmod n$.

THEOREM 9.2.3: Let F be a field of prime characteristic p, and let m be composite, $p \nmid m$. Then $F \subseteq E_d \subseteq E_n$ (E_n is the splitting field of $C_n(x)$), where d is a divisor of n. Moreover, if $d = q_1 q_2 \ldots q_r$ is the product of distinct primes then $(E_n/E_d) \mid n$.

Proof: Let $n = kd$. Now any root of $C_d(x)$ is a root $\neq 1$ of $x^d - 1 = 0$, and hence of $x^{dk} - 1 = 0$, and finally, of $C_{dk}(x) = C_n(x)$. Hence $F \subseteq E_d \subseteq E_n$.

Let $A_F = A(p,m)$. If $n = p_1^{r_1} \ldots p_r^{r_r}$ then[1]

$$\phi(n) = n\left(1 - \frac{1}{p_1}\right)\left(1 - \frac{1}{p_2}\right)\ldots\left(1 - \frac{1}{p_r}\right)$$

from which it follows that $\phi(d) \mid \phi(n)$ whenever $d \mid n$. Since $\phi(d) \mid \phi(n)$, it follows from Theorem 9.2.2 that $(E_d/F) = a$ where a is the least exponent for which $p^{da} \equiv 1 \pmod d$ and $d = (\phi(n),m)$. Now if a and b are relatively prime positive integers such that $a \equiv 1 \pmod b$, then $a^{b^{s-1}} \equiv 1 \pmod{b^s}$, for any positive integer s. Thus it follows that

[1] See MacDuffee, Intro. to Abstract Alg. p.23.

$$(p^d)^{e(n/d)} \equiv 1 (\mathrm{mod}\ n).$$

Therefore, if

$$n = q_1^{k_1} q_2^{k_2} \cdots q_r^{k_r},$$

the exponent to which p^d belongs (mod n) is $eq_1^{s_1} \cdots q_r^{s_r}$ where $0 \leq s_i \leq k_i$ $(i = 1, 2, \ldots, r)$. Thus from Theorem 9.2.2 $(E_n/F) = eq_1^{s_1} q_2^{s_2} \cdots q_r^{s_r}$ and thus $(E_n/E_d) = q_1^{s_1} q_2^{s_2} \cdots q_r^{s_r}$, a divisor of n.

9.3. Solvability by Radicals.

Both the fact that primitive n-th roots of unity exist and the fact that $C_n(x)$ is solvable by radicals over a field of characteristic zero for every positive integer n is made use of in the Galois criterion(cf. p.75). However, primitive roots of unity do not exist over a field F of prime characteristic p if $n \equiv 0 (\mathrm{mod}\ p)$, and if $n \not\equiv 0 (\mathrm{mod}\ p)$, $C_n(x)$ may not be solvable by radicals. The recognition of these facts leads to the criterion of Theorem 9.3.1 for solvability by radicals over any field. In the following we let E be a normal extension of F. By Theorem 3.4.3 E is the splitting field of a separable polynomial f(x) in F.

Let K be any extension of F and let N be the splitting field of f(x) in K. The root field N is independent of the particular choice of f(x), and is uniquely determined by F, E, and K. We shall denote it by $N = \{E, K\}$. Now $E \subseteq \{E, K\}$, and $K \subseteq \{E, K\}$. Finally, M will denote the maximal separable extension of F contained in E. As usual, G is the group of E over F, and G is isomorphic to the group of M over F, so that[1] $(M:F) = n$.

THEOREM 9.3.1: Let $f(x)$ be a polynomial in a field F, and let n be the order of the Galois group of $f(x)$ relative to a field F. Then $f(x)$ is solvable by radicals over F if and only if:

(1) G is solvable,

(2) Primitive n-th roots of unity exist over F,

(3) $C_n(x)$ is solvable by radicals over F.

