ADVANCED ALGEBRA

Objectives of the Course	To study field extension, roots of polynomials, Galois Theory, finite fields, division rings, solvability by radicals and to develop computational skill in abstract algebra.
Course Outline	Unit I : Extension Fields – Transcendence of e Unit II : Roots of Polynomials – More about roots Unit III : Elements of Galois Theory Unit IV : Finite Fields – Wedderburn's theorem of finite division rings Unit V : Solvability by radicals – A theorem of Frobenius – Integral Quaternions and the Four-Square theorem.
Recommended Text	I.N. Herstein, Topics in Algebra (II Edition), Wiley Eastern Limited, New Delhi, 1975.

UNIT – I

1.1 EXTENSION FIELDS

In this section we shall be concerned with the relation of one field to another. Let Fbe a field; a field $K$is said to be an *extension* of$F$if Kcontains$F$. Equivalently, $K$is an extension of$F$if$F$ is a subfield of K.*Throughout this chapter F will denote a given field and K an extension of F.*

As was pointed out earlier, in the chapter on vector spaces, if Kisan extension of$F$, then, under the ordinary field operations in$K$, $K$is a vectorspace over F. As a vector space we may talk about linear dependence, dimension, bases, etc., in$K$ relative to F.

DEFINITION The *degree* of Kover $F$is the dimension of Kas a vectorspace over F.

We shall always denote the degree of Kover F by $[K:F]$. Of particular interest to us is the case in which $[K:F]$ is finite, that is, when $K$is finitedimensionalas a vector space over F. This situation is described by saying that $K$is a *finite extension* of F.

We start off with a relatively simple but, at the same time, highly effective result about finite extensions, namely,

THEOREM 1.1.1 *If L is a finite extension of K and if K is a finite extension of F, then L is a finite extension of F. Moreover,* $[L:F] = [L:K][K:F]$.

Proof. The strategy we employ in the proof is to write down explicitly a basis of L over F. In this way not only do we show that L is a finite extension of F, but we actually prove the sharper result and the one which is really the heart of the theorem, namely that $[L:F] = [L:K]\,[K:F]$.

Suppose, then, that $[L:K] = m$ and that $[K:F] = n$.

Let $v_1, v_2, \ldots, v_m$be a basis of Lover $K$and let $w_1, w_2, \ldots, w_n$be a basis of Kover F. What could possibly be nicer or more natural than to have the elements $v_i\, w_j$, where $i = 1, 2, \ldots, m, j = 1, 2, \ldots, n$, serve as a basis of Lover F?

Whatever else, they do at least provide us with the right number of elements. We now proceed to show that they do in fact form a basis of Lover F. What do we need to establish this? First we must show that every element in $L$is a linear combination of them with coefficients in F, and then we must demonstrate that these mnelements are linearly independent over F.

Let t be any element in L.

Since every element in $L$is a linear combination of $v_1, v_2, \dots, v_m$with coefficients in K, in particular, $t$must be of this form.

Thus $t = k_1v_1 + \cdots + k_mv_m$,where the elements $k_1, \dots, k_m$are all in K. However, every element in $K$is a linear combination of$w_1, \dots, w_n$withcoefficients in F.

Thus $k_1 = f_{11}w_1 + \cdots + f_{1n}w_n, \dots, k_i = f_{i1}w_1 + \cdots + f_{in}w_n, \dots, k_m = f_{m1}w_1 + \cdots + f_{mn}w_n$, where every $f_{ij}$is in F.

Substituting these expressions for $k_1, \dots, k_m$into $t = k_1v_1 + \cdots + k_mv_m$,we obtain $t = (f_{11}w_1 + \cdots + f_{1n}w_n)v_1 + \cdots + (f_{m1}w_1 + \cdots + f_{mn}w_n)v_m$

Multiplying this out, using the distributive and associative laws, we finally arrive at $t = f_{11}v_1w_1 + \cdots + f_{1n}v_1w_n + \cdots + f_{ij}v_iw_j + \cdots + f_{mn}v_mw_n$.

Since the $f_{ij}$are in F, we have realized $t$as a linear combination over F of the elements v_iw_j.

Therefore, the elements $v_iw_j$do indeed span all of L over F, and so they fulfill the first requisite property of a basis.

We still must show that the elements $v_iw_j$are linearly independent over F.

Suppose that $f_{11}v_1w_1 + \cdots + f_{1n}v_1w_n + \cdots + f_{ij}v_iw_j + \cdots + f_{mn}v_mw_n = 0$, where the f_{ij} are in F.

Our objective is to prove that each $f_{ij} = 0$.

Regrouping the above expression yields $(f_{11}w_1 + \cdots + f_{1n}w_n)v_1 + \cdots + (f_{i1}w_1 + \cdots + f_{in}w_n)v_i + \cdots + (f_{m1}w_1 + \cdots + f_{mn}w_n)v_m = 0$.

Since the w_i are in K, and since $K \supset F$, all the elements $k_i = f_{i1}w_1 + \cdots + f_{in}w_n$are in K. Now $k_1v_1 + \cdots + k_mv_m = 0$ with $k_1, \ldots, k_m \in K$.

But, by assumption, $v_1, \ldots, v_m$form a basis of Lover K, so, in particular they must be linearly independent over K.

The net result of this is that$k_1 = k_2 = \cdots = k_m = 0$. Using the explicit values of the k_i, we get

$f_{i1}w_1 + \cdots + f_{in}w_n = 0$ for $i = 1,2, \ldots, m$.

But now we invoke the fact that the $w_i$are linearly independent over F; this yields that each $f_{ij} = 0$.

In other words, we have proved that the$v_iw_j$are linearly independent over F. In this way they satisfy the other requisite property for a basis.

We have now succeeded in proving that the mnelements v_iw_j form abasis of L over F. Thus $[L: F] = mn$; since $m = [L: K]$and $n = [K: F]$we have obtained the desired result $[L : F] = [L: K][K: F]$.

Suppose that $L, K, F$are three fields in the relation $L \supset K \supset F$and, suppose further that $[L: F]$ is finite.

Clearly, any elements in Llinearly independent over $K$are, all the more so, linearly independent over F.Thus the assumption that $[L: F]$ is finite forces the conclusion that $[L: K]$is finite. Also, since $K$is a subspace of L, $[K: F]$ is finite. By the theorem,$[L: F] = [L: K][K: F]$, whence $[K: F]|[L: F]$. We have proved the result.

COROLLARY: *If L is a finite extension of$F$ and K is a subjield of L which contains F, then* $[K: F]|[L: F]$.

Thus, for instance, if $[L:F]$ is a prime number, then there can be nofields properly between $F$and L.

A little later, in Section 5.4, when we discuss the construction of certain geometric figures by straightedge and compass, this corollary will be of great significance.

DEFINITION An element $a \in K$is said to be *algebraic over* Fif there existelements $\alpha_0, \alpha_1, \ldots, \alpha_n$in F, not all 0, such that$\alpha_0 a^n + \alpha_1 a^{n-1} + \cdots + \alpha_n = 0$.

If the polynomial $q(x) \in F[x]$, the ring of polynomials in $x$over F, and$q(x) = \beta_0 a^m + \beta_1 a^{m-1} + \cdots + \beta_m$, then for any element $b \in K$, by $q(b)$ we shall mean the element $\beta_0 b^m + \beta_1 b^{m-1} + \cdots + \beta_m$in K.

In the expression commonly used, $q(b)$is the *value* of the polynomial $q(x)$obtainedby substituting b for x.

The element b is said to *satisfy* $q(x)$ if $q(b) = 0$. In these terms, $a \in K$is algebraic over Fif there is a nonzero polynomial$p(x) \in F[x]$which $a$satisfies, that is, for which $p(a) = 0$.

Let K be an extension of$F$and let $a$be in K.

Let $\mathcal{M}$ be the collection ofall subfields of Kwhich contain both $F$and a.

$\mathcal{M}$ is not empty, for Kitselfis an element of $\mathcal{M}$.

Now, as is easily proved, the intersection of any number of subfields of $K$is again a subfield of K.

Thus the intersection of all those subfields of Kwhich are members of $\mathcal{M}$is a subfield of K. We denote this subfield by $F(a)$. What are its properties? Certainly it contains both $F$and a, since this is true for every subfield of Kwhich is a member of $\mathcal{M}$.

Moreover, by the very definition of intersection, every subfield of Kin $\mathcal{M}$contains $F(a)$, yet $F(a)$itself is in $\mathcal{M}$.

Thus $F(a)$ is the smallest subfield of K containing both F and a. We call $F(a)$ the subfield obtained by *adjoining* a to F.

Our description of $F(a)$, so far, has been purely an external one.

We now give an alternative and more constructive description of $F(a)$. Consider all these elements in K which can be expressed in the form $\beta_0 + \beta_1 a + \cdots + \beta_s a^s$; here the $\beta's$ can range freely over F and s can be any nonnegative integer. As elements in K, one such element can be divided by another, provided the latter is not 0. Let U be the set of all such quotients. We leave it as an exercise to prove that U is a subfield of K.

On one hand, U certainly contains F and a, whence $U \supset F(a)$.

On the other hand, any subfield of K which contains both F and a, by virtue of closure under addition and multiplication, must contain all the elements $\beta_0 + \beta_1 a + \cdots + \beta_s a^s$ where each $\beta_i \in F$.

Thus $F(a)$ must contain all these elements; being a subfield of K, $F(a)$ must also contain all quotients of such elements.

Therefore, $F(a) \supset U$. The two relations $U \subset F(a)$, $U \supset F(a)$ of course imply that $U = F(a)$.

In this way we have obtained an internal construction of $F(a)$, namely as U.

We now intertwine the property that $a \in K$ is algebraic over F with macroscopic properties of the field $F(a)$ itself. This is

THEOREM 1.1.2 *The element $a \in K$ is algebraic over F if and only if $F(a)$ is a finite extension of F.*

Proof. As is so very common with so many such "if and only if" propositions, one-half of the proof will be quite straightforward and easy, whereas the other half will be deeper and more complicated.

Suppose that $F(a)$is a finite extension of $F$and that $[F(a):F] = m$.

Consider the elements $1, a, a^2, \dots, a^m$; they are all in $F(a)$and are $m + 1$in number.

By Lemma, these elements are linearly dependent over F.

Therefore, there are elements$\alpha_0, \alpha_1, \dots, \alpha_n$in F, not all 0, such that $\alpha_0 1 + \alpha_1 a + \alpha_2 a^2 + \cdots + \alpha_m a^m = 0$.

Hence a is algebraic over F and satisfies the nonzero polynomial $p(x) = \alpha_0 + \alpha_1 x + \cdots + \alpha_m x^m$in $F[x]$of degree at most $m = [F(a):F]$.

This proves the "if" part of the theorem.

Now to the "only if" part.

Suppose that a in $K$is algebraic over F.

By assumption, a satisfies some nonzero polynomial in $F[x]$; let $p(x)$ be a polynomial in $F[x]$of smallest positive degree such that $p(a) = 0$.

We claim that $p(x)$ is irreducible over F. For, suppose that $p(x) = f(x)g(x)$,where$f(x), g(x) \in F[x]$; then $0 = p(a) = f(a)g(a)$(see Problem 1) and since,$f(a)$and $g(a)$are elements of the field K, the fact that their product is 0 forces $f(a) = 0$ or $g(a) = 0$.

Since $p(x)$ is of lowest positive degree$p(a) = 0$, we must conclude that one of $\deg f(x) \geq \deg p(x)$or$\deg g(x) \geq \deg p(x)$ must hold. But this proves the irreducibility of $p(x)$.

We define the mapping $\Psi$from $F[x]$into $F(a)$as follows. For any $h(x) \in F[x]$, $h(x)\Psi = h(a)$.

We leave it to the reader to verify that $\Psi$is aring homomorphism of the ring $F[x]$into the field $F(a)$(see Problem 1).

What is V, the kernel of Ψ? By the very definition of Ψ, $V = \{h(x) \in F[x] | h(a) = 0\}$. Also, $p(x)$is an element of lowest degree in the ideal V of $F[x]$.

Thus, every element in V is a multiple of $p(x)$, and since $p(x)$ is irreducible, by Lemma $V$is a maximal ideal of $F[x]$. Therefore, $F[x]/V$is a field.

