II FIELD THEORY

A. Extension Fields.

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

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

THEOREM 6. If F, B, E are three fields such that $F \subset B \subset E$, then

$$(E/F) = (B/F)(E/B).$$

Let $A_1, A_2, \ldots, A_r$ be elements of E which are linearly independent with respect to B and let $C_1, C_2, \ldots, C_s$ be elements of B which are independent

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

Corollary. If $F \subset F_1 \subset F_2 \subset \ldots \subset F_n$, then $(F_n/F) = (F_1/F)\cdot(F_2/F_1)\cdot\ldots\cdot(F_n/F_{n-1})$.

---

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

B. Polynomials.

An expression of the form $a_0x^n + a_1x^{n-1} + \ldots + a_n$ is called a polynomial in F of degree n if the coefficients $a_0,\ldots,a_n$ are elements of the field F and $a_0 \neq 0$. Multiplication and addition of polynomials are performed in the usual way[1].

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 reducible in F are called irreducible in F.

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

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

---

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

uniquely determined polynomial of a degree less than that of $g(x)$ such that $f(x) - r(x)$ is divisible by $g(x)$. We shall call $r(x)$ the remainder of $f(x)$.

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

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

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

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

By the division algorithm,

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

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

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

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

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

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

As we saw, many of the theorems of elementary algebra hold in any field F. However, the so-called Fundamental Theorem of Algebra, at least in its customary form, does not

hold. It will be replaced by a theorem due to Kronecker which guarantees for a given polynomial in F the existence of an extension field in which the polynomial has a root. We shall also show that, in a given field, a polynomial can not only be factored into irreducible factors, but that this factorization is unique up to a constant factor. The uniqueness depends on the theorem of Kronecker.

C. Algebraic Elements.

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

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

We consider now the subset 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 (n being the degree of $f(x)$). This set E_0 is closed under addition and multiplication. The latter may be verified as follows:

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

We remark that the internal structure of the set E_0 does not depend on the nature of α but only on the irreducible $f(x)$. The knowledge of this polynomial enables us to perform the operations of addition and multiplication in our set E_0. We shall see very soon that E_0 is a field; in fact, E_0 is nothing but the field $F(\alpha)$. As soon as this is shown we have at once the degree, $(F(\alpha)/F)$, determined as n, since the space $F(\alpha)$ is generated by the linearly independent $1, \alpha, \alpha^2, \ldots, \alpha^{n-1}$.

We shall now try to imitate the set E_0 without having an extension field E and an element α at our disposal. We shall assume only an irreducible polynomial

$$f(x) = x^n + a_{n-1}x^{n-1} + \ldots + a_0$$

as given.

We select a variable ξ and let E_1 be the set of all polynomials

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

of a degree lower than n. This set forms a group under addition. We now introduce besides the ordinary multiplication

a new kind of multiplication of two elements $g(\xi)$ and $h(\xi)$ of E_1 denoted by $g(\xi) \times h(\xi)$. It is defined as the remainder $r(\xi)$ of the ordinary product $g(\xi)\, h(\xi)$ under division by $f(\xi)$. We first remark that any product of m terms $g_1(\xi), g_2(\xi), \ldots, g_m(\xi)$ is again the remainder of the ordinary product $g_1(\xi)\, g_2(\xi) \ldots g_m(\xi)$. This is true by definition for $m = 2$ and follows for every m by induction if we just prove the easy lemma: The remainder of the product of two remainders (of two polynomials) is the remainder of the product of these two polynomials. This fact shows that our new product is associative and commutative and also that the new product $g_1(\xi) \times g_2(\xi) \times \ldots \times g_m(\xi)$ will coincide with the old product $g_1(\xi)\, g_2(\xi) \ldots g_m(\xi)$ if the latter does not exceed n in degree. The distributive law for our multiplication is readily verified.

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 ξ. Multiplying it i-times with itself, clearly will just lead to ξ^i as long as $i < n$. For $i = n$ this is not any more the case since it leads to the remainder of the polynomial ξ^n. This remainder is

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

We now give up our old multiplication altogether and keep only the new one; we also change notation, using the point (or juxtaposition) as symbol for the new multiplication.

Computing in this sense

$$c_0 + c_1\xi + c_2\xi^2 + \ldots + c_{n-1}\xi^{n-1}$$

will really lead to this element, since all the degrees involved are below n. But

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

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

We thus have constructed a set E_1 and an addition and multiplication in E_1 that already satisfies most of the field axioms. E_1 contains F as subfield and ξ satisfies the equation $f(\xi) = 0$. We next have to show: If $g(\xi) \neq 0$ and $h(\xi)$ are given elements of E_1, there is an element

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

in E_1 such that

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

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

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

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

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

have only the trivial solution.

The homogeneous problem would occur if we should ask for the set of elements $X(\xi)$ satisfying $g(\xi) \cdot X(\xi) = 0$. Going back for a moment to the old multiplication this would mean that the ordinary product $g(\xi)\,X(\xi)$ has the remainder 0, and is therefore divisible by $f(\xi)$. According to the lemma, page 16, this is only possible for $X(\xi) = 0$.

Therefore E_1 is a field.

Assume now that we have also our old extension E with a root α of $f(x)$, leading to the set E_0. We see that E_0 has in a certain sense the same structure as E_1 if we map the element $g(\xi)$ of E_1 onto the element $g(\alpha)$ of E_0. This mapping will have the property that the image of a sum of elements is the sum of the images, and the image of a product is the product of the images.

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

We see that E_0 is also a field and that it is isomorphic to E_1.

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

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

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

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

Proof: E and E' are both isomorphic to E_0.

D. Splitting Fields.

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

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

A splitting field is of finite degree since it is constructed by a finite number of adjunctions of algebraic elements, each defining an extension field of finite degree. Because of the Corollary on page 14, the total degree is finite.

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

We factor $p(x)$ in F into irreducible factors $f_1(x) \cdot \ldots \cdot f_r(x) = p(x)$. If each of these 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 7 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.

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

THEOREM 10. Let σ be an isomorphism mapping the field 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 σ. Finally, let E be a splitting field of $p(x)$ and E' a splitting field of $p'(x)$. Under these conditions the isomorphism σ can be extended to an isomorphism between E and E'.