Proof: Sufficiency: Suppose (1), (2), (3) hold. From (2) there exists a chain of fields

$$F \subset F_1 \subset \dots \subset F_r,\ F_r \supseteq E_n$$

where each F_j is pure and of prime degree over F_{j-1}. From (1), H is solvable and hence there exists a chain of fields

$$F_r \subseteq F_{r+1} \subseteq \dots \subseteq F_{r+s} = \{M, F_r\},\ F_{r+s} \supseteq M$$

where each F_{r+i} is normal and of prime degree q_i over F_{r+i-1}. Since $F_r \supseteq E_n$, and $n \equiv 0 (\bmod q_i)$ it follows that $F_r \supseteq E_{q_i}$ and hence F_{r+i} is pure over F_{r+i-1}, $(i = 1,2,\dots,s)$. If $M = E$ then $f(x)$ is solvable by radicals over F. If $M \neq E$, then F is of prime characteristic p, and there exists a chain of fields

$$M = K \subset K_1 \subset \dots \subset K_v = E$$

where $K_j = K_{j-1}(\alpha_i)$, α_i being a root of an irreducible

[1] B.L. van der Waerden, Moderne Algebra, vol.1, sec. ed. Berlin, Julius Springer, 1937, p.125-129.

binomial $x^p - a_j$, a_j in K_{j-1}. Let $K = F_{r+s}$, $K_1 = K(\alpha_1)$, $\ldots$, $K_j = K_{j-1}(\alpha_j)$. Then either $K_j = K_{j-1}$ or K_j is pure and of prime degree p over K_{j-1}, $(j = 1,2,\ldots,v)$. Therefore there exists a chain of fields

$F \subset F_1 \subset \ldots \subset F_r \subset F_{r+1} \subset \ldots \subset F_{r+s} \subset F_{r+s+1} \subset \ldots \subset F_{r+s+t}$, where $F_{r+s+t} \supseteq E$ where each F_i is pure and of prime degree over F_{i-1}, $(i = 1,2,\ldots,r+s+t)$. Hence f(x) is solvable by radicals over F.

<u>Necessity</u>: Suppose f(x) is solvable by radicals over F. If $n = 1$, it is clear that (1), (2), and (3) hold. Suppose $n \neq 1$, and let $p_1,\ldots,p_r$ be the distinct prime factors of n. By our assumption, there exists a chain of fields

(9.3.1) $\quad F \subset F_1 \subset \ldots \subset F_s$, $F_s \supseteq E$,

where $F_i = F_{i-1}(\beta_i)$, β_i being a root of an irreducible binomial $x^{q_i} - b_i$ of prime degree q_i in F_{i-1}, $(i = 1,2,\ldots,s)$. Let $q_{i_1}, q_{i_2}, \ldots, q_{i_g}$ be those primes found among $q_1, q_2, \ldots, q_s$ which are not equal to the characteristic of F. Then if $m = q_{i_1} q_{i_2} \cdots q_{i_g}$, primitive m-th roots of unity exist over F. Now E_m is metacyclic[1] over F and hence there exists a chain of fields

---

[1]A normal field N over F is called metacyclic if there exists a chain of subfields

$$F = N_0 \subset N_1 \subset \ldots \subset N_t = N$$

where N_i is cyclic of prime degree p_i over N_{i-1}, $(i = 1, \ldots, t)$

$$F = K \subset K_1 \subset \dots \subset K_t = E_m,$$

where K_i is normal and of prime degree over K_{i-1}, $(i = 1,2,\dots,t)$. Let $L = K_t$, $L_1 = L(\beta),\dots,$ $L_i = L_{i-1}(\beta_i)$, $(i = 1,2,\dots,s)$. Then since $E_{q_{i_j}} \subseteq K_t$ $(j = 1,2,\dots,g)$, it follows from (9.3.1) that either $L_i = L_{i-1}$ or L_i is pure and of prime degree over L_{i-1} $(i = 1,2,\dots,s)$. Hence there exists a chain of fields

$$F = K \subset K_1 \subset \dots \subset K_t \subset K_{t+1} \subset \dots \subset K_{t+u},\ K_{t+u} \supset M$$

where each K_i is normal and of prime degree over K_{i-1}. Hence H is solvable and likewise G.