Now by the general homomorphism theorem for rings, $F[x]/V$ is isomorphic to the image of $F[x]$ under Ψ.

Summarizing, we have shown that the image of $F(x)$under Ψ is a subfield of $F(a)$.

This image contains $x\Psi = a$ and, for every $\alpha \in F, \alpha\Psi = \alpha$.

Thus the image of $F[x]$under Ψ is a subfield of $F[a]$which contains both F and a; by the very definition of $F(a)$we are forced to conclude that the image of $F[x]$under Ψ is all of $F(a)$. Put more succinctly, $F[x]/V$is isomorphic to $F(a)$.

Now, $V = (p(x))$, the ideal generated by $p(x)$; from this we claim that dimension of $F[x]/V$, as a vector space over F, is precisely equal to$p(x)$. In view of the isomorphism between $F[x]/V$ and $F(a)$ we obtain the fact that $[F(a):F] = deg\ p(x)$.

Therefore, $[F(a):F]$ is certainly finite; this is the contention of the "only if" part of the theorem.

Note that we have actually proved more, namely that $[F(a):F]$ is equal to the degree of the polynomial of least degree satisfied by $a$over F.

The proof we have just given has been somewhat long-winded, but deliberately so. The route followed contains important ideas and ties in results and concepts developed earlier with the current exposition. No part of mathematics is an island unto itself.

We now redo the "only if" part, working more on the inside of $F(a)$. This reworking is, in fact, really identical with the proof already given; the constituent pieces are merely somewhat differently garbed.

Again let $p(x)$ be a polynomial over $F$of lowest positive degree satisfied by a. Such a polynomial is called a *minimal polynomial* for a over F. We may assume that its coefficient of the highest power of *x* is 1, that is, it is monic; in that case we can speak of *the* minimal polynomial for $a$over Fforany two minimal, monic polynomials for $a$over $F$are equal. (Prove!)

Suppose that $p(x)$is of degree n; thus $p(x) = x^n + \alpha_1 x^{n-1} + \cdots + \alpha_n$where the $\alpha_i$are in F. By assumption, $a^n + \alpha_1 a^{n-1} + \cdots + \alpha_n = 0$,whence $a^n = -\alpha_1 a^{n-1} - \alpha_2 a^{n-2} - \cdots - \alpha_n$. What about a^{n+1}?

From the above, $a^{n+1} = -\alpha_1 a^n - \alpha_2 a^{n-1} - \cdots - \alpha_n a$; if we substitute the expression for a^ninto the right-hand side of this relation, we realize a^{n+1}as a linear combination of the elements $1, a, \ldots, a^{n-1}$ over F. Continuing this way, we get that a^{n+k}, for $k \geq 0$, is a linear combination over$F$of $1, a, \ldots, a^{n-1}$.

Now consider $T = \{\beta_0 + \beta_1 a + \cdots + \beta_{n-1} a^{n-1} | \beta_0, \beta_1, \ldots, \beta_{n-1} \in F\}$.

Clearly, T is closed under addition; in view of the remarks made in the paragraph above, it is also closed under multiplication.

Whatever further it may be, T has at least been shown to be a ring. Moreover, T contains both $F$and a. We now wish to show that T is more than just a ring, that it is, in fact, a field.

Let $0 \neq u = \beta_0 + \beta_1 a + \cdots + \beta_{n-1} a^{n-1}$be in T and

let $h(x) = \beta_0 + \beta_1 x + \cdots + \beta_{n-1} x^{n-1} \in F[x]$.

Since $u \neq 0$, and $u = h(a)$, we have that $h(a) \neq 0$, whence $p(x) \nmid h(x)$. By the irreducibility of $p(x)$, $p(x)$and $h(x)$ must therefore be relatively prime. Hence we can find polynomials $s(x)$ and $t(x)$ in $F[x]$ such that $p(x)s(x) + h(x)t(x) = 1$. But then $1 = p(a)s(a) + h(a)t(a) = h(a)t(a)$, since $p(a) = 0$; putting into this that $u = h(a)$, we obtain $ut(a) = 1$.

The inverse of u is thus $t(a)$; in $t(a)$ all powers of a higher than $n-1$ can be replaced by linear combinations of $1, a, \ldots, a^{n-1}$over F, whence $t(a) \in T$. We have shown that every nonzero element of Thas its inverse in T; consequently, $T$is a field.

However,$T \subset F(a)$, yet $F$and $a$are both contained in T, which results in $T = F(a)$.We have identified $F(a)$as the set of all expressions $\beta_0 + \beta_1 a + \cdots + \beta_{n-1}a^{n-1}$.

Now T is spanned over F by the elements $1, a, \ldots, a^{n-1}$in consequence of which $[T:F] \leq n$.

However, the elements $1, a, \ldots, a^{n-1}$ are linearly independent over F, for any relation of the form $\gamma_0 + \gamma_1 a + \cdots + \gamma_{n-1}a^{n-1}$, with the elements $\gamma_i \in F$, leads to the conclusion that a satisfies the polynomial $\gamma_0 + \gamma_1 a + \cdots + \gamma_{n-1}a^{n-1}$ over $F$of degree less than n.

This contradiction proves the linear independence of $1, a, \ldots, a^{n-1}$, and so these elements actually form a basis of Tover F, whence, in fact, we now know that $[T:F] = n$.

Since $T = F(a)$, the result$[F(a):F] = n$follows.

DEFINITION The element $a \in K$ is said to be *algebraic of degree* $n$over F if it satisfies a nonzero polynomial over $F$of degree $n$but no nonzeropolynomial of lower degree.

In the course of proving Theorem 1.1.2 (in each proof we gave), we proved somewhat sharper result than that stated in that theorem, namely,

THEOREM 1.1.3 *If $a \in K$ is algebraic of degree $n$over F, then $[F(a):F] = n$.*

This result adapts itself to many uses. We give now, as an immediate consequence thereof, the very interesting.

THEOREM 1.1.4 *If a, b in K are algebraic over F then $a \pm b$, ab, and $a|b$(if $b \neq 0$) are all algebraic over F. In other words, the elements in K which arealgebraic over F form a subfield of K.*

Proof. Suppose that a is algebraic of degree m over F while b is algebraic of degree n over F. *Thus,* the subfield $T = F(a)$of K is of degree m *over* F.

Now b is algebraic of degree n over F, *a fortiori* it is algebraic of degree at most $n$over T which contains F. Thus the subfield $W = T(b)$of K, again by Theorem 1.1.3, is of degree at most n *over*T. But $[W:F] = [W:T][T:F]$by Theorem 1.1.1; therefore, $[W:F] \leq mn$ and so $W$is afinite extension of F.

However, $a$and $b$are both in W, whence all of $a \pm b, ab,$ and $a|b$ are in W.

By Theorem 1.1.2, since $[W:F]$ is finite, these elements must be algebraic over F, thereby proving the theorem.

Here, too, we have proved somewhat more. Since $[W:F] \leq mn$, every element in Wsatisfies a polynomial of degree at most mnover F, whence the

COROLLARY: *If a and $b$in K are algebraic over F of degrees m and n, respectively,then $a \pm b, ab,$ and $a|b$ (if $b \neq 0$) are algebraic over F of degree at most mn.*

In the proof of the last theorem we made two extensions of the field F . The first we called T; it was merely the field $F(a)$. The second we called W and it was $T(b)$. Thus, $W = (F(a))(b)$; it is customary to write it as$F(a, b)$.

Similarly, we could speak about $F(b, a)$; it is not too difficult to prove that $F(a, b) = F(b, a)$. Continuing this pattern, we can define$F(a_1, a_2, \ldots, a_n)$for elements $a_1, a_2, \ldots, a_n$in$K$.

DEFINITION The extension $K$of F is called an *algebraic extension* of F if every element in$K$ is algebraic over F.

We prove one more result along the lines of the theorems we have proved so far.

THEOREM 1.1.5 *If $L$is an algebraic extension of K and if K is an algebraic extension of F, then L is an algebraic extension of F.*

Proof. Let $u$be any arbitrary element of $L;$ our objective is to show that$u$satisfies some nontrivial polynomial with coefficients in F.

What information do we have at present? We certainly do know that $u$satisfies somepolynomial $x^n + \sigma_1 x^{n-1} + \cdots + \sigma_n$where $\sigma_1, \sigma_2, \ldots, \sigma_n$are in K. But $K$is algebraic over $F;$ therefore, by several uses of Theorem 1.1.3, $M = F(\sigma_1, \sigma_2, \ldots, \sigma_n)$is a finite extension of F.

Since u satisfies the polynomial$x^n + \sigma_1 x^{n-1} + \cdots + \sigma_n$whose coefficients are in M, u is algebraic over M. Invoking Theorem 1.1.2 yields that $M(u)$is a finite extension of M.

However, by Theorem 1.1.1, $[M(u):F] = [M(u):M][M:F]$, whence $M(u)$is a finite extension of F.

But this implies that $u$is algebraic over F,completing proof of the theorem.

A quick description of Theorem 1.1.5: algebraic over algebraic is algebraic.

The preceding results are of special interest in the particular case in which $F$is the field of rational numbers and $K$the field of complex numbers.

DEFINITION A complex number is said to be an *algebraic number* if it is algebraic over the field of rational numbers.

A complex number which is not algebraic is called *transcendental.* At the present stage we have no reason to suppose that there are any transcendental numbers. In the next section we shall prove that the familiar real number e is transcendental. This will, of course, establish the existence of transcendental numbers. In actual fact, they exist in great abundance; in a very well-defined way there are more of them than there are algebraic numbers.

Theorem 1.1.4 applied to algebraic numbers proves the interesting fact that *the algebraic numbers form a field;* that is, the sum, products, and quotients of algebraic numbers are again algebraic numbers.

Theorem 1.1.5 when used in conjunction with the so-called "fundamental theorem of algebra," has the implication that the roots of a polynomial whose coefficients are algebraic numbers are themselves algebraic numbers.

1.2 THE TRANSCENDENCE OF e

In defining algebraic and transcendental numbers we pointed out that it could be shown that transcendental numbers exist. One way of achieving this would be the demonstration that some specific number is transcendental.

In 1851 Liouville gave a criterion that a complex number be algebraic using this, he was able to write down a large collection of transcendental numbers. For instance, it follows from his work that the number. $101001000000100 \ldots 10 \ldots$ is transcendental; here the number of zeros between successive ones goes as $1!, 2!, \ldots, n!, \ldots$.

This certainly settled the question of existence. However, the question whether some given, familiar numbers were transcendental still persisted. The first success in this direction was by Hermite, who in 1873 gave a proof that e is transcendental. His proof was greatly simplified by Hilbert. The proof that we shall give here is a variation, due to Hurwitz, of Hilbert's proof.

The number π offered greater difficulties. These were finally overcomeby Lindemann, who in 1882 produced a proof that $\pi$is transcendental.One immediate consequence of this is the fact that it is impossible, by straight edge and compass, to square the circle, for such a construction would lead to an algebraic number θsuch that $\theta^2 = \pi$. But if θ is algebraic then so is θ^2, in virtue of which π would be algebraic, in contradiction to Lindemann's result.

In 1934, working independently, Gelfond and Schneider proved that if$a$and $b$are algebraic numbers and if $b$is irrational, then $a^b$is transcendental.This answered in the affirmative the question raised by Hilbert whether$2^{\sqrt{2}}$ was transcendental.

For those interested in pursuing the subject of transcendental numbers further, we would strongly recommend the charming books by C. L. Siegel, entitled *Transcendental Numbers,* and by I. Niven, *Irrational Numbers.*

To prove that e is irrational is easy; to prove that $\pi$is irrational is muchmore difficult. For a very clever and neat proof of the latter, see the paperby Niven entitled "A simple proof that $\pi$is irrational," *Bulletin of the AmericanMathematical Society,* Vol. 53 (194 7), page 509.

Now to the transcendence of e. Aside from its intrinsic interest, its proofoffers us a change ofpace. Up to this point all our arguments have been ofan algebraic nature; now, for a short while, we return to the more familiargrounds of the calculus. The proof itself will use only elementary calculus;the deepest result needed, therefrom, will be the mean value theorem.