If $f(x)$ is an irreducible factor of $p(x)$ in F, then E contains a root of $f(x)$. For let $p(x) = (x-\alpha_1)(x-\alpha_2)\ldots(x-\alpha_s)$ be the splitting of $p(x)$ in E. Then $(x-\alpha_1)(x-\alpha_2)\ldots(x-\alpha_s) = f(x)\cdot g(x)$. We consider $f(x)$ as a polynomial in E and construct the extension field $B = E(\alpha)$ in which $f(\alpha) = 0$. Then $(\alpha-\alpha_1)\cdot(\alpha-\alpha_2)\cdot\ldots\cdot(\alpha-\alpha_s) = f(\alpha)\cdot g(\alpha) = 0$ and $\alpha-\alpha_1$ being elements of the field B can have a product equal to 0 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 $f(x)$.

Now in case $(E/F) = 1$, 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 σ preserves all operations of addition and multiplication in the process of multiplying out the

factors of $p(x)$ and collecting to get the original form. Since $p'(x)$ can be split in F', we must have $F' = E'$. In this case, σ itself is the required extension and the theorem is proved if $(E/F) = 1$.

We proceed by complete induction. Let us suppose the theorem proved for all cases in which the degree is less than $n > 1$, and suppose $(E/F) = n$. We factor $p(x)$ into irreducible factors in F; $p(x) = f_1(x) \cdot f_2(x) \cdot \ldots \cdot f_m(x)$. Not all of these factors can be of degree 1, since otherwise $p(x)$ would split in F, and we should have $(E/F) = 1$ contrary to assumption. Hence, we may suppose the degree of $f_1(x)$ to be $r > 1$. Let $f_1'(x) \cdot f_2'(x) \cdot \ldots \cdot f_m'(x) = p'(x)$ be the factorization of $p'(x)$ into the polynomials corresponding to $f_1(x), \ldots, f_m(x)$ under σ. $f_1'(x)$ is irreducible in F', for a factorization of $f_1'(x)$ in F' would induce[1] under σ^{-1} a factorization of $f_1(x)$, which was however taken to be irreducible. Let α be a root of $f_1(x)$ in E and α' a root of $f_1'(x)$ in E'. We have $(F(\alpha)/F) = (F'(\alpha')/F') = r > 1$.

Also, by Theorem 8, the isomorphism σ can be extended to an isomorphism σ_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 $p'(x)$. But $(E/F) = (F(\alpha)/F)(E/F(\alpha)) = r \cdot (E/F(\alpha))$. Hence, $(E/F(\alpha)) < n$, and, by our inductive assumption,

---

1) See page 30 for the definition of σ^{-1}.

σ_1 can be extended from an isomorphism between $F(\alpha)$ and $F'(\alpha')$ to an isomorphism σ_2 between E and E'. Since σ_1 is an extension of σ, and σ_2 an extension of σ_1, then σ_2 is an extension of σ 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.

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

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

E. Unique Decomposition of Polynomials into Irreducible Factors.

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

Let $F(\alpha)$ be an extension of F in which $p_1(\alpha) = 0$. We may suppose the leading coefficients of the $p_i(x)$ and the $q_i(x)$ to be 1, for, by factoring out all leading coefficients and combining, the constant multiplier on each side of the equation must be

the leading coefficient of $p(x)$ and hence can be divided out of both sides of the equation. Since $0 = p_1(\alpha)\cdot p_2(\alpha)\cdot\ldots\cdot p_r(\alpha) = p(\alpha) = q_1(\alpha)\cdot\ldots\cdot q_s(\alpha)$ and since a product of elements of $F(\alpha)$ can be 0 only if one of these is 0, it follows that one of the $q_1(\alpha)$, say $q_1(\alpha)$, is 0. This gives (see page 17) $p_1(x) = q_1(x)$. Thus $p_1(x)\cdot p_2(x)\cdot\ldots\cdot p_r(x) = p_1(x)\cdot q_2(x)\cdot\ldots\cdot q_s(x)$ or $p_1(x)\cdot[p_2(x)\cdot\ldots\cdot p_r(x) - q_2(x)\cdot\ldots\cdot q_s(x)] = 0$. Since the product of two polynomials is 0 only if one of the two is the 0 polynomial, it follows that the polynomial within the brackets is 0 so that $p_2(x)\cdot\ldots\cdot p_r(x) = q_2(x)\cdot\ldots\cdot q_s(x)$. If we repeat the above argument r times we obtain $p_i(x) = q_i(x)$, $i = 1,2,\ldots,r$. Since the remaining q's must have a product 1, it follows that $r = s$.

F. Group Characters.

If G is a multiplicative group, F a field and σ a homomorphism mapping G into F, then σ is called a character of G in F. By homomorphism is meant a mapping σ such that for α, β any two elements of G, $\sigma(\alpha)\cdot\sigma(\beta) = \sigma(\alpha\cdot\beta)$ and $\sigma(\alpha) \neq 0$ for any α. (If $\sigma(\alpha) = 0$ for one element α, then $\sigma(x) = 0$ for each $x\varepsilon G$, since $\sigma(\alpha y) = \sigma(\alpha)\cdot\sigma(y) = 0$ and αy takes all values in G when y assumes all values in G).

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

characters are not dependent they are called independent.

THEOREM 12. If $\sigma_1, \sigma_2, \ldots, \sigma_n$ are n mutually distinct characters of a group G in a field F, then $\sigma_1, \sigma_2, \ldots, \sigma_n$ are independent.

One character cannot be dependent, since $a_1 \sigma_1(x) = 0$ implies $a_1 = 0$ due to the assumption that $\sigma_1(\alpha) \neq 0$. Suppose $n > 1$. We make the inductive assumption that no set of less than n distinct characters is dependent. Suppose now that $a_1 \sigma_1(x) + a_2 \sigma_2(x) + \ldots + a_n \sigma_n(x) = 0$ is a non-trivial dependence between the σ's. None of the elements a_i is zero, else we should have a dependence between less than n characters contrary to our inductive assumption. Since σ_1 and σ_n are distinct, there exists an element α in G such that $\sigma_1(\alpha) \neq \sigma_n(\alpha)$. Multiply the relation between the σ's by a_n^{-1}. We obtain a relation

(*) $b_1\sigma_1(x) + \ldots + b_{n-1}\sigma_{n-1}(x) + \sigma_n(x) = 0$,

$b_i = a_n^{-1}a_i \neq 0$.