If F is of characteristic zero, it is clear that (2) and (3) hold. Suppose F is of characteristic p. Since from (9.3.1) $F_s \supseteq E$, there exists for each p_i, $(i = 1,2,\dots,r)$ a $q_{j_i} = p_i$ such that $\left[\{M,F_{j_i-1}\}, F_{j_i}\right] = F_{j_i}$. Moreover, since M is separable over F, $\left(\{M,F_{j-1}\},F_{j_i}\right)$ is separable over F_{j_i-1}, and being pure over F_{j_i-1} cannot be of degree p over F_{j_i-1}. Hence $p_i \neq p$ $(i = 1,\dots,r)$, and thus primitive n-th roots of unity exist over F. Since $F_{j_i} = F_{j_i-1}(\beta_{j_i}) \subseteq \{M,F_{j_i-1}\}$ and $\{M,F_{j_i-1}\}$ is normal over F_{j_i-1}, $x^{p_i} - b_{j_i}$ has all of its roots in $\{M,F_{j_i-1}\}$, a subfield of F_s $(i = 1,2,\dots,r)$. This implies that $E_{p_i} \subset F_s$, $(i = 1,2,\dots,r)$, and hence $E_d \subseteq F_s$, where $d = p_1p_2\cdots p_r$. If $\{E_n,F_s\} = F_s$, then $C_n(x)$ is solvable by radicals and the proof is complete. If $\{E_n, F_s\} \neq F_s$, it follows from Theorem 9.2.3 that $[\{E_n, F_s\} : F_s]$ is a divisor of n. Thus, since $\{E_n, F_s\}$ is cyclic over F_s, and $E_{p_i} \subseteq F_s$ $(i = 1,2,\ldots,r)$,

there exists a chain of fields

$$F_s \subset F_{s+1} \subset \ldots \subset F_{s+t} = \{E_n, F_s\},$$

where each F_{s+i} is pure and of prime degree over F_{s+i-1}. But $E_n \subseteq \{E_n, F_s\}$; and hence $C_n(x)$ is solvable by radicals over F, and (3) holds. This completes the proof of Theorem 9.3.1.

If F is of characteristic zero, Theorem 9.3.1 is a classical Galois criterion which is equivalent to a number-theoretic condition on the index series of G. If F is of prime characteristic, we will show by means of the next two theorems concerning the cyclotomic polynomial, that the above Theorem 9.3.1 is equivalent to a similar condition on the index series of G.

<u>THEOREM 9.3.2</u>: <u>If</u> n <u>is composite</u>, $n \not\equiv 0 \pmod p$, $C_n(x)$ <u>is solvable by radicals over</u> F <u>of characteristic</u> p, <u>if and only if</u> $C_d(x)$ <u>is solvable by radicals over</u> F <u>for every prime divisor</u> d <u>of</u> n.

<u>Proof</u>: From the definition of solvability by radicals and Theorem 9.2.4 the condition is necessary.

To show that the condition is sufficient, let $p_1, p_2, \ldots, p_r$ be the distinct prime factors of n, and suppose that $C_{p_i}(x)$ is solvable by radicals over F, $(i = 1,2,\ldots,r)$.

Then there exists a sequence of fields

$$F \subset F_1 \subset F_2 \subset \dots \subset F_s,$$

where $F_s \supseteq E_{p_i}$ $(i = 1,2,\dots,r)$ and where F_j is pure and of prime degree over F_{j-1}. As in Theorem 9.3.1, this implies that $C_n(x)$ is solvable by radicals over F.