THEOREM 1.2.1 *The numbere is transcendental.*

Proof.In the proof we shall use the standard notation $f^{(i)}(x)$to denote the *ith* derivative of $f(x)$with respect to x.

Suppose that $f(x)$ is a polynomial of degree r with real coefficients.

Let $F(x) = f(x) + f^{(1)}(x) + f^{(2)}(x) + \cdots + f^{(r)}(x)$.

We compute $(d/dx)\left(e^{-x}F(x)\right)$; using the fact that$f^{(r+1)}(x) = 0$ (Since $f(x)$ is of degree r) and the basic property of e, namely that$(d/dx)e^{x} = e^{x}$, we obtain$(d/dx)\left(e^{-x}F(x)\right) = -e^{-x}f(x)$.

The mean value theorem asserts that if $g(x)$is a continuously differentiable, single-valued function on the closed interval $[x_1, x_2]$then

$\frac{g(x_1)-g(x_2)}{x_1-x_2} = g^{(1)}\left(x_1 + \theta(x_2 - x_1)\right)$, where $0 < \theta < 1$.

We apply this to our function $e^{-x}F(x)$, which certainly satisfies all the required conditions for the mean value theorem on the closed interval$[x_1, x_2]$where $x_1 = 0$ and $x_2 = k$, where $k$is any positive integer. We then obtain that $e^{-x}F(k) - F(0) = -e^{-\theta_k k}f(\theta_k k)k$, where $\theta_k$depends on $k$andis some real number between 0 and 1. Multiplying this relation through bye^{k}yields $F(k) - F(0)e^{k} = -e^{(1-\theta_k)k}f(\theta_k k)k$.We write this out explicitly:

$$F(1) - eF(0) = -e^{(1-\theta_1)}f(\theta_1) = \varepsilon_1,$$

$$F(2) - e^2F(0) = -2e^{2(1-\theta_2)}f(2\theta_2) = \varepsilon_2 \qquad (1)$$

$$\vdots$$

$$F(n) - e^nF(0) = -ne^{n(1-\theta_n)}f(n\theta_n) = \varepsilon_n.$$

Suppose now that $e$is an algebraic number; then it satisfies some relationof the form

$$c_ne^n + c_{n-1}e^{n-1} + \cdots + c_1e + c_0 = 0, \qquad (2)$$

where$c_1, c_2, \ldots, c_n$are integers and where $c_0 > 0$.

In the relations (1) let us multiply the first equation by c_1, the second by$c_2$and so on; adding these up we get $c_1F(1) + c_2F(2) + \cdots + c_nF(n) - F(0)(c_1e + c_2e^2 + \cdots + c_ne^n) = c_1\varepsilon_1 + c_2\varepsilon_2 + \cdots + c_n\varepsilon_n$.

In view of relation (2), $c_1e + c_2e^2 + \cdots + c_ne^n = -c_0$, whence theabove equation simplifies to

$$c_0F(0) + c_1F(1) + \cdots + c_nF(n) = c_1\varepsilon_1 + c_2\varepsilon_2 + \cdots + c_n\varepsilon_n \qquad (3)$$

All this discussion has held for the $F(x)$constructed from an arbitrarypolynomial $f(x)$. We now see what all this implies for a very specificpolynomial, one first used by Hermite, namely,

$$f(x) = \frac{1}{(p-1)!}x^{p-1}(1-x)^p(2-x)^p \ldots (n-x)^p.$$

Here $p$can be any prime number chosen so that $p > n$ and $p > c_0$.

For this polynomial we shall take a very close look at $F(0), F(1), \ldots, F(n)$and we shall carry out an estimate on the size of $\varepsilon_1, \varepsilon_2, \ldots, \varepsilon_n$.

When expanded, $f(x)$is a polynomial of the form

$$\frac{(n!)^p}{(p-1)!}x^{p-1} + \frac{a_0x^p}{(p-1)!} + \frac{a_1x^{p+1}}{(p-1)!} + \cdots,$$

wherea_0, a_1, ..., are integers.

When $i \geq p$we claim that $f^{(i)}(x)$is a polynomial, with coefficientswhich are integers all of which are multiples of p. (Prove! See Problem 2.)

Thus for any integer j, $f^{(i)}(j)$, for $i \geq p$, is an integer and is a multiple of p.

Now, from its very definition,$f(x)$ has a root of multiplicity p at $x = 1,2,\ldots,n$. Thus for $j = 1,2,\ldots,n, f(j) = 0, f^{(1)}(j) = 0, \ldots, f^{(p-1)}(j) = 0$.

However, $F(j) = f(j) + f^{(1)}(j) + \cdots + f^{(p-1)}(j) + f^{(p)}(j) + \cdots + f^{(r)}(j)$; by the discussion above, for $j = 1,2,\ldots,n$, $F(j)$ *is an integer and is a multiple of$p$.*

What about $F(0)$? Since $f(x)$has a root of multiplicity $p-1$at $x = 0, f(0) = f^{(1)}(0) = \cdots = f^{(1p-2)}(0) = 0$. For $i \geq p, f^{(i)}(0)$is an integer which is a multiple of p.

But $f^{(p-1)}(0) = (n!)^p$and since $p > n$and is aprime number, $p \nmid (n!)^p$ so that $f^{(p-1)}(0)$*is an integer not divisible by p.*

Since $F(0) = f(0) + f^{(1)}(0) + \cdots + f^{(p-2)}(0) + f^{(p-1)}(0) + f^{(p)}(0) + \cdots + f^{(r)}(0)$, we conclude that $F(0)$ *is an integer not divisible by p.*

Because$c_0 > 0$ and $p > c_0$and because $p \nmid F(0)$whereas $p|F(1), p|F(2), \ldots, p|F(n)$, we can assert that $c_0F(0) + c_1F(1) + \cdots + c_nF(n)$*is an integer and is not divisible by p.*

However, by (3), $c_0F(0) + c_1F(1) + \cdots + c_nF(n) = c_1\varepsilon_1 + c_2\varepsilon_2 + \cdots + c_n\varepsilon_n$.

What can we say about ε_i*?* Let us recall that

$$\varepsilon_i = \frac{-e^{i(1-\theta_i)}(1 - i\theta_i)^p \ldots (n - i\theta_i)^p (i\theta_i)^{p-1} i}{(p-1)!},$$

Where$0 < \theta_i < 1$.Thus

$$|\varepsilon_i| \leq e^n \frac{n^p (n!)^p}{(p-1)!}$$

As $p \to \infty$,

$$\frac{e^n n^p (n!)^p}{(p-1)!} \to 0,$$

(Prove!) whence we can find a prime number larger than both $c_0$and n and large enough to force $|c_1\varepsilon_1 + c_2\varepsilon_2 + \cdots + c_n\varepsilon_n| < 1$. But $c_1\varepsilon_1 + c_2\varepsilon_2 + \cdots + c_n\varepsilon_n = c_0F(0) + \cdots + c_nF(n) = 0$, *so must be an integer;* since it is smaller than 1 insize our only possible conclusion is that $c_1\varepsilon_1 + c_2\varepsilon_2 + \cdots + c_n\varepsilon_n = 0$.

Consequently,$c_0F(0) + \cdots + c_nF(n) = 0$; this however is sheer nonsense, sincewe know that$p \nmid \big(c_0F(0) + \cdots + c_nF(n)\big)$, whereas $p|0$. This contradiction,stemming from the assumption that $e$is algebraic, proves that $e$mustbe transcendental.

UNIT – II

2.1 ROOTS OF POLYNOMIALS

In Section 1.1 we discussed elements in a given extension $K$of$F$ which were algebraic over F, that is, elements which satisfied polynomials in $F[x]$. We now turn the problem around; given a polynomial $p(x)$in $F[x]$ we wish to find a field K which is an extension of F in which $p(x)$has a root.No longer is the field Kavailable to us; in fact it is our prime objective toconstruct it. Once it is constructed, we shall examine it more closely and see what consequences we can derive.

DEFINITIONIf $p(x) \in F[x]$, then an element a lying in some extension field of F is called a *root* of $p(x)$if $p(a) = 0$.

We begin with the familiar result known as the *Remainder Theorem.*

LEMMA 2.1.1: *If $p(x) \in F[x]$ and if K is an extension of F, then for any element $b \in K$,*

$p(x) = (x - b)q(x) + p(b)$ *where* $q(x) \in K[x]$ *and where* $\deg q(x) \deg p(x) - 1$.

Proof: Since $F \subset K$, $F[x]$is contained in $K[x]$, whence we can consider $p(x)$ to be lying in $K[x]$.

By the division algorithm for polynomials in $K[x]$, $p(x) = (x - b)q(x) + r$, where $q(x) \in K[x]$ and where $r = 0$ or $\deg r < \deg(x - b) = 1$.

Thus either $r = 0$ or $\deg r = 0$; in either case r must be an element of K.

But exactly what element of K is it? Since $p(x) = (x - b)q(x) + r$, $p(b) = (b - b)q(b) + r = r$.

Therefore, $p(x) = (x - b)q(x) + p(b)$. That the degree of $q(x)$ is one less than that of $p(x)$ is easy to verify and is left to the reader.

COROLLARY: *If $a \in K$ is a root of $p(x) \in F[x]$, where $F \subset K$, then in $K[x]$,$(x - a)|p(x)$.*

Proof: From Lemma 2.1.1, in $K[x]$, $p(x) = (x-a)q(x) + p(a) = (x-a)q(x)$since $p(a) = 0$. Thus $(x-a)|p(x)$ in $K[x]$.

DEFINITION: The element $a \in K$ is a root of $p(x) \in F[x]$ of *multiplicity* m if $(x-a)^m | p(x)$, where as $(x-a)^{m+1} \nmid p(x)$.

A reasonable question to ask is, How many roots can a polynomial have in a given field? Before answering we must decide how to count a root of multiplicity m. *We shall always count it as m roots.* Even with this convention we can prove.

LEMMA 2.1.2 *A polynomial of degree n over a field can have at most n roots in any extension field.*

Proof: We proceed by induction on n, the degree of the polynomial$p(x)$. If $p(x)$ is of degree 1, then it must be of the form $\alpha x + \beta$where α, β are in a field $F$and where $\alpha \neq 0$.

Any a such that $p(a) = 0$ must then imply that $\alpha a + \beta = 0$, from which we conclude that $a = -\beta/\alpha$.

That is, $p(x)$ has the unique root $-\beta/\alpha$, whence the conclusion of the lemma certainly holds in this case.

Assuming the result to be true in any field for all polynomials of degree less than n, let us suppose that $p(x)$ is of degree n over F.

Let K be any extension of F. If $p(x)$ has no roots in$K$, then we are certainly done, for the number of roots in K, namely zero, is definitely at most n.

So, suppose that $p(x)$ has at least one root $a \in K$and that $a$is a root of multiplicity m. Since $(x-a)^m | p(x), m \leq n$follows.

Now $p(x) = (x-a)^m q(x)$, where $q(x) \in K[x]$is of degree $n-m$. From the fact that $(x-a)^{m+1} \nmid p(x)$, we get that$(x-a) \nmid q(x)$, whence, by the corollary to Lemma 2.1.1, a is not a root of $q(x)$.

If $b \neq a$ is a root, in K, of $p(x)$, then $0 = p(b) = (b-a)^m q(b)$; however, since $b - a \neq 0$ and since we are in a field, we conclude that $q(b) = 0$.

That is, any root of $p(x)$, in K, other than a, must be a root of $q(x)$. Since $q(x)$ is of degree $n - m < n$, by our induction hypothesis, $q(x)$ has at most $n - m$ roots in K, which, together with the other root a, counted m times, tells us that $p(x)$has at most $m + (n - m) = n$roots in K.

This completes the induction and proves the lemma.

One should point out that commutativity is essential in Lemma 2.1.2.

If we consider the ring of real quaternions, which falls short of being a field only in that it fails to be commutative, then the polynomial $x^2 + 1$has atleast 3 roots, i, j, k (in fact, it has an infinite number of roots).

In a somewhat different direction we need, even when the ring is commutative, that it be an integral domain, for if $ab = 0$ with $a \neq 0$ and $b \neq 0$ in the commutativering R, then the polynomial ax of degree 1 over R has at least two distinct roots $x = 0$ and $x = b$ in R.