Replace in this relation x by αx. We have

$b_1\sigma_1(\alpha)\sigma_1(x) + \ldots + b_{n-1}\sigma_{n-1}(\alpha)\sigma_{n-1}(x) + \sigma_n(\alpha)\sigma_n(x) = 0$,

or $\sigma_n(\alpha)^{-1}b_1\sigma_1(\alpha)\sigma_1(x) + \ldots + \sigma_n(x) = 0$.

Subtracting the latter from (*) we have

(**) $[b_1 - \sigma_n(\alpha)^{-1}b_1\sigma_1(\alpha)]\sigma_1(x) + \ldots + c_{n-1}\sigma_{n-1}(x) = 0$.

The coefficient of $\sigma_1(x)$ in this relation is not 0, otherwise we should have $b_1 = \sigma_n(\alpha)^{-1}b_1\sigma_1(\alpha)$, so that

$\sigma_n(\alpha)b_1 = b_1\sigma_1(\alpha) = \sigma_1(\alpha)b_1$

and since $b_1 \neq 0$, we get $\sigma_n(\alpha) = \sigma_1(\alpha)$ contrary to

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

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

This follows from Theorem 12, since E without the 0 is a group and the σ's defined in this group are mutually distinct characters.

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

Lemma. The set of fixed points of E is a subfield of E. We shall call this subfield the fixed field.

For if a and b are fixed points, then

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

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

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

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

THEOREM 13. If $\sigma_1,\ldots,\sigma_n$ are n mutually distinct isomorphisms of a field E into a field E', and if F is the fixed field of E, then $(E/F) \geqslant n$.

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

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

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

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

Adding these last equations and using

$$\begin{aligned}
&\sigma_1(a_1\omega_1) + \sigma_1(a_2\omega_2) + \ldots + \sigma_1(a_r\omega_r)\\
&\qquad = \sigma_1(a_1\omega_1 + \ldots + a_r\omega_r) = \sigma_1(\alpha)
\end{aligned}$$

we obtain

$$\sigma_1(\alpha)x_1 + \sigma_2(\alpha)x_2 + \ldots + \sigma_n(\alpha)x_n = 0.$$

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

Corollary: If $\sigma_1,\sigma_2,\ldots,\sigma_n$ are automorphisms of the field E, and F is the fixed field, then $(E/F) \geq n$.

If F is a subfield of the field E, and σ an automorphism of E, we shall say that σ leaves F fixed if for each element a of F, $\sigma(a) = a$. If σ and τ are two automorphisms of E, then the mapping $\sigma(\tau(x))$ written briefly $\sigma\tau$ is an automorphism, as the reader may readily verify. [E.g., $\sigma\tau(x\cdot y) = \sigma(\tau(x\cdot y)) = \sigma(\tau(x)\cdot\tau(y)) = \sigma(\tau(x))\cdot\sigma(\tau(y))$]. We shall call $\sigma\tau$ the product of σ and τ. If σ is an automorphism ($\sigma(x) = y$), then we shall call σ^{-1} the mapping of y into x, i.e., $\sigma^{-1}(y) = x$ the inverse of σ. The reader may readily verify that σ^{-1} is an automorphism. The automorphism $I(x) = x$ shall be called the unit automorphism.

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

The product of two automorphisms which leave F fixed clearly leaves F fixed. Also, the inverse of any automorphism in G is in G.

The reader will observe that G, the set of automorphisms which leave F fixed, does not necessarily have F as its fixed field. It may be that certain elements in E which do not belong to F are left fixed by every automorphism which

leaves F fixed. Thus, the fixed field of G may be larger than F.

G. Normal Extensions.

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.

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

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

If $\sigma_1, \sigma_2, \ldots, \sigma_n$ is a group, then the identity occurs, say, $\sigma_1 = I$. The fixed field consists of those elements x which are not moved by any of the σ's, i.e., $\sigma_i(x) = x$, $i = 1,2,\ldots n$. Suppose that $(E/F) > n$. 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, there exists a non-trivial solution in E to the system of equations

$$
\begin{aligned}
&x_1\sigma_1(\alpha_1) + x_2\sigma_1(\alpha_2) + \ldots + x_{n+1}\sigma_1(\alpha_{n+1}) = 0 \\
&x_1\sigma_2(\alpha_1) + x_2\sigma_2(\alpha_2) + \ldots + x_{n+1}\sigma_2(\alpha_{n+1}) = 0 \qquad (1') \\
&\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots \\
&x_1\sigma_n(\alpha_1) + x_2\sigma_n(\alpha_2) + \ldots + x_{n+1}\sigma_n(\alpha_{n+1}) = 0 .
\end{aligned}
$$

We note that the solution cannot lie in F, otherwise, since σ_1 is the identity, the first equation would be a dependence between $\alpha_1, \ldots, \alpha_{n+1}$.

Among all non-trivial solutions $x_1, x_2, \ldots, x_{n+1}$ we choose one which has the least number of elements different from 0. We may suppose this solution to be $a_1, a_2, \ldots, a_r, 0, \ldots, 0$, where the first r terms are different from 0. Moreover, $r \neq 1$ because $a_1\sigma_1(\alpha_1) = 0$ implies $a_1 = 0$ since $\sigma_1(\alpha_1) = \alpha_1 \neq 0$. Also, we may suppose $a_r = 1$, since if we multiply the given solution by a_r^{-1} we obtain a new solution in which the r^{th} term is 1. Thus, we have

(*) $a_1\sigma_i(\alpha_1) + a_2\sigma_i(\alpha_2) + \ldots + a_{r-1}\sigma_i(\alpha_{r-1}) + \sigma_i(\alpha_r) = 0$

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

$$\sigma_k(a_1)\cdot\sigma_k\sigma_j(\alpha_1) + \ldots + \sigma_k(a_{r-1})\cdot\sigma_k\sigma_j(\alpha_{r-1}) + \sigma_k\sigma_j(\alpha_r) = 0$$

for $j = 1,2,\ldots,r$, so that from $\sigma_k\sigma_j = \sigma_i$

(**) $\sigma_k(a_1)\sigma_i(\alpha_1) + \ldots + \sigma_k(a_{r-1})\sigma_i(\alpha_{r-1}) + \sigma_i(\alpha_r) = 0$

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

$$[a_1 - \sigma_k(a_1)]\cdot\sigma_i(\alpha_1) + \ldots + [a_{r-1} - \sigma_k(a_{r-1})]\sigma_i(\alpha_{r-1}) = 0$$

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

Corollary 1: If F is the fixed field for the finite group G, then each automorphism σ that leaves F fixed

must belong to G.