Let $F \supseteq$ M.A.(p,m). We define a class C(p,m) of primes recursively as follows: Let q be any prime(including 1).

1. If $q < p$, then $q \in C(p,m)$,

2. $p \notin C(p,m)$,

3. If $q > p$, let k be the least exponent such that $p^{(\phi(q),m)k} \equiv 1 \pmod{q}$, and let $k = q_1^{v_1} q_2^{v_2} \dots q_s^{v_s}$. Then $q_i < q$, and $q \in C(p,m)$ if and only if $q_i \in C(p,m)$.

<u>THEOREM 9.3.3</u>: <u>Let</u> $F \supseteq$ M.A.(p,m). <u>If</u> q <u>is a prime</u> $\neq p$, $C_q(x)$ <u>is solvable by radicals over</u> F, <u>if and only if</u> $q \in C(p,m)$.

<u>Proof</u>: This follows from Theorems 9.2.2, 9.3.1, and 9.3.2.

<u>THEOREM 9.3.4</u>: <u>Let</u> $F \supseteq$ M.A.(p,m). <u>Then</u> f(x) <u>over</u> F <u>is solvable by radicals if and only if the index series of the Galois group of</u> f(x) <u>relative to</u> F <u>consists of prime numbers belonging to</u> C(p,m).

<u>Proof</u>: It follows from Theorems 9.3.2, and 9.3.3 that this result is equivalent to Theorem 9.3.1 when F has prime characteristic.

<u>THEOREM 9.3.5</u>: <u>Let</u> $F \supseteq$ M.A.(p,m). <u>A neccessary</u>

<u>and sufficient condition that</u> $C_n(x)$ <u>in</u> F <u>whose roots are the</u> $\phi(n)$ <u>distinct primitive</u> n-<u>th roots of unity be solvable by radicals over</u> F <u>for every</u> $n \not\equiv 0 \pmod p$ <u>is that</u> $p^{\infty} \mid m$.

<u>Proof</u>: <u>Necessity</u>: Suppose $C_n(x)$ is solvable by radicals over F for every $n \not\equiv 0 \pmod p$. Suppose that the exponent d of p in the factorization of m is finite. Let $k = p^{p^{d+1}} - 1$, so that $(k,p) = 1$. Then p is the least exponent such that $p^{(\phi(k),m)p} \equiv 1 \pmod k$. From Theorems 9.2.2 and 9.3.4, $C_n(x)$ is not solvable by radicals over F.

<u>Sufficiency</u>: By Theorems 9.3.2 and 9.3.3, if $p^{\infty} \mid m$, every prime $\neq p$ belongs to the class $C(p,m)$.

BIBLIOGRAPHY

Albert, A.A., Modern Higher Algebra. Chicago: University of Chicago Press, 1947.

Artin, E., Galois Theory. Ann Arbor: Edwards Brothers, 1948.

Birkoff, G., and MacLane S., A Survey of Modern Algebra. New York: MacMillan, 1948.

Brewer, B.W., A Criterion for Solvability by Radicals. American Journal of Mathematics, V.63(1941), p.119-126.

Dickson, L.E., Linear Groups. Leipzig: Teubner, 1901.

Jacobson, N., Lectures in Abstract Algebra. New York: Von Nostrand, 1951.

MacDuffee, C.C., An Introduction to Abstract Algebra. New York: Wiley, 1940.

Rauter, H., Höhere Kreiskörper. Journal für die reine und angewandte Mathematik, V.159(1928), p.220-227.

Steinitz, E., Algebraische Theorie der Körper. New York: Chelsea, 1950.

Van der Waerden, B.L., Moderne Algebra. Berlin: Springer, 1937.

Weiss, M.J., Higher Algebra for the Undergraduate. New York: Wiley, 1952.

Wilson, R.L., A Method for the Determination of the Galois Group. Duke Math. Journal, V.17(1950), p.403-408.