The previous two lemmas, while interesting, are of subsidiary interest.

We now set ourselves to our prime task, that of providing ourselves with suitable extensions of F in which a given polynomial has roots.

Once this is done, we shall be able to analyze such extensions to a reasonable enoughdegree of accuracy to get results. The most important step in the construction is accomplished for us in the next theorem.

The argument used will be very reminiscent of some used in Section 1.1.

THEOREM 2.1.1: *If $p(x)$ is a polynomial in $F[x]$ of degree $n \geq 1$and is irreducible over F, then there is an extension E of F, such that $[E:F] = n$, in whichp(x) has a root.*

Proof. Let $F[x]$ be the ring of polynomials in $x$over $F$and let $V = (p(x))$ be the ideal of $F[x]$generated by $p(x)$.

By Lemma, $V$is amaximal ideal of $F[x]$, whence by Theorem, $E = F[x]|V$ is a field. This Ewill be shown to satisfy the conclusions of the theorem.

First we want to show that E is an extension of F; however, in fact, it is not! But let F be the image of$F$in E; that is,$F = \{\alpha + V | \alpha \in F\}$.

We assert that F is a field isomorphic to F; in fact, if Ψ is the mapping from$F[x]$ into $F[x]|V = E$defined by $f(x)\Psi = f(x) + V$, then the restriction of Ψ to F induces an isomorphism of F onto F. (Prove!)

Using this isomorphism, we identify F and *in this way we can consider E to be an extension of F*.

We claim that E is a finite extension of F of degree $n = \deg p(x)$, for the elements $1 + V, x + V, (x + V)^2 = x^2 + V, \dots, (x + V)^i = x^i + V, \dots, (x + V)^{n-1} = x^{n-1} + V$ form a basis of Eover F. (Prove!)

For convenience of notation let us denote the element $x\Psi = x + V$ in the field Eas a. Given $f(x) \in F[x]$, what is $f(x)\Psi$?

We claim that it is merely,$f(a)$, for, since Ψ is a homomorphism, if $f(x) = \beta_0 + \beta_1 x + \cdots + \beta_k x^k$,then $f(x)\Psi = \beta_0\Psi + (\beta_1\Psi)(x\Psi) + \cdots + (\beta_k\Psi)(x\Psi)^k$and using the identification indicated above of $\beta\Psi$ with β, we see that $f(x)\Psi = f(a)$.

In particular, since $p(x) \in V$, $p(x)\Psi = 0$; however, $p(x)\Psi = p(a)$. *Thus the element $a = x\Psi$ in E is a root of $p(x)$*. The field E has been shown to satisfy all the properties required in the conclusion of Theorem 2.1.1, and so this theorem is now proved.

An immediate consequence of this theorem is the

COROLLARY: *If $f(x) \in F[x]$, then there is a finite extension E of F in which $f(x)$ has a root. Moreover,* $[E:F] \leq \deg f(x)$.

Proof. Let $p(x)$ be an irreducible factor of $f(x)$; any root of $p(x)$ is a root of $p(x)$.

By the theorem there is an extension E of F with $[E:F] = \deg p(x) \leq deg\ f(x)$ in which $p(x)$, and so, $f(x)$ has a root.

Although it is, in actuality, a corollary to the above corollary, the next theorem is of such great importance that we single it out as a theorem.

THEOREM 2.1.2 *Let $f(x) \in F[x]$ be of degree $n \geq 1$. Then there is an extension E of F of degree at most $n!$ in which $f(x)$ has n roots (and so, a full complement of roots).*

Proof. In the statement of the theorem, a root of multiplicity *m* is, of course, counted as *m* roots.

By the above corollary there is an extension E_0 of F with $[E_0:F] \leq n$ in which $f(x)$ has a root α. Thus in $E_0(x)$, $f(x)$ factors as $f(x) = (x-\alpha)q(x)$, where $q(x)$ is of degree $n-1$. Using induction (or continuing the above process), there is an extension E of E_0 of degree at most $(n-1)!$ in which $q(x)$ has $n-1$ roots.

Since any root of $f(x)$ is either α or a root of $q(x)$, we obtain in E all n roots of $f(x)$. Now, $[E:F] = [E:E_0][E_0:F] \leq (n-l)!\,n = n!$.

All the pieces of the theorem are now established.

Theorem 2.1.2 asserts the existence of a finite extension E in which the given polynomial $f(x)$, of degree n, over F has n roots.

If $f(x) = a_0x^n + a_1x^{n-1} + \cdots + a_n, a_0 \neq 0$ and if the n roots in E are $\alpha_1, \ldots, \alpha_n$ making use of the corollary to Lemma 2.1.1, $f(x)$ can be factored over E as

$$f(x) = a_0(x-\alpha_1)(x-\alpha_2)\ldots(x-\alpha_n).$$

Thus $f(x)$ splits up completely over E as a product of *linear* (first degree) factors.

Since a finite extension of F exists with this property, a *finite extension of F of minimal degree* exists which also enjoys this property of decomposing $f(x)$ as a product of linear factors.

For such a minimal extension, no proper subfield has the property that $f(x)$ factors over it into the product of linear factors.

DEFINITION If $f(x) \in F[x]$, a finite extension E of F is said- to be a *splitting field* over F for $f(x)$ if over E (that is, in $E[x]$), but not over any proper subfield of E, $f(x)$ can be factored as a product of linear factors.

We reiterate: *Theorem 2.1.2 guarantees for us the existence of splitting fields.*

In fact, it says even more, for it assures that given a polynomial of degree n over F there is a splitting field of this polynomial which is an extension of F of degree at most $n!$ over F.

We shall see later that this upper bound of $n!$ is actually taken on; that is, given n, we can find a field F and a polynomial of degree n in $F[x]$ such that the splitting field of $f(x)$ over F has degree $n!$.

Equivalent to the definition we gave of a splitting field for $f(x)$ over F is the statement: *E is a splitting field of $f(x)$ over F if E is a minimal extension of F in which $f(x)$ has n roots, where $n = deg\ f(x)$.*

An immediate question arises: given two splitting fields E_1 and E_2 of the same polynomial $f(x)$ in $F[x]$, what is their relation to each other?

At first glance, we have no right to assume that they are at all related.

Our next objective is to show that they are indeed intimately related; in fact, that they are isomorphic by an isomorphism leaving every element of F fixed. It is in this direction that we now turn.

Let F and F' be two fields and let τ be an isomorphism of F onto F'. For convenience let us denote the image of any $\alpha \in F$ under τ by α'; that is, $\alpha\tau = \alpha'$. We shall maintain this notation for the next few pages.

Can we make use of τ to set up an isomorphism between $F[x]$ and $F'[t]$, the respective polynomial rings over F and F'? Why not try the obvious?

For an arbitrary polynomial $f(x) = \alpha_0 x^n + \alpha_1 x^{n-1} + \cdots + \alpha_n \in F[x]$ we define τ^* by $f(x)\tau^* = (\alpha_0 x^n + \alpha_1 x^{n-1} + \cdots + \alpha_n)\tau^* = \alpha_0' t^n + \alpha_1' t^{n-1} + \cdots + \alpha_n'$

It is an easy and straightforward matter, which we leave to the reader to verify.

LEMMA 2.1.3 : *τ^* defines an isomorphism of $F[x]$ onto $F'[t]$ with the property that $\alpha\tau^* = \alpha'$ for every $\alpha \in F$.*

If $f(x)$is in $F[x]$we shall write $f(x)\,\tau^*$ as $f'(t)$. Lemma 2.1.3 immediately implies that factorizations of $f(x)$in $F[x]$ result in like factorizations of $f'(t)$in $F'[t]$, and vice versa.

In particular, $f(x)$ is irreducible in $F[x]$ if and only if $f'(t)$ is irreducible in $F'[t]$.

However, at the moment, we are not particularly interested in polynomial rings, but rather, in extensions of F. Let us recall that in the proof of Theorem 1.1.2 we employed quotient rings of polynomial rings to obtain suitable extensions of F.

In consequence it should be natural for us to study the relationship between $F[x]/(f(x))$ and $F'[t]/(f'(t))$, where $(f(x))$ denotes the ideal generated by $f(x)$ in $F[x]$and $(f'(t))$that generated by $f'(t)$in $F'[t]$.

The next lemma, which is relevant to this question, is actually part of a more general, purely ring-theoretic result, but we shall content ourselves with it as applied in our very special setting.

LEMMA 2.1.4 *There is an isomorphism τ^{**} if $F[x]/(f(x))$ onto $F'[t]/(f'(t))$* with the property that for every $\alpha \in F, \alpha\tau^{**} = \alpha', \Big(x + \big(f(x)\big)\Big)\tau^{**} = t + (f'(t))$.

Proof. Before starting with the proof proper, we should make clear what is meant by the last part of the statement of the lemma.

As we have already done several times, we can consider F as imbedded in $F[x]/(f(x))$ by identifying the element $\alpha \in F$ with the coset $\alpha + (f(x))$ in $F[x]/(f(x))$.

Similarly, we can consider F' to be contained in $F'[t]/(f'(t))$.

The isomorphism τ^{**} is then supposed to satisfy $[\alpha + (f(x))]\tau^{**} = \alpha' + (f'(t))$.

We seek an isomorphism $\tau^{**}$of $F[x]/(f(x))$onto $F'[t]/(f'(t))$.

What could be simpler or more natural than to try the τ^{**}defined by$[g(x) + (f(x))]\ \tau^{**} = g'(t) + (f'(t))$for every $g(x) \in F[x]$*?*

We leave it as an exercise to fill in the necessary details that the τ^{**} so defined is well defined and is an isomorphism of $F[x]/(f(x))$onto $F'[t]/(f'(t))$with theproperties needed to fulfill the statement of Lemma 2.1.4.

For our purpose-that of proving the uniqueness of splitting fields Lemma2.1.4 provides us with the entering wedge, for we can now prove

THEOREM 2.1.3 *If $p(x)$ is irreducible in $F[x]$ and if v is a root if$p(x)$, then $F(v)$ is isomorphic to $F'(w)$ where w is a root if $p'(t)$; moreover, this isomorphismσ can so be chosen that*

1. $v\sigma = w$.
2. $\alpha\sigma = \alpha'$*for every* $\alpha \in F$.

Proof. Let v be a root of the irreducible polynomial $p(x)$ lying in some extension $K$of F.

Let $M = \{f(x) \in F[x] | f(v) = 0\}$.

Trivially $M$is anideal of $F[x]$, and $M \neq F[x]$.

Since $p(x) \in M$ and is an irreducible polynomial, we have that $M = (p(x))$.

As in the proof of Theorem 1.1.2, map$F[x]$into $F(v) \subset K$ by the mapping Ψ defined by $q(x)\Psi = q(v)$ for every $q(x) \in F[x]$.

We saw earlier (in the proof of Theorem 1.1.2) that Ψ maps$F[x]$onto $F(v)$. The kernel of Ψ is precisely M, so must be $(p(x))$.

By the fundamental homomorphism theorem for rings there is an isomorphism Ψ^* of $F[x]/(p(x))$ onto $F(v)$.

Note further that $\alpha\Psi^* = \alpha$ for every $\alpha \in F$. Summing up: Ψ^* is an isomorphism of $F[x]/(p(x))$ onto $F(v)$ leaving every element of F fixed and with the property that $v = [x + (p(x))]\Psi^*$.

Since $p(x)$ is irreducible in $F[x]$, $p'(t)$is irreducible in $F'[t]$(by Lemma2.1.3), and so there is an isomorphismθ^* of $F'[t]/(p'(t))$ onto $F'(w)$ where w is a root of $p'(t)$ such that θ^* leaves every element of F' fixed and such that $[t + (p'(t)]\ \theta^* = w$.

We now stitch the pieces together to prove Theorem 2.1.3.

By· Lemma2.1.4 there is an isomorphism $\tau^{**}$of $F[x]/(p(x))$ onto $F'[t]/(p'(t))$ which coincides with τ on F and which takes $x + (p(x))$ onto $t + (p'(t))$. Consider the mapping $\sigma = (\Psi^*)^{-1}\tau^{**}\theta^*$ (motivated by

$$F(v) \xrightarrow{(\Psi^*)^{-1}} \frac{F[x]}{(p(x))} \xrightarrow{\tau^{**}} \frac{F'[t]}{(p'(t))} \xrightarrow{\theta^*} F'(w))$$

of $F(v)$onto $F'(w)$.