(E/F) = order of G = n. Assume there is a σ not in G. Then F would remain fixed under the n+1 elements consisting of σ and the elements of G, thus contradicting the Corollary to Theorem 13.

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

This follows immediately from Corollary 1.

If f(x) is an irreducible polynomial in F, then f(x) is called separable if it does not have repeated roots. If E is an extension of the field F, the element α of E is called separable if it is root of a separable polynomial f(x) in F, and E is called a separable extension if each element of E is separable.

THEOREM 15. E is a normal extension of F if and only if E is the splitting field of a polynomial p(x) in F whose irreducible factors are separable.

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

If (E/F) = 1, then our proposition is trivial, since then E = F and only the unit automorphism leaves F fixed.

Let us suppose that (E/F) = n > 1. We make the inductive assumption that for all pairs of fields with degree less than n our proposition holds.

Let $p(x) = p_1(x) \cdot p_2(x) \cdot \ldots \cdot p_r(x)$

be a factorization of p(x) into separable factors. We may suppose one of these to have a degree greater than

one, for otherwise we should have $(E/F) = 1$. Suppose $\deg p_1(x) = s > 1$. Let α_1 be a root of $p_1(x)$. Then $(F(\alpha_1)/F) = \deg p_1(x) = s$. From $(E/F(\alpha_1))\cdot(F(\alpha_1)/F) = (E/F) = n$ it follows that $(E/F(\alpha_1)) < n$. From the fact that $p(x)$ lies in $F(\alpha_1)$ and E is a splitting field of $p(x)$ over $F(\alpha_1)$, it follows by our inductive assumption 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.

$p_1(x)$ being separable its roots $\alpha_1, \alpha_2, \ldots, \alpha_s$ are s distinct elements of E. By Theorem 8 there exist isomorphisms $\sigma_1, \sigma_2, \ldots, \sigma_s$ 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. Since σ_1 is the identity mapping, the fixed field F' of $\alpha_1, \ldots, \alpha_s$ consists of those elements of $F(\alpha_1)$ which are not moved by any one of the mappings $\sigma_1, \sigma_2, \ldots, \sigma_s$. The isomorphisms $\sigma_1, \sigma_2, \ldots, \sigma_s$ are mutually distinct since α_1 has s different images. Therefore, by Theorem 13, $(F(\alpha_1)/F') \geq s$. Since $F \subset F'$, $(F'/F)\cdot(F(\alpha_1)/F') = (F(\alpha_1)/F) = s$, from which it follows that $(F(\alpha_1)/F') \leq s$, and this combined with the preceding inequality gives $(F(\alpha_1)/F') = s$. This implies $(F'/F) = 1$ or $F = F'$. Each point of $F(\alpha_1)$ which is not in F is moved by one of the mappings $\sigma_1, \sigma_2, \ldots \sigma_s$.

We now apply Theorem 10. E is a splitting field of $p(x)$ in $F(\alpha_1)$ and is also a splitting field of $p(x)$ in $F(\alpha_1)$. Hence, the isomorphism σ_1, which makes $p(x)$ in

$F(\alpha_1)$ correspond to the same $p(x)$ in $F(\alpha_1)$, can be extended to an isomorphic mapping of E on E, that is, to an automorphism σ_1'.

The sufficiency is now established. For, any element of E which is not in F, either is not in $F(\alpha_1)$ and is then moved by an automorphism which even leaves $F(\alpha_1)$ fixed, or else is in $F(\alpha_1)$ and is then moved by one of the automorphisms $\sigma_1', \ldots, \sigma_s'$.

Necessity. If E is a normal extension of F, then E is splitting field of a polynomial $p(x)$ whose irreducible factors are separable. We first prove the

Lemma. If E is a normal extension of F, then E is a separable extension of F.

Let $\sigma_1, \sigma_2, \ldots, \sigma_s$ be the group G of automorphisms of E whose fixed field is F. Let α be an element of E, and let $\alpha, \alpha_2, \alpha_3, \ldots, \alpha_r$ be the set of distinct elements in the sequence $\sigma_1(\alpha), \sigma_2(\alpha), \ldots, \sigma_s(\alpha)$. Since G is a group,

$$\sigma_j(\alpha_i) = \sigma_j(\sigma_k(\alpha)) = \sigma_j\sigma_k(\alpha) = \sigma_m(\alpha) = \alpha_n.$$

Therefore, the elements $\alpha, \alpha_2, \ldots, \alpha_r$ are permuted by the automorphisms 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 belong to F, $f(x)$ is a polynomial in F. If $g(x)$ is a polynomial in F which also has α as root, then applying the automorphisms of G to the expression $g(\alpha) = 0$ we obtain $g(\alpha_i) = 0$, so that the degree of $g(x) \geq s$. Hence $f(x)$ is irreducible, and the lemma is

established.

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

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 group of the equation f(x) = 0. We come now to a theorem known in algebra as the Fundamental Theorem of Galois Theory which gives the relation between the structure of a splitting field and its group of automorphisms.

THEOREM 16. (Fundamental Theorem). If p(x) is a polynomial in a field F, and G the group of the equation p(x) = 0, where E is the splitting field of p(x), then: (1) Each intermediate field is the fixed field for a subgroup G_B of G, and distinct subgroups have distinct fixed fields. We say B and G_B "belong" to each other. (2) The intermediate field B is a normal extension of F if and only if the subgroup G_B is a normal subgroup of G. In this case the group of automorphisms of B which leaves F fixed is isomorphic to the factor group (G/G_B). (3) For each intermediate field B, we have (B/F) = index of G_B and (E/B) = order of G_B.