It is an isomorphism of $F(v)$ onto $F'(w)$ since all the mappingΨ^*, τ^{**}, and $\theta^*$are isomorphism's and onto.

Moreover, since$v = [x + (p(x))]\Psi^*$, $v\sigma = (v(\Psi^*)^{-1})\tau^{**}\theta^* = ([x + (p(x)]\tau^{**})\theta^* = [t + (p'(t))]\theta^* = w$. Also, for $\alpha \in F, \alpha\sigma = (\alpha(\Psi^*)^{-1})\tau^{**}\theta^* = (\alpha\tau^{**})\theta^* = \alpha'\theta^* = \alpha'$.

We have shown that $\sigma$is an isomorphism satisfying all therequirements of the isomorphism in the statement of the theorem. Thus Theorem 2.1.3 has been proved.

COROLLARY *If $p(x) \in F[x]$ is irreducible and if a, b are two roots of $p(x)$, then $F(a)$ is isomorphic to $F(b)$ by an isomorphism which takesa onto b and which leaves every element of F fixed.*

We now come to the theorem which is, as we indicated earlier, the foundation stone on which the whole Galois theory rests. For us it is the focal point of this whole section.

THEOREM 2.1.4 *Any splitting fields E and E' of the polynomials $f(x) \in F[x]$ and $f'(t) \in F'[t]$, respectively, are isomorphic by an isomorphism ϕ with the property that $\alpha\phi = \alpha'$ for every $\alpha \in F$. (In particular, any two splitting .fields of the same polynomial over a given field F are isomorphic by an isomorphism leaving every element of F fixed.)*

Proof. We should like to use an argument by induction; in order to do so, we need an integer-valued indicator of size which we can decrease by some technique or other.

We shall use as our indicator the degree of some splitting field over the initial field.

It may seem artificial (in fact, it may even be artificial), but we use it because, as we shall soon see, Theorem 2.1.3 provides us with the mechanism for decreasing it.

If $[E: F] = 1$, then $E = F$, whence $f(x)$ splits into a product of linear factors over F itself. By Lemma 2.1.3 $f'(t)$ splits over F' into a product of linear factors, hence $E' = F'$.

But then $\phi = \tau$ provides us with an isomorphism of E onto E' coinciding with τ on F.

Assume the result to be true for any field F_0 and any polynomial $f(x) \in F_o[x]$ provided the degree of some splitting field E_0 of $f(x)$ has degree less than n over F_0, that is, $[E_0: F_0] < n$.

Suppose that $[E: F] = n > 1$, where E is a splitting field of $f(x)$ over F.

Since $n > 1$, $f(x)$ has an irreducible factor $p(x)$ of degree $r > 1$.

Let $p'(t)$ be the corresponding irreducible factor of $f'(t)$.

Since E splits $f(x)$, a full complement of roots of $f(x)$, and so, *a priori*, of roots of $p(x)$, are in E.

Thus there is a $v \in E$ such that $p(v) = 0$; by Theorem 1.1.3, $[F(v): F] = r$.

Similarly, there is a $w \in E'$ such that $p'(w) = 0$. By Theorem 2.1.4 there is an isomorphism σ of $F(v)$onto $F'(w)$ with the property that $\alpha\sigma = \alpha'$for every $\alpha \in F$.

Since $[F(v):F] = r > 1$,

$$[E:F(v)] = \frac{[E:F]}{[F(v):F]} = \frac{n}{r} < n\,.$$

We claim that E is a splitting field for $f(x)$considered as a polynomial over $F_0 = F(v)$, for no subfield of E, containing $F_0$and hence F, can split$f(x)$,since $E$is assumed to be a splitting field of $f(x)$over F.

Similarly E' is a splitting field for $f'(t)$over $F_0' = F'(w)$.

By our induction hypothesis there is an isomorphism ϕ of Eonto E'such that $a\phi = a\sigma$ for all $a \in F_0$.

But for every $\alpha \in F$, $\alpha\sigma = \alpha'$ hence for every $\alpha \in F \subset F_0$, $\alpha\phi = \alpha\sigma = \alpha'$.

This completes the induction and proves the theorem.

To see the truth of the "(in particular ...)" part, let $F = F'$and let τ be the identity map at $\alpha\tau = \alpha$ for every $\alpha \in F$. Suppose that E_1 and E_2 are two splitting fields of $f(x) \in F[x]$. Considering $E_1 = E \supset F$and $E_2 = E' \supset F' = F$, and applying the theorem just proved, yields that E_1 and $E_2$are isomorphic by an isomorphism leaving every element of$F$fixed.

In view of the fact that any two splitting fields of the same polynomial over F are isomorphic and by an isomorphism leaving every element of F fixed, we are justified in speaking about *the* splitting field, rather than *a* splitting field, for it is essentially unique.

Examples

1. Let F be any field and let$p(x) = x^2 + \alpha x + \beta, \alpha, \beta \in F$, be in $F[x]$. If K is any extension of F in which $p(x)$ has a root, a, then the element $b = -\alpha.\ -a$ also in K is also a root of $p(x)$. If $b = a$it is easy to check that $p(x)$ must then be $p(x) = (x-a)^2$, and so both roots of $p(x)$are in$K$. If $b \neq a$ then again both roots of $p(x)$ are in K. Consequently,

$p(x)$can be split by an extension of degree 2 of F. We could also get this result directly by invoking Theorem 2.1.2.

2. Let F be the field of rational numbers and let $f(x) = x^3 - 2$. In the field of complex numbers the three roots of $f(x)$are $\sqrt[3]{2}, \omega\sqrt[3]{2}, \omega^2\sqrt[3]{2}$, where $\omega = \left(-1 + \sqrt{3}i/2\right)$ and where $\sqrt[3]{2}$ is a real cube root of 2. Now $F(\sqrt[3]{2})$ cannot split $x^3 - 2$, for, as a subfield of the real field-, it cannotcontain the complex, but not real, number $\omega\sqrt[3]{2}$. Without explicitly determining it, what can we say about E, the splitting field of $x^3 - 2$ over$F$? By Theorem 2.1.2, $[E:F] \leq 3! = 6$; by the above remark, since$x^3 - 2$ is irreducible over $F$and since $[F(\sqrt[3]{2}):F] = 3$, by the corollary toTheorem 5.1.1, $3 = [F(\sqrt[3]{2}):F]|[E:F]$. Finally, $[E:F] > [F(\sqrt[3]{2}):F] = 3$. The only way out is $[E:F] = 6$. We could, of course, get this result bymaking two extensions $F_1 = F(\sqrt[3]{2})$and $E = F_1(\omega)$ and showing that ωsatisfies an irreducible quadratic equation over F_1.
3. Let Fbe the field of rational numbers and let

$$f(x) = x^4 + x^2 + 1 \in F[x].$$

We claim that $E = F(\omega)$, where $\omega = (-1 + \sqrt{3}i)/2$, is a splitting field of $f(x)$.

Thus $[E:F] = 2$, far short of the maximum possible $4! = 24$.

2.2 MORE ABOUT ROOTS

We return to the general exposition. Let Fbe any field and, as usual, let$F[x]$be the ring of polynomials in x over F.

DEFINITION If $f(x) = \alpha_0 x^n + \alpha_1 x^{n-1} + \cdots + \alpha_i x^{n-i} + \cdots + \alpha_{n-1}x + \alpha_n$ in $F[x]$, then the *derivative of* $f(x)$, written as $f'(x)$, is the polynomial $f'(x) = n\alpha_0 x^{n-1} + (n-1)\alpha_1 x^{n-2} + \cdots + (n-i)\alpha_i x^{n-i-1} + \cdots + \alpha_{n-1}$in $F[x]$.

To make this definition or to prove the basic formal properties of the derivatives, as applied to polynomials, does not require the concept of a limit. However, since the field F is arbitrary, we might expect some strangethings to happen.

At the end of Section 1.2, we defined what is meant by the characteristic of a field.

Let us recall it now. A field F is said to be of characteristic 0 if $ma \neq 0$ for $a \neq 0$ in F and $m > 0$, an integer. If $ma = 0$ for some $m > 0$ and some $a \neq 0 \in F$, then F is said to be of finite characteristic.

In this second case, the characteristic of F is defined to be the smallest positive integer p such that $pa = 0$ for all $a \in F$.

It turned out that if F is of finite characteristic then its characteristic p is a prime number.

We return to the question of the derivative.

Let Fbe a field of characteristic $p \neq 0$. In this case, the derivative of the polynomial x^p is $px^{p-1} = 0$.

Thus the usual result from the calculus that a polynomial whose derivativeis 0 must be a constant no longer need hold true.

However, if the characteristic of F is 0 and if $f'(x) = 0$for $f(x) \in F[x]$, it is indeed true that$f(x) = \alpha \in F$(see Problem 1). Even when the characteristic of $F$is$p \neq 0$, we can still describe the polynomials with zero derivative; if $f'(x) = 0$, then $f(x)$ is a polynomial in x^p(see Problem 2).

We now prove the analogs of the formal rules of differentiation that weso well.

LEMMA 2.2.1*For any $f(x), g(x) \in F[x]$ and any $\alpha \in F$,*

1. $(f(x) + g(x))' = f'(x) + g'(x)$.
2. $(\alpha f(x))' = \alpha f'(x)$.
3. $(f(x)g(x))' = f'(x)g(x) + f(x)g'(x)$.

Proof.The proofs of parts 1 and 2 are extremely easy and are left asexercises. To prove part 3, note that from parts 1 and 2 it is enough toprove it in the highly special case $f(x) = x^i$and $g(x) = x^j$where both$i$and $j$are positive. But then $f(x)g(x) = x^{i+j}$, whence $(f(x)g(x))' = (i + j)x^{i+i-1}$; however, $f'(x)g(x) = ix^{i-1}x^j = ix^{i+j-1}$and $f(x)g'(x) = jx^i x^{j-1} = jx^{i+j-1}$; consequently, $f'(x)g(x) + f(x)g'(x) = (i + j)x^{i+j-1} = (f(x)g(x))'$.

Recall that in elementary calculus the equivalence is shown between the existence of a multiple root of a function and the simultaneous vanishing of the function and its derivative at a given point. Even in our setting, where F is an arbitrary field, such an interrelation exists.

LEMMA 2.2.2 *The polynomial $f(x) \in F[x]$ has a multiple root if and only if $f(x)$ and $f'(x)$ have a nontrivial (that is, of positive degree) common factor.*

Proof. Before proving the lemma proper, a related remark is in order, namely, if $f(x)$ and $g(x)$ in $F[x]$ have a nontrivial common factor in $K[x]$, for K an extension of F, then they have a nontrivial common factor in $F[x]$.

For, were they relatively prime as elements in $F[x]$, then we would beable to find two polynomials $a(x)$and $b(x)$in $F[x]$such that $a(x)f(x) + b(x)g(x) = 1$.

Since this relation also holds for those elements viewed as elements of $K[x]$, in $K[x]$ they would have to be relatively prime.

Now to the lemma itself. From the remark just made, we may assume, without loss of generality, that the roots *of* $f(x)$ all lie in F(otherwise extend$F$to K, ·the splitting field of $f(x)$). *If* $f(x)$has a multiple root α, then $f(x) = (x - \alpha)^m q(x)$, where $m > 1$.

However, as is easily computed, $((x - \alpha)^m)' = m(x - \alpha)^{m-1}$ whence, by Lemma 2.2.1, $f'(x) = (x - \alpha)^m q'(x) + m(x - \alpha)^{m-1} q(x) = (x - \alpha) r(x)$, since $m > 1$.

But this $f(x)$ and $f'(x)$ have the common factor $x - \alpha$, thereby proving the lemma in one direction.

On the other hand, if $f(x)$ has no multiple root then $f(x) = (x - \alpha_1)(x - \alpha_2) \ldots \ldots (x - \alpha_n)$where the $\alpha_i's$ are all distinct (we are supposing$f(x)$ to be monic). But then

$$f'(x) = \sum_{i=1}^{n} (x - \alpha_1) \ldots \widehat{(x - \alpha_i)} \ldots (x - \alpha_n)$$

where the ∧ denotes the term is omitted. We claim no root of$f\ (x)$ is a root of $f'(x)$, for

$$f'(\alpha_i) = \prod_{j \neq i} (\alpha_i - \alpha_j) \neq 0,$$

since the roots are all distinct.

However, if $f(x)$ and $f'(x)$have a nontrivial common factor, they have a common root, namely, any root of this commonfactor.

The net result is that $f(x)$ and $f'(x)$ have no nontrivial common factor, and so the lemma has been proved in the other direction.

COROLLARY 1 *If $f(x) \in F[x]$ is irreducible, then*

1. *If the characteristic of F is 0,$f(x)$ has no multiple roots.*
2. *If the characteristic of F is $p \neq 0$, $f(x)$ has a multiple root only if it is of the form$f(x) = g(x^p)$.*

Proof. Since$f(x)$ is irreducible, its only factors in $F[x]$ are 1 and$f(x)$.

*If $f(x)$*has a multiple root, then$f(x)$and $f'(x)$ have a nontrivial common factor by the lemma, hence $f(x)|f'(x)$.

However, since the degree of $f'(x)$ is less than that of $f(x)$, the only possible way that this can happen is for $f'(x)$ to be 0. In characteristic 0 this implies that $f(x)$ is a constant, which has no roots; in characteristic $p \neq 0$, this forces $f(x) = g(x^p)$.

We shall return in a moment to discuss the implications of Corollary 1 more fully.

COROLLARY 2 *If F is a field of characteristic $p \neq 0$, then the polynomial $x^{p^n} - x \in F[x]$,* for *$n \geq 1$, has distinct roots.*

Proof. The derivative of $x^{p^n} - x$is $p^n x^{p^n} - 1 = -1$, since F is of characteristic p. Therefore, $x^{p^n} - x$ and its derivative are certainly relatively prime, which, by the lemma, implies that $x^{p^n} - x$has no multipleroots.

Corollary 1 does not rule out the possibility that in characteristic $p \neq 0$an irreducible polynomial might have multiple roots.

To clinch matters, we exhibit an example where this actually happens.

Let F_0 be a field of characteristic 2 and let $F = F_0(x)$ be the field of rational functions in $x$over F_0.

We claim that the polynomial $t^2 - x$ in $F[t]$ is irreducible over $F$and that its roots are equal.

To prove irreducibility we must show that there is no rational function in $F_0(x)$whose square is x; this is the content of Problem 4.

To see that $t^2 - x$ has a multiple root, notice that its derivative(the derivative is with respect to t; for x, being in F, is considered as a constant) is $2t = 0$.

Of course, the analogous example works for any primecharacteristic.

Now that the possibility has been seen to be an actuality, it points out a sharp difference between the case of characteristic 0 and that of characteristic p.

The presence of irreducible polynomials with multiple roots in the latter case leads to many interesting, but at the same time complicating subtleties,

These require a more elaborate and sophisticated treatment which we prefer to avoid at this stage of the game.

Therefore, we make the flat assumption for the rest of this chapter that all fields occurring in the text material proper are fields of characteristic 0.

DEFINITION: The extension $K$of $F$is a *simple extension of* Fif $K = F(\alpha)$for some α in K.

In characteristic 0 (or in properly conditioned extensions in characteristic$p \neq 0$; see Problem 14) all finite extensions are realizable as simple extensions.This result is

THEOREM 2.2.1 *If F is of characteristic 0 and if a, b, are algebraic over F, then there exists an element $c \in F(a, b)$ such that $F(a, b) = F(c)$.*

Proof. Let $f(x)$and $g(x)$, of degrees m and n, be the irreducible polynomials over F satisfied by a and b, respectively.

Let K be an extension of F in which both $f(x)$and $g(x)$split completely. Since the characteristic of $F$is 0, all the roots of$f(x)$are distinct, as are all those of $g(x)$.

Let the roots of $f(x)$be $a = a_1, a_2, \dots, a_m$and those of $g(x), b = b_1, b_2, \dots, b_n$.

If $j \neq 1$, then $b_j \neq b_1 = b$, hence the equation $a_i + \lambda b_j = a_1 + \lambda b_1 = a + \lambda b$ has only one solution λ in K, namely,

$$\lambda = \frac{a_i - a}{b - b_j}$$

Since$F$ is of characteristic 0 it has an infinite number of elements, so we can find an element $\gamma \in F$such that $a_i + \lambda b_j \neq a + \gamma b$for all $i$and for$j \neq 1$.

Let $c = a + \gamma b$; our contention is that $F(c) = F(a, b)$.

Since,$c \in F(a, b)$, we certainly do have that $F(c) \subset F(a, b)$. We will now show that both a and b are in $F(c)$ from which it will follow that $F(a, b) \subset F(c)$.·

Now b satisfies the polynomial $g(x)$ over F, hence satisfies $g(x)$considered asa polynomial over $K = F(c)$.

Moreover, if $h(x) = f(c - \gamma x)$then $h(x) \in K[x]$ and $h(b) = f(c - \gamma b) = f(a) = 0$, since $a = c - \gamma b$.

Thus in some extension of K, $h(x)$and $g(x)$ have $x - b$ as a common factor.

We assert that $x - b$ is in fact their greatest common divisor.

For, if $b_j \neq b$ is another root of $g(x)$, then $h(b_j) = f(c - \gamma b_j) \neq 0$, since by our choice$\gamma$, $c - \gamma b_j$ *for*$j \neq 1$ avoids all roots a_i of $f(x)$.

Also, since $(x-b)^2 \nmid g(x)$,$(x-b)^2$cannot divide the greatest common divisor of $h(x)$and $g(x)$.

Thus$x - b$ is the greatest common divisor of $h(x)$and $g(x)$over some extension of K.

But then they have a nontrivial greatest common divisor over K, which must be a divisor of $x - b$.

Since the degree of $x - b$is 1, we see that the greatest common divisor of $g(x)$and $h(x)$in $K[x]$is exactly $x - b$.

Thus $x - b \in K[x]$, whence $b \in K;$ remembering that $K = F(c)$, we obtain that $b \in F(c)$.

Since, $a = c - \gamma b$, and since $b, c \in F(c)$, $\gamma \in F \subset F(c)$, we get that $a \in F(c)$, whence $F(a, b) \subset F(c)$. The two opposite containing relations combine to yield $F(a, b) = F(c)$.

A simple induction argument extends the result from 2 elements to anyfinite number, that is, if $\alpha_1, \dots, \alpha_n$are algebraic over F, then there is an element $c \in F(\alpha_1, \dots, \alpha_n)$such that $F(c) = F(\alpha_1, \dots, \alpha_n)$·

COROLLARY *Any finite extension of afield of characteristic* 0 *is a simple extension.*

UNIT – III

3.1 THE ELEMENTS OF GALOIS THEORY

Given a polynomial $p(x)$ in $F[x]$, the polynomial ring in x over F, we shall associate with $p(x)$ a group, called the *Galois group* of $p(x)$. There is a very close relationship between the roots of a polynomial and its Galois group; in fact, the Galois group will turn out to be a certain permutation group of the roots of the polynomial. We shall make a study of these ideas in this, and in the next section.

The means of introducing this group will be through the splitting field of $p(x)$ over F, the Galois group of $p(x)$ being defined as a certain group of automorphisms of this splitting field. This accounts for our concern, in so manyof the theorems to come, with the automorphisms of a field. A beautiful duality, expressed in the fundamental theorem of the Galois theory. (Theorem 3.1.6), exists between the subgroups of the Galois group and the subfields of the splitting field. From this we shall eventually derive a condition for the solvability by means of radicals of the roots of a polynomial interms of the algebraic structure of its Galois group. From this will follow the classical result of Abel that the general polynomial of degree 5 is not solvable by radicals. Along the way we shall also derive, as side results, theorems of great interest in their own right. One such will be the fundamental theoremon symmetric functions. Our approach to the subject is founded on the treatment given it by Artin.

Recall that we are assuming that all our fields are of characteristic 0, hence we can (and shall) make free use of Theorem 2.2.1 and its corollary.

By an *automorphism of the field K* we shall mean, as usual, a mapping σ of K onto itself such that $\sigma(a+b) = \sigma(a) + \sigma(b)$ and $\sigma(ab) = \sigma(a)\sigma(b)$ for all $a, b \in K$. Two automorphisms σ and τ of K are said to be distinct $\sigma(a) \neq \tau(a)$ for some element a in K.

THEOREM 3.2.1 *If K is a field and if $\sigma_1, \dots, \sigma_n$ are distinct automorphisms of K, then it is impossible to find elements $a_1, \dots, a_n$ not all 0, in K such that $a_1\sigma_1(u) + a_2\sigma_2(u) + \cdots + a_n\sigma_n(u) = 0$ for all $u \in K$.*

Proof. Suppose we could find a set of elements $a_1, \ldots, a_n$ in K, not all 0, such that $a_1\sigma_1(u) + a_2\sigma_2(u) + \cdots + a_n\sigma_n(u) = 0$ for all $u \in K$. Then we could find such a relation having as few nonzero terms as possible; on renumbering we can assume that this minimal relation is

$$a_1\sigma_1(u) + \cdots + a_m\sigma_m(u) = 0 \tag{1}$$

where $a_1, \ldots, a_m$ are all different from 0.

If m were equal to 1 then $a_1\sigma_1(u)$ for all $u \in K$, leading to $a_1 = 0$, contrary to assumption. Thus we may assume that $m > 1$.

Since the automorphisms are distinct there is an element $c \in K$ such that $\sigma_1(c) \neq \sigma_m(c)$.

Since $cu \in K$ for all $u \in K$, relation (1) must also hold for cu, that is, $a_1\sigma_1(cu) + a_2\sigma_2(cu) + \cdots + a_m\sigma_m(cu) = 0$ for all $u \in K$.

Using the hypothesis that the σ's are automorphisms of K, this relation becomes

$$a_1\sigma_1(c)\sigma_1(u) + a_2\sigma_2(c)\sigma_2(u) + \cdots + a_n\sigma_m(c)\sigma_n(u) = 0 \tag{2}$$

Multiplying relation (1) by $\sigma_1(c)$ and subtracting the result from (2) yields

$$a_2\big(\sigma_2(c) - \sigma_1(c)\big)\sigma_2(u) + \cdots + a_n\big(\sigma_m(c) - \sigma_1(c)\big)\sigma_n(u) = 0 \tag{3}$$

If we put $b_i = a_i\big(\sigma_i(c) - \sigma_1(c)\big)$ for $i = 2, \ldots, m$, then the b_i are in K, $b_m = a_m\big(\sigma_m(c) - \sigma_1(c)\big) \neq 0$, since $a_m \neq 0$, and $\sigma_m(c) - \sigma_1(c) \neq 0$ yet $b_2\sigma_2(u) + \cdots + b_m\sigma_m(u) = 0$ for all $u \in K$.

This produces a shorter relation, contrary to the choice made; thus the theorem is proved.

DEFINITION If G is a group of automorphisms of K, then the *fixed field* of G is the set of all elements $a \in K$ such that $\sigma(a) = a$ for all $\sigma \in G$.

Note that this definition makes perfectly good sense even if $G$is not agroup but is merely a set of automorphisms of K.

However, the fixed field of a set of automorphisms and that of the group of automorphisms generated by this set (in the group of all automorphisms of K) are equal (Problem 1), hence we lose nothing by defining the concept just for groups of automorphisms. Besides, we shall only be interested in the fixed fields of groups of automorphisms.

Having called the set, in the definition above, the fixed *field* of G, it would be nice if this terminology were accurate. That it is we see in the next Lemma.

LEMMA 3.1.1 *The fixed field of G is a subfield of K.*

Proof: Let a, b be in the fixed field of G.

Thus for all $\sigma \in G$, $\sigma(a) = a$and$\sigma(b) = b$.

But then $(\sigma(a \pm b) = (\sigma(a) \pm (\sigma(b) = a \pm b$ and $(\sigma(ab) = \sigma(a)\sigma(b) = ab;$ hence $a \pm b$ and ab are again in the fixed field of G.