The first part of the theorem comes from the observation that E is splitting field for p(x) when p(x) is taken to be in any intermediate field. Hence, E is a normal extension of each intermediate field B, so that B is the fixed field of the subgroup of G

consisting of the automorphisms which leave B fixed. That distinct subgroups have distinct fixed fields is stated in Corollary 2 to Theorem 14.

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

The number $i(G_B)$ is equal to the number of left cosets of G_B. The elements of G, being automorphisms of E, are isomorphisms of B; that is, 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 $\sigma \cdot \sigma_1$ and $\sigma \cdot \sigma_2$ be two elements of the coset σG_B. Since σ_1 and σ_2 leave B fixed, for each α in B we have $\sigma\sigma_1(\alpha) = \sigma(\alpha) = \sigma\sigma_2(\alpha)$. Elements of different cosets give different isomorphisms, for if σ and τ give the same isomorphism, $\sigma(\alpha) = \tau(\alpha)$ for each α in B, then $\sigma^{-1}\tau(\alpha) = \alpha$ for each α in B. Hence, $\sigma^{-1}\tau = \sigma_1$, where σ_1 is an element of G_B. But then $\tau = \sigma\sigma_1$ and $\tau G_B = \sigma\sigma_1 G = \sigma G_B$ so that σ and τ belong to the same coset.

Each isomorphism of B which is the identity on F is given by an automorphism belonging to G. For let σ be an isomorphism mapping B on B' and the identity

on F. Then under σ, 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 10, σ can be extended to an automorphism σ' of E, and since σ' leaves F fixed it belongs to G. Therefore, the number of distinct isomorphisms of B is equal to the number of cosets of G_B and is therefore equal to (B/F).

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

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

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

subgroup of G.

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

H. Finite Fields.

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

THEOREM 17. If 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.

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

Lemma 1. If in an abelian group A and B are two elements of orders a and b, and if c is the least common multiple of a and b, then there is an element C of order c in the group.

Proof: (a) If a and b are relatively prime, C = AB has the required order ab. The order of $C^a = B^a$ is b and

therefore c is divisible by b. Similarly it is divisible by a. Since $C^{ab} = 1$ it follows $c = ab$.

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

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

$$a = p_1^{n_1} p_2^{n_2} \ldots p_r^{n_r}$$

$$b = p_1^{m_1} p_2^{m_2} \ldots p_r^{m_r} .$$

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

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

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

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

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

We now prove Theorem 17. Let n be the order 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 $r \geq n$. On the other hand $r \leq n$ because the order of each element divides n. S is therefore a cyclic group consisting of $1, \varepsilon, \varepsilon^2, \ldots, \varepsilon^{n-1}$ where $\varepsilon^n = 1$.

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

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

If a is an element of a field F, let us denote the n-fold of a, i.e., the element of F obtained by adding a to itself n times, by na. It is obvious that $n \cdot (m \cdot a) = (nm) \cdot a$ and $(n \cdot a)(m \cdot b) = nm \cdot ab$. If for one element $a \neq 0$, there is an integer n such that $n \cdot a = 0$ then $n \cdot b = 0$ for each b in F, since $n \cdot b = (n \cdot a) \cdot (a^{-1}b) = 0 \cdot a^{-1}b = 0$. If there is a positive integer p such that $p \cdot a = 0$ for each a in F, and if p is the smallest integer with this property, then F is said to have the characteristic p. If no such positive integer exists then we say F has characteristic 0. The characteristic of a field is always a prime number, for if $p = r \cdot s$ then $pa = rs \cdot a = r \cdot (s \cdot a)$. However, $s \cdot a = b \neq 0$ if $a \neq 0$ and $r \cdot b \neq 0$ since both r and s are less than p, so that $pa \neq 0$ contrary to the definition of the characteristic. If $na = 0$ for $a \neq 0$, then p divides n, for $n = qp + r$ where $0 \leq r < p$ and $na = (qp + r)a = qpa + ra$. Hence $na = 0$ implies $ra = 0$ and from the definition of the characteristic since $r < p$, we must have $r = 0$.

If F is a finite field having q elements and E an extension of F such that $(E/F) = n$, then E has q^n elements. For 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. E is finite, hence, <u>there is an element α of E so that $E = F(\alpha)$.</u> (The non-zero elements of E form a cyclic group generated by an element α).

If we denote by $P \equiv [0,1,2,\ldots,p-1]$ 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. In fact, P is isomorphic to the field of integers reduced mod p. If F is a finite field, then the degree of F over P is finite, say $(F/P) = n$, and F contains p^n elements. In other words, <u>the order of any finite field is a power of its characteristic.</u>

If F and F' are two finite fields having the same order q, then by the preceding, they have the same characteristic since q is a power of the characteristic. The multiples of the unit in 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, therefore, satisfy the equation $x^{q-1} - 1 = 0$. 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 10, the isomorphism between P and P' can be extended to an isomorphism between F and F'. We have thus proved

<u>THEOREM 18. Two finite fields having the same number of elements are isomorphic.</u>

<u>Differentiation.</u> If $f(x) = a_0 + a_1x + \ldots + a_nx^n$ is a polynomial in a field F, then we define

$f' = a_1 + 2a_2x + \ldots + na_nx^{n-1}$. The reader may readily verify that for each pair of polynomials f and g we have

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

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

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

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

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'.

Corollary. If F is a field of characteristic 0 then each irreducible polynomial in F is separable.

Suppose to the contrary that 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 (its leading coefficient is a multiple of the leading coefficient of f(x) and is not zero since the characteristic is 0) and of degree 1 less than the degree of f(x). But α is also a root of f'(x) which contradicts the irreducibility of f(x).