If $b \neq 0$, then $\sigma(b^{-1}) = \sigma(b)^{-1} = b^{-1}$, hence b^{-1} also falls in the fixed field of G.

Thus we have verified that the fixed field of G is indeed a subfield of K.

We shall be concerned with the automorphisms of a field which behave in a prescribed manner on a given subfield.

DEFINITION Let K be a field and let Fbe a subfield of K. Then the *group of automorphisms of K relative to F,* written $G(K, F)$, is the set of *all automorphisms of K* leaving every element of F fixed; that is, the automorphism σ of K is in $G\ (K, F)$if and only if $\sigma(\alpha) = \alpha$ for every $\alpha \in F$.

LEMMA 3.1.2 *$G(K, F)$ is a subgroup of the group of all automorphisms of K.*

We leave the proof of this lemma to the reader. One remark: K contains the field of rational numbers F_0, since K is of characteristic 0, and it is easy to see that the fixed field of any group of automorphisms of K, being a field, must contain F_0.

Hence, every rational number is left fixed by every automorphismof K.

We pause to examine a few examples of the concepts just introduced.

Example 3.1.1 Let K be the field of complex numbers and let F be the field of real numbers.

We compute $G(K, F)$.

If σ is any automorphism of$K$since$i^2 = -1, \sigma(i)^2 = \sigma(i^2) = \sigma(-1) = -1$, hence $\sigma(i) = \pm i$.

If, in addition, σ leaves every real number fixed, then for any $a + bi$ where a, b are real, $(\sigma(a + bi) = \sigma(a) + \sigma(b)\sigma(i) = a \pm bi$. Each of these possibilities, namely the mapping $\sigma_1(a + bi) = a + bi$and $\sigma_2(a + bi) = a - bi$; defines an automorphism of K, σ_1 being the identity automorphism and σ_2 complex-conjugation.

Thus $G\ (K, F)$is a group of order 2.

What is the fixed field of $G\ (K, F)$? It certainly must contain F, but does it contain more? If $a + bi$is in the fixed field of $G(K, F)$ then $a + bi = \sigma_2(a + bi) = a - bi$, whence $b = 0$ and $a = a + bi \in F$. In this case we see that the fixed field of $G\ (K, F)$is precisely F itself.

Example 3.1.2 Let F_0be the field of rational numbers and let $K = F_0(\sqrt[3]{2})$ where $\sqrt[3]{2}$ is the real cube root of 2.

Every element in $K$is of the form $\alpha_0 + \alpha_1\sqrt[3]{2} + \alpha_2(\sqrt[3]{2})^2$, where $\alpha_0, \alpha_1, \alpha_2$are rational numbers.

If σ is an automorphism of K,then$\sigma(\sqrt[3]{2})^3 = \sigma\left((\sqrt[3]{2})^3\right) = \sigma(2) = 2$, hence$\sigma(\sqrt[3]{2})$must also be a cube root of 2 lying in K.

However, there is only one real cube root of 2, and since $K$is a subfield of the real field, we musthave that $\sigma(\sqrt[3]{2}) = \sqrt[3]{2}$. But then$\sigma\left(\alpha_0 + \alpha_1\sqrt[3]{2} + \alpha_2(\sqrt[3]{2})^2\right) = \alpha_0 + \alpha_1\sqrt[3]{2} + \alpha_2(\sqrt[3]{2})^2$, that is, $\sigma$is the identity automorphism of K. We thus see that $G(K, F_0)$consists only of the

identity map, and in this case the*fixed field of* $G(K, F_0)$ *is not* F_0 *but is, in fact, larger, being all of* K.

Example 3.1.3 Let F_0be the field of rational numbers and let $\omega = e^{2\pi i/5}$; thus $\omega^5 = 1$ and ω satisfies the polynomial $x^4 + x^3 + x^2 + x + 1$ over F_0.

By the Eisenstein criterion one can show that $x^4 + x^3 + x^2 + x + 1$ is irreducible over F_0(see Problem 3).

Thus $K = F_0(\omega)$is of degree4 over $F_0$and every element in K is of the form $\alpha_0 + \alpha_1\omega + \alpha_2\omega^2 + \alpha_3\omega^3$ where all of $\alpha_0, \alpha_1, \alpha_2$ and α_3 are in F_0.

Now, for any automorphism σ of K, $\sigma(\omega) \neq 1$, since $\sigma(1) = 1$, and $\sigma(\omega)^5 = \sigma(\omega^5) = \sigma(1) = 1$,whence $\sigma(\omega)$ is also a 5th root of unity.

In consequence, $\sigma(\omega)$ can onlybe one of $\omega, \omega^2, \omega^3$ or ω^4.

We claim that each of these possibilitiesactually occurs, for let us define the four mappings $\sigma_1, \sigma_2, \sigma_3$ and σ_4 by$\sigma_i(\alpha_0 + \alpha_1\omega + \alpha_2\omega^2 + \alpha_3\omega^3) = \alpha_0 + \alpha_1\omega^i + \alpha_2(\omega^i)^2 + \alpha_3(\omega^i)^3$ for $i = 1, 2, 3,$and 4.

Each of these defines an automorphism of K(Problem4).

Therefore, since $\sigma \in G(K, F_0)$is completely determined by $\sigma(\omega)$, $G(K, F_0)$ is a group of order 4, with σ_1 as its unit element.

In light of $\sigma_2^2 = \sigma_4, \sigma_2^3 = \sigma_3, \sigma_2^4 = \sigma_1$, $G(K, F_0)$ is a cyclic group of order 4.

One can easily prove that the fixed field of $G(K, F_0)$is F_0itself (Problem 5).

The subgroup $A = \{\sigma_1, \sigma_4\}$of $G(K, F_0)$ has as its fixed field the set of all elements $\alpha_0 + \alpha_2(\omega^2 + \omega^3)$, which is an extension of $F_0$of degree 2.

The examples, although illustrative, are still too special, for note that in each of them $G\ (K, F)$turned out to be a cyclic group. This is highlyatypical for, in general, $G\ (K, F)$need not even be abelian (see Theorem 3.1.3).

However, despite their speciality, they do bring certain importantthings to light.

For one thing they show that we must study the effect ofthe automorphisms on the roots of polynomials and, for another, they point out that *F need not* be equal to all of the fixed field of $G\ (K, F)$.

The cases in which this does happen are highly desirable ones and are situations with which we shall soon spend much time and effort.

We now compute an important bound on the size of $G\ (K, F)$.

THEOREM 3.1.2 *If K is a finite extension of F, then $G(K, F)$ is a finite group and its order, $o(G(K, F))$ satisfies $o\big(G(K, F)\big) \leq [K: F]$.*

Proof. Let $[K: F] = n$ and suppose that $u_1, \ldots, u_n$is a basis of Kover$F$. Suppose we can find $n + 1$ distinct automorphisms $\sigma_1, \sigma_2, \ldots, \sigma_{n+1}$in $G(K, F)$.

The system of $n$homogeneouslinear equations in the $n + 1$unknowns$x_1, \ldots, x_{n+1}$:

$$\sigma_1(u_1)x_1 + \sigma_2(u_1)x_2 + \cdots + \sigma_{n+1}(u_1)x_{n+1} = 0$$

$$\vdots$$

$$\sigma_1(u_i)x_1 + \sigma_2(u_i)x_2 + \cdots + \sigma_{n+1}(u_i)x_{n+1} = 0$$

$$\vdots$$

$$\sigma_1(u_n)x_1 + \sigma_2(u_n)x_2 + \cdots + \sigma_{n+1}(u_n)x_{n+1} = 0$$

has a nontrivial solution (not all 0) $x_1 = a_1, \ldots, x_{n+1} = a_{n+1}$in K. Thus,

$$a_1\sigma_1(u_i) + a_2\sigma_2(u_i) + \cdots + a_n\sigma_{n+1}(u_i) = 0 \qquad (1)$$

for$i = 1, 2, \ldots, n$.

Since every element in F is left fixed by each σ_i and since an arbitraryelement t in $K$is of the form $t = \alpha_1 u_1 + \cdots + \alpha_n u_n$with $\alpha_1, \ldots, \alpha_n$in F, then from the system of equations (1) we get $a_1\sigma_1(t) + \cdots + a_{n+1}\sigma_{n+1}(t) = 0$ for all $t \in K$.

But this contradicts the result of Theorem 3.1.1. Thus Theorem 3.1.2 has been proved.

Theorem 3.1.2 is of central importance in the Galois theory. However, aside from its key role there, it serves us well in proving a classic result concerned with symmetric rational functions.

This result on symmetric functions in its turn will play an important part in the Galois theory.,

First a few remarks on the field of rational functions in n-variables over a field F.

We defined the ring of polynomials in the n-variab1es $x_1, \ldots, x_n$over F and from this defined the field of rational functions in $x_1, \ldots, x_n, F(x_1, \ldots, x_n)$, over F as the ring of all quotients of such polynomials..

Let S_n be the symmetric group of degree $n$considered to be acting on theset $[1, 2, \ldots, n]$; for $\sigma \in S_n$and $i$an integer with$1 \leq i \leq n$, let $\sigma(i)$bethe image of i under u.

We can make $S_n$act on $F(x_1, \ldots, x_n)$ in the following natural way: for $\sigma \in S_n$and $(x_1, \ldots, x_n) \in F(x_1, \ldots, x_n)$, define the mapping which takes $r(x_1, \ldots, x_n)$ onto $r(x_{\sigma(1)}, \ldots, x_{\sigma(n)})$.

We shall write this mapping of $F(x_1, \ldots, x_n)$ onto itself also as σ.

It is obvious that these mappings define automorphisms of $F(x_1, \ldots, x_n)$·

What is the fixed field of $F(x_1, \ldots, x_n)$with respect to S_n? It consists of all rational functions $r(x_1, \ldots, x_n)$such that $r(x_1, \ldots, x_n) = r(x_{\sigma(1)}, \ldots, x_{\sigma(n)})$ for all$\sigma \in S_n$.

But these are precisely those elements in $F(x_1, \ldots, x_n)$which are known as the *symmetric rational functions.*

Being the fixed field of S_n they form a subfield of $F(x_1, \dots, x_n)$, called the field of symmetric rational functions which we shall denote by S. We shall be concerned with three questions:

1. What is $[F(x_1, \dots, x_n) : S]$?
2. What is $G(F(x_1, \dots, x_n), S)$?
3. Can we describe S in terms of some particularly easy extension of F?

We shall answer these three questions simultaneously.

We can explicitly produce in S some particularly simple functions constructed from $x_1, \dots, x_n$ known as the *elementary symmetric functions* in $x_1, \dots, x_n$. These are defined as follows:

$$a = x_1 + x_2 + \cdots + x_n = \sum_{i=1}^{n} x_i$$

$$a_2 = \sum_{i<j} x_i x_j$$

$$a_3 = \sum_{i<j<k} x_i x_j x_k$$

$$\vdots$$

$$a_n = x_1 x_2 \dots x_n.$$

That these are symmetric functions is left as an exercise. For $n = 2, 3$ and 4 we write them out explicitly below.

$$n = 2$$

$$a_1 = x_1 + x_2$$

$$a_2 = x_1 x_2$$

$$n = 3$$

$$a_1 = x_1 + x_2 + x_3$$

$$a_2 = x_1x_2 + x_1x_3 + x_2x_3$$

$$a_3 = x_1x_2x_3$$

$$n = 4$$

$$a_1 = x_1 + x_2 + x_3 + x_4$$

$$a_2 = x_1x_2 + x_1x_3 + x_1x_4 + x_2x_3 + x_2x_4 + x_3x_4$$

$$a_3 = x_1x_2x_3 + x_1x_2x_4 + x_1x_3x_4 + x_2x_3x_4$$

$$a_4 = x_1x_2x_3x_4.$$

Note that when $n = 2, x_1$ and $x_2$are the roots of the polynomial$t^2 - a_1t + a_2$, that when $n = 3, x_1, x_2$ and x_3 are roots of $t^3 - a_1t^2 + a_2t - a_3$ and that when $n = 3, x_1, x_2, x_3$ and x_4 are all roots of $t^4 - a_1t^3 + a_2t^2 - a_3t + a_4$.

Since $a_1, \dots, a_n$are all in S, the field $F(a_1, \dots, a_n)$obtained by adjoining$a_1, \dots, a_n$to Fmust lie in S. Our objective is now twofold, namely, to prove

1. $[F(x_1, \dots, x_n): S] = n!$
2. $S = F(a_1, \dots, a_n)$

Since the group $S_n$is a group of automorphisms of $F(x_1, \dots, x_n)$ leaving S fixed, $S_n \subset G\big(F(x_1, \dots, x_n)\big)$.

Thus, by Theorem 3.1.2, $[F(x_1, \dots, x_n): S] \geq o\big(G(F(x_n, \dots, x_n), S)\big) \geq o(S_n) = n!$.

If we could show that$[F(x_1, \dots, x_n): F(a_1, \dots, a_n)] \leq n!$, well then, since $F(a_1, \dots, a_n)$is a subfield of S, we would have $n! \geq [F(x_1, \dots, x_n): F(a_1, \dots, a_n)] = [F(x_1, \dots, x_n): S][S: F(a_1, \dots, a_n)] \geq n!$.

But then we would get that$[F(x_1, \dots, x_n): S] = n!$, $[S: F(a_1, \dots, a_n)] = 1$ and so $S = F(a_1, \dots, a_n)$, finally, $S_n = G(F(x_1, \dots, x_n), S)$ (this latter from the second senofthis paragraph). These are precisely the conclusions we seek.

Thus we merely must prove that $[F(x_1, \dots, x_n): F(a_1, \dots, a_n)] \leq n!$.

To see how this settles the whole affair, note that the polynomial

$$p(t) = t^n - a_1 t^{n-1} + a_2 t^{n-2} + \cdots + (-1)^n a_n$$

which has coefficients in $F(a_1, \dots, a_n)$,factors over $F(x_1, \dots, x_n)$as $p(t) = (t - x_1)(t - x_2) \dots (t - x_n)$ (This is in fact the origin of the elementary symmetric functions.)

Thus $p(t)$, of degree n over $F(a_1, \dots, a_n)$, splits as a product of linear factors over $F(x_1, \dots, x_n)$.

It cannot split over a proper subfield of $F(x_1, \dots, x_n)$ which contains $F(a_1, \dots, a_n)$ for this subfield would then have to contain both $F$and each of the roots of $p(t)$, namely, $x_1, x_2, \dots, x_n$; but then this subfield would be all of $F(x_1, \dots, x_n)$.

Thus we see that $F(x_1, \dots, x_n)$ *isthe splitting field of the polynomial* $p(t) = t^n - a_1 t^{n-1} + a_2 t^{n-2} + \cdots + (-1)^n a_n$*over* $F(a_1, \dots, a_n)$.Since $p(t)$is of degree n, by Theorem we get$[F(x_1, \dots, x_n): F(a_1, \dots, a_n)] \leq n!$. Thus all our claims are established summarize the whole discussion in the basic and important result

THEOREM 3.1.3 *Let F he a field and let* $F(x_1, \dots, x_n)$ *be the field of rational functions in* $x_1, \dots, x_n$ *over* F. *Suppose that S is the field of symmetric rational functions; then*

1. $[F(x_1, \dots, x_n): S] = n!$
2. $G(F(x_1, \dots, x_n), S) = S_n$, *the symmetric group of degree n.*
3. *If* $a_1, \dots, a_n$ *are the elementary symmetric functions in* $x_1, \dots, x_n$ *then* $S = F(a_1, a_2, \dots, a_n)$.
4. $F(x_1, \dots, x_n)$ *is the splitting field over* $F(a_1, \dots, a_n) = S$ *of the polynomial* $t^n - a_1 t^{n-1} + a_2 t^{n-2} + \cdots + (-1)^n a_n$.

We mentioned earlier that given any integer n it is possible to construct a field and a polynomial of degree $n$over this field whose splitting field is ofmaximal possible degree, $n!$, over this field.

Theorem 3.1.3 explicitly provides us with such an example for if we put $S = F(a_1, a_2, \ldots, a_n)$, the rational function field in n variables $a_1, \ldots, a_n$and consider the splittingof the polynomial $t^n - a_1 t^{n-1} + a_2 t^{n-2} + \cdots + (-1)^n a_n$over$S$ then it is of degree $n!$ over S.

Part 3 of Theorem 3.1.3 is a very classical theorem. *It asserts that a symmetric rational function in n variables is a rational function in the elementary symmetric functions of these variables.*

This result can even be sharpened to: A symmetric polynomial in n variables is a *polynomial* in their elementary symmetric functions (see Problem 7). This result is known as the *theorem on symmetric polynomials.*

In the examples we discussed of groups of automorphisms of fields and of fixed fields under such groups, we saw that it might very well happen that F is actually smaller than the whole fixed field of $G(K, F)$.

Certainly F is always contained in this field but need not fill it out. Thus to impose the condition on an extension K of F that F be precisely the fixed field of $G(K, F)$ is a genuine limitation on the type of extension of F that we are considering. It is in this kind of extension that we shall be most interested.

DEFINITION $K$is a *normal extension of* F if K is a finite extension of F such that F is the fixed field of $G(K, F)$.

Another way of saying the same thing: If K is a normal extension of F, then every element in K which is outside F is moved by some element in $G\ (K, F)$.

In the examples discussed, Examples 3.1.1 and 3.1.3 were normal extensions whereas Example 3.1.2 was not.

An immediate consequence of the assumption of normality is that it allows us to calculate with great accuracy the size of the fixed field of any subgroup of $G\ (K, F)$and, in particular, to sharpen Theorem 3.1.2 from an inequality to an equality.

THEOREM 3.1.4 *Let K be a normal extension of F and let H be a subgroup of $G\ (K, F)$; let $K_H = \{x \in K | \sigma(x) = x\ for\ all\ \sigma \in H\}$ be the fixed field of H.Then*

1. $[K: K_H] = o(H)$.
2. $H = G(K, K_H)$.

(In particular, when $H = G(K, F), [K: F] = o(G(K, F))$.)

Proof. Since very element in H leaves K_H elementwise fixed, certainly $H \subset G(K, K_H)$.

By Theorem 3.1.2 we know that $[K: K_H) \geq o(G(K, K_H))$; and since $o\big(G(K, K_H)\big) \geq o(H)$ we have the inequalities $[K: K_H] \geq o\big(G(K, K_H)\big) \geq o(H)$. If we could show that $[K: K_H] = o(H)$, it would immediately follow that $o(H) = o(G(K, K_H))$ and as a subgroup of $G\ (K, K_H)$ having order that of $G\ (K, K_H)$, we would obtain that $H = G(K, K_H)$. So we must merely show that $[K: K_H] = o(H)$ to prove everything.

By Theorem 2.2.1 there exists an $a \in K$such that $K = K_H(a)$; this $a$must therefore satisfy an irreducible polynomial over $K_H$of degree $m = [K: K_H]$and no nontrivial polynomial of lower degree (Theorem 1.1.3).

Let the elements of H be $\sigma_1, \sigma_2, \dots, \sigma_h$, where σ_1 is the identity of $G(K, F)$ and where $h = o(H)$.

Consider the elementary symmetric functions of $a = \sigma_1(a), \sigma_2(a), \dots, \sigma_h(a)$, namely,

$$\alpha_1 = \sigma_1(a), \sigma_2(a), \dots, \sigma_h(a) = \sum_{i=1}^{h} \sigma_i(a)$$

$$\alpha_2 = \sum_{i<j} \sigma_i(a)\sigma_j(a)$$

$$\vdots$$

$$\alpha_h = \sigma_1(a)\sigma_2(a) \dots \sigma_h(a)$$

Each α_i is invariant under every$\sigma \in H$. (Prove!) Thus, by the definition of K_H, $\alpha_1, \alpha_2, \dots, \alpha_h$ are all elements of K_H. However, a (as well as $\sigma_2(a), \dots, \sigma_h(a)$) is a root of the polynomial $p(x) = \big(x - \sigma_1(a)\big)\big(x - \sigma_2(a)\big) \dots \big(x - \sigma_h(a)\big)$

$$= x^h - \alpha_1 x^{h-1} + \alpha_2 x^{h-2} + \cdots + (-1)^h \alpha_h$$

having coefficients in K_H. By the nature of a, this forces $h \geq m = [K: K_H]$, whence $o(H) \geq [K: K_H]$.

Since we already know that $o(H) \leq [K: K_H]$ we obtain $o(H) = [K: K_H]$, the desired conclusion.

When $H = G(K, F)$, *by the normality of* K *over* F, $K_H = F$; consequently for this particular case we read off the result $[K: F] = o(G(K, F))$

We are rapidly nearing the central theorem of the Galois theory. What we still lack is the relationship between splitting fields and normal extensions.

THEOREM 3.1.5 *K is a normal extension of F if and only if K is the splitting field of some polynomial over F.*

Proof. In one direction the proof will be highly reminiscent of that of Theorem 3.1.4.

Suppose that $K$is a normal extension of$F$; by Theorem 2.2.1, $K = F(a)$.

Consider the polynomial $p(x) = \big(x - \sigma_1(a)\big)\big(x - \sigma_2(a)\big) \dots \big(x - \sigma_n(a)\big)$ over K, where $\sigma_1, \sigma_2, \dots, \sigma_n$ are all the elements of $G(K, F)$.

Expanding $P(x)$we see that $p(x) = x^n - \alpha_1 x^{n-1} + \alpha_2 x^{n-2} + \cdots + (-1)^n \alpha_n$ where $\alpha_1, \dots, \alpha_n$ are the elementary symmetric functions in $a = \sigma_1(a), \sigma_2(a), \dots, \sigma_n(a)$,

But then $\alpha_1, \ldots, \alpha_n$ are each invariant with respect to every $\sigma \in G(K, F)$, whence by the normality of K over F, must all be in F.

Therefore, K splits the polynomial $p(x) \in F[x]$ into a product of linear factors.

Since a is a root of $p(x)$ and since a generates K over F, a can be no proper subfield of K which contains F.

Thus K is the splitting field of $p(x)$ over F.

Now for the other direction; it is a little more complicated.

LEMMA 3.1.3 *Let K be the splitting field of $f(x)$ in $F[x]$ and let $p(x)$ be an irreducible factor of $f(x)$ in $F[x]$. If the roots of $p(x)$ are $\alpha_1, \ldots, \alpha_n$, then for each i there exists an automorphism σ_i in $G(K, F)$ such that $\sigma_i(\alpha_1) = \alpha_i$.*

Proof . Since every root of $p(x)$ is a root of $f(x)$, it must lie in K.

Let α_1, α_i be any two roots of $p(x)$. By Theorem 2.1.3, there is an isomorphism τ of $F_1 = F(\alpha_1)$ onto $F_1' = F(\alpha_i)$ taking α_1 onto α_i and leaving every element of F fixed.

Now K is the splitting field of $f(x)$considered as a polynomial over F_1 likewise, K is the splitting field of $f(x)$considered as a polynomial over F_1'. By Theorem 2.1.4 there is an isomorphism σ_i of K onto K(thus an automorphism of K) coinciding with τ on F_1.

But then $\sigma_i(\alpha_1) = \tau(\alpha_1) = \alpha_i$ and σ_i leaves every element of F fixed. This is, of course, exactly what Lemma 3.1.3 claims.

We return to the completion of the proof of Theorem 3.1.5.

Assume that K is the splitting field of the polynomial $f(x)$ in $F[x]$.

We want to show that K is normal over F.

We proceed by induction on $[K:F]$, assuming that for any pair of fields K_1, F_1 of degree less than $[K:F]$ that wheneverK_1 is the splitting field over F_1 of a polynomial in $F_1[x]$, then K_1 is normalover F_1.

If$f(x) \in F[x]$ splits into linear factors over F, then $K = F$, which is certainly a normal extension of F.

So, assume that $f(x)$ has an irreducible factor $p(x) \in F[x]$ of degree $r > 1$.

The r *distinct* roots $\alpha_1, \alpha_2, \dots, \alpha_r$ of $p(x)$ all lie in K and K is the splitting field of $f(x)$considered as a polynomial over $F(\alpha_1)$. Since

$$[K:F(\alpha_1)] = \frac{[K:F]}{[F(\alpha_1):F]} = \frac{