I. Roots of Unity.

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

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, therefore, no roots in common with $x^n - 1$. Thus, E is a normal extension of F. If $\varepsilon_1, \varepsilon_2, \ldots, \varepsilon_n$ are the roots of $x^n - 1$ in E, they form a group under multiplication and by Theorem 17 this group will be cyclic. If $1, \varepsilon, \varepsilon^2, \ldots, \varepsilon^{n-1}$ are the elements of the group, we shall call ε a primitive n^{th} root of unity. The smallest power of ε which is 1 is the n^{th}.

<u>THEOREM 19. If E is the field generated from F by a primitive n^{th} root of unity, then the group G of E over F is abelian for any n and cyclic if n is a prime number.</u>

We have $E = F(\varepsilon)$, since the roots of $x^n - 1$ are powers of ε. Thus, if σ and τ are distinct elements of G, $\sigma(\varepsilon) \neq \tau(\varepsilon)$. But $\sigma(\varepsilon)$ is a root of $x^n - 1$ and, hence, a power of ε. Thus, $\sigma(\varepsilon) = \varepsilon^{n_\sigma}$ where n_σ is an integer $1 \leq n_\sigma < n$. Moreover,

$\tau\sigma(\varepsilon) = \tau(\varepsilon^{n_\sigma}) = (\tau(\varepsilon))^{n_\sigma} = \varepsilon^{n_\tau \cdot n_\sigma} = \sigma\tau(\varepsilon)$. Thus, $n_{\sigma\tau} \equiv n_\sigma n_\tau \bmod n$. Thus, the mapping of σ on n_σ is a homomorphism of G into a multiplicative subgroup of the integers mod n. Since $\tau \neq \sigma$ implies $\tau(\varepsilon) \not\equiv \sigma(\varepsilon)$, it follows that $\tau \neq \sigma$ implies $n_\sigma \not\equiv n_\tau \bmod n$. Hence, the homomorphism is an isomorphism. If n is a prime number, the multiplicative group of numbers forms a cyclic group.

J. Noether Equations.

If E is a field, and $G = (\sigma, \tau, \ldots)$ a group of automorphisms of E, any set of elements $x_\sigma, x_\tau, \ldots$ in E will be said to provide a solution to Noether's equations if $x_\sigma \cdot \sigma(x_\tau) = x_{\sigma\tau}$ for each σ and τ in G. If one element $x_\sigma = 0$ then $x_\tau = 0$ for each $\tau \in G$. As τ traces G, $\sigma\tau$ assumes all values in G, and in the above equation $x_{\sigma\tau} = 0$ when $x_\sigma = 0$. Thus, in any solution of the Noether equations no element $x_\sigma = 0$ unless the solution is completely trivial. We shall assume in the sequel that the trivial solution has been excluded.

THEOREM 20. The system $x_\sigma, x_\tau, \ldots$ is a solution to Noether's equations if and only if there exists an element α in E, such that $x_\sigma = \alpha/\sigma(\alpha)$ for each σ.

For any α, it is clear that $x_\sigma = \alpha/\sigma(\alpha)$ is a solution to the equations, since

$\alpha/\sigma(\alpha) \cdot \sigma(\alpha/\tau(\alpha)) = \alpha/\sigma(\alpha) \cdot \sigma(\alpha)/\sigma\tau(\alpha) = \alpha/\sigma\tau(\alpha)$.

Conversely, let $x_\sigma, x_\tau, \ldots$ be a non-trivial solution. Since the automorphisms $\sigma, \tau, \ldots$ are distinct they are linearly independent, and the equation

$x_\sigma \cdot \sigma(z) + x_\tau \tau(z) + \ldots = 0$ does not hold identically. Hence, there is an element a in E such that $x_\sigma \sigma(a) + x_\tau \tau(a) + \ldots = \alpha \neq 0$. Applying σ to α gives

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

Multiplying by x_σ gives

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

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

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

so that

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

A solution to the Noether equations defines a mapping C of G into E, namely $C(\sigma) = x_\sigma$. If F is the fixed field of G, and the elements x_σ lie in F, then C is a <u>character</u> of G. For $C(\sigma\tau) = x_{\sigma\tau} = x_\sigma \cdot \sigma(x_\tau) = x_\sigma x_\tau = C(\sigma) \cdot C(\tau)$ since $\sigma(x_\tau) = x_\tau$ if $x_\tau \in F$. Conversely, each character C of G in F provides a solution to the Noether equations. Call $C(\sigma) = x_\sigma$. Then, since $x_\tau \in F$, we have $\sigma(x_\tau) = x_\tau$. Thus, $x_\sigma \cdot \sigma(x_\tau) = x_\sigma \cdot x_\tau = C(\sigma) \cdot C(\tau) = C(\sigma\tau) = x_{\sigma\tau}$. We therefore have, by combining this with Theorem 19,

<u>THEOREM 21. 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 $C(\sigma) = \alpha/\sigma(\alpha)$ and, conversely, if $\alpha/\sigma(\alpha)$ is in F for each σ, then $C(\sigma) = \alpha/\sigma(\alpha)$ is a character of G. If r is the least common multiple of the orders of elements of G, then $\alpha^r \in F$.</u>

We have already shown all but the last sentence of Theorem 21. To prove this we need only show $\sigma(\alpha^r) = \alpha^r$

for each $\sigma \in G$. But $\alpha^r/\sigma(\alpha^r) = (\alpha/\sigma(\alpha))^r = (C(\sigma))^r$ $= C(\sigma^r) = C(I) = 1$.

K. Kummer's Fields.

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

If a field F contains a primitive n^{th} root of unity, the number n is not divisible by the characteristic of F. Suppose, to the contrary, F has characteristic p and $n = qp$. Then $y^p - 1 = (y - 1)^p$ since in the expansion of $(y - 1)^p$ each coefficient other than the first and last is divisible by p and therefore is a multiple of the p-fold of the unit of F and thus is equal to 0. Therefore $x^n - 1 = (x^q)^p - 1 = (x^q - 1)^p$ 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 $1, \varepsilon, \varepsilon^2, \ldots, \varepsilon^{n-1}$ would be 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 $x^n - a_i$. Therefore, 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 $\varepsilon_1, \varepsilon_2, \ldots, \varepsilon_n$ are the n distinct n^{th} roots of unity in F, then $\alpha_i\varepsilon_1, \alpha_i\varepsilon_2, \ldots, \alpha_i\varepsilon_n$ will be n distinct roots of $x^n - a_i$, and hence will be the roots of $x^n - a_i$, so that $E = F(\alpha_1, \alpha_2, \ldots, \alpha_r)$.

Let σ and τ be two automorphisms in the group G of E over F. For each α_i, both σ and τ map α_i on some other root of $x^n - a_i$. Thus, $\tau(\alpha_i) = \varepsilon_{i\tau}\,\alpha_i$ and $\sigma(\alpha_i) = \varepsilon_{i\sigma}\cdot\alpha_i$ where $\varepsilon_{i\sigma}$ and $\varepsilon_{i\tau}$ are n^{th} roots of unity in the basic field F. It follows that $\tau(\sigma(\alpha_i)) = \tau(\varepsilon_{i\sigma}\alpha_i) = \varepsilon_{i\sigma}\tau(\alpha_i) = \varepsilon_{i\sigma}\varepsilon_{i\tau}\alpha_i = \sigma(\tau(\alpha_i))$. Since σ and τ are commutative over the generators of E, they commute over each element of E. Hence, G is commutative. If $\sigma \varepsilon G$, then $\sigma(\alpha_i) = \varepsilon_{i\sigma}\alpha_i$, $\sigma^2(\alpha_i) = \varepsilon_{i\sigma}{}^2\alpha_i$, etc. Thus, $\sigma^{n_i}(\alpha_i) = \alpha_i$ for n_i such that $\varepsilon_{i\sigma}{}^{n_i} = 1$. Since the order of an n^{th} root of unity is a divisor of n, we have n_i a divisor of n and the least common multiple m of $n_1, n_2, \ldots, n_r$ is a divisor of n. Since $\sigma^m(\alpha_i) = \alpha_i$ for $i = 1,2,\ldots,r$ it follows that m is the order of σ. Hence, the order of each element of G is a divisor of n and, therefore, the least common multiple r of the orders of the elements of G is a divisor of n. If ε is a primitive n^{th} root of unity, then $\varepsilon^{n/r}$ is a primitive r^{th} root of unity. These remarks can be summarized in the following

THEOREM 22. If E is a Kummer field, i.e., a splitting field of $p(x) = (x^n - a_1)(x^n - a_2)\ldots(x^n - a_t)$, where a_i lie in F, and F contains a primitive n^{th} root of unity, then: (a) E is a normal extension of F, (b) the group G of E over F is abelian, (c) the least common multiple of the orders of the elements of G is a divisor of n.

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

. is cyclic of order p.

The order of each element of G is, by Theorem 22, a divisor of p and, hence, if the element is not the unit its order must be p. If α is a root of $x^p - a$, then $\alpha, \varepsilon\alpha, \ldots, \varepsilon^{p-1}\alpha$ are all the 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 $x^p - a = 0$.

The properties (a), (b) and (c) in Theorem 22 actually characterize Kummer fields.

Let us suppose that E is a normal extension of a field F, whose group G over F is abelian. Let us further assume that if the least common multiple of the orders of elements of G is r, then F contains a primitive r^{th} root of unity.

The group of characters X of G into the group of r^{th} roots of unity is isomorphic to G. Moreover, to each $\sigma \varepsilon G$, if $\sigma \neq 1$, there exists a character $C \varepsilon X$ such that $C(\sigma) \neq 1$.

Let A denote the set of those non-zero elements α of E for which $\alpha^r \varepsilon F$ and let F_1 denote the non-zero elements of F. It is obvious that A is a multiplicative group and that F_1 is a subgroup of A. Let A^r denote the set of r^{th} powers of elements in A and $F_1{}^r$ the set of r^{th} powers of elements

of F_1. The following theorem provides in most applications a convenient method for computing the group G.

THEOREM 23. The factor groups (A/F_1) and (A^r/F_1^r) are isomorphic to each other and to the groups G and X.

We map A on A^r by making $\alpha \varepsilon A$ correspond to $\alpha^r \varepsilon A^r$. If $a^r \varepsilon F_1^r$, where $a \varepsilon F_1$ then $b \varepsilon A$ is mapped on a^r if and only if $b^r = a^r$, that is, if b is a solution to the equation $x^r - a^r = 0$. But $a, \varepsilon a, \varepsilon^2 a, \ldots, \varepsilon^{r-1} a$ are distinct solutions to this equation and since ε and a belong to F_1, it follows that b must be one of these elements and must belong to F_1. Thus, the inverse set in A of the subgroup F_1^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 $(\alpha/\sigma(\alpha))^r = \alpha^r/\sigma(\alpha^r) = 1$. Hence, $\alpha/\sigma(\alpha)$ is an r^{th} root of unity and lies in F_1. By Theorem 21, $\alpha/\sigma(\alpha)$ defines a character $C(\sigma)$ of G in F. We map α on the corresponding character C. Each character C is by Theorem 21, image of some α. Moreover, $\alpha \cdot \alpha'$ is mapped on the character $C^*(\sigma) = \alpha \cdot \alpha'/\sigma(\alpha \cdot \alpha') = \alpha \cdot \alpha'/\sigma(\alpha) \cdot \sigma(\alpha') = C(\sigma) \cdot C'(\sigma) = C \cdot C'(\sigma)$, so that the mapping is a homomorphism. The kernel of this homomorphism is the set of those elements α for which $\alpha/\sigma(\alpha) = 1$ for each σ, hence is F_1. It follows, therefore, that (A/F_1) is isomorphic to X and hence also to G. In particular, (A/F_1) is a finite group.

We now prove the equivalence between Kummer fields and fields satisfying (a), (b) and (c) of Theorem 22.

THEOREM 24. If E is an extension field over F, then E is a Kummer field if and only if E is normal, its group G is abelian and F contains a primitive r^{th} root ε of unity where r is the least common multiple of the orders of the elements of G.

The necessity is already contained in Theorem 22. We prove the sufficiency. Out of the group A, let $\alpha_1F_1, \alpha_2F_1, \ldots, \alpha_tF_1$ be the cosets of F_1. Since $\alpha_i \varepsilon A$, we have $\alpha_i^r = a_i \varepsilon F$. Thus, α_i is a root of the equation $x^r - a_i = 0$ and since $\varepsilon\alpha_i, \varepsilon^2\alpha_i, \ldots, \varepsilon^{r-1}a_i$ are also roots, $x^r - a_i$ must split in E. We prove that E is the splitting field of $(x^r - a_1)(x^r - a_2)\ldots(x^r - a_t)$ which will complete the proof of the Theorem. To this end it suffices to 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 $F(\alpha_1, \ldots, \alpha_t)$ there exists an automorphism $\sigma \varepsilon G, \sigma \neq 1$, which leaves $F(\alpha_1, \ldots, \alpha_t)$ fixed. There exists a character C of G for which $C(\sigma) \neq 1$. Finally, there exists an element α in E such that $C(\sigma) = \alpha/\sigma(\alpha) \neq 1$. But $\alpha^r \varepsilon F_1$ by Theorem 21, hence $\alpha \varepsilon A$. Moreover, $A \subset F(\alpha_1, \ldots, \alpha_t)$ since all the cosets α_iF_1 are contained in $F(\alpha_1, \ldots, \alpha_t)$. Since $F(\alpha_1, \ldots, \alpha_t)$ is by assumption left fixed by σ, $\sigma(\alpha) = \alpha$ which contradicts $\alpha/\sigma(\alpha) \neq 1$. It follows, therefore, that $F(\alpha_1, \ldots, \alpha_t) = E$.

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 splitting field of an irreducible polynomial $x^p - a$ in F.

E is generated by elements $\alpha_1,\ldots,\alpha_n$ where $\alpha_1^p \in F$. 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 the product theorem for the degrees, p would not be a prime number, contrary to assumption. $E = F(\alpha_1)$ is the splitting field of $x^p - a$.

L. Simple Extensions.

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

THEOREM 25. A finite extension E of F is primitive over F if and only if there are only a finite number of intermediate fields.

(a) Let $E = F(\alpha)$ and call $f(x) = 0$ 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. $g(x)$ is irreducible in B, hence also in B'. Since $E = B'(\alpha)$ we see $(E/B) = (E/B')$. This proves $B' = B$. So B is uniquely determined by the polynomial $g(x)$. But $g(x)$ is a divisor of $f(x)$, and there are only a finite number of possible divisors of $f(x)$ in E. Hence there are only a finite number of possible B's.

(b) Assume there are only a finite number of fields between E and F. Should F consist only of a finite number of elements, then E is generated by one element according to the Corollary on page 41. We may therefore assume F to

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

THEOREM 26. If $E = F(\alpha_1,\alpha_2,\ldots,\alpha_n)$ is a finite extension of the field F, and $\alpha_1,\alpha_2,\ldots,\alpha_n$ are separable elements in E, then there exists a primitive θ in E such that $E = F(\theta)$.

Proof: Let $f_1(x)$ be the irreducible equation of α_1 in F and let B be an extension of E that splits $f_1(x)f_2(x)\ldots f_n(x)$. Then B is normal over F and contains, therefore, only a finite number of intermediate fields (as many as there are subgroups of G). So the subfield E contains only a finite number of intermediate fields. Theorem 25 now completes the proof.

M. Existence of a Normal Basis.

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

THEOREM 27. If E is a normal extension of F and $\sigma_1,\sigma_2,\ldots,\sigma_n$ are the elements of its group G, there is an element

θ in E such that the n elements $\sigma_1(\theta), \sigma_2(\theta), \ldots, \sigma_n(\theta)$ are linearly independent with respect to F.

According to Theorem 26 there is an α such that $E = F(\alpha)$. Let $f(x)$ be the equation for α, put $\sigma_1(\alpha) = \alpha_1$, $g(x) = \frac{f(x)}{(x-\alpha)f'(\alpha)}$ and $g_1(x) = \sigma_1(g(x)) = \frac{f(x)}{(x-\alpha_1)f'(\alpha_1)}$.

$g_1(x)$ is a polynomial in E having α_k as root for $k \neq 1$ and hence

(1) $\quad g_1(x)\, g_k(x) \equiv 0 \pmod{f(x)}$ for $i \neq k$.

In the equation

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

the left side is of degree at most n - 1. If (2) is true for n different values of x, the left side must be identically 0. Such n values are $\alpha_1, \alpha_2, \ldots \alpha_n$, since $g_1(\alpha_1) = 1$ and $g_k(\alpha_1) = 0$ for $k \neq i$.

Multiplying (2) by $g_1(x)$ and using (1) shows:

(3) $\quad (g_1(x))^2 \equiv g_1(x) \pmod{f(x)}$.

We next compute the determinant

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

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

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

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

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

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

N. Theorem of Natural Rationality.

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 us denote by EB the splitting field of p(x) when p(x) is taken to lie in B. If $\alpha_1,\ldots,\alpha_s$ are the roots of p(x) in EB, then $F(\alpha_1,\ldots,\alpha_s)$ is a subfield of EB which is readily seen to form a splitting field for p(x) in F. By Theorem 10, E and $F(\alpha_1,\ldots,\alpha_s)$ are isomorphic. There is therefore no loss of generality if in the sequel we take $E = F(\alpha_1,\ldots,\alpha_s)$ and assume therefore that E is a subfield of EB. Also $EB = B(\alpha_1,\ldots,\alpha_s)$.

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

THEOREM 28. If G is the group of automorphisms of E over F, and H the group of EB over B, then H is isomorphic to the subgroup of G having $E \cap B$ as its fixed field.

Each automorphism of EB over B simply permutes $\alpha_1,\ldots,\alpha_s$ in some fashion and leaves B, and hence also F, fixed. Since the elements of EB 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 EB 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 EB 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. However, 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. It follows that $E \cap B$ is the fixed field of H.

Corollary: If, under the conditions of Theorem 28, the group G is of prime order, then either $H = G$ or H consists of the unit element alone.

Remark. The inductions in the proofs of Theorems 10 and 15 may be based on the number n of roots of the polynomial which are in the extension but not in the given field. This relieves the proofs of their dependence on Theorem 6, and also simplifies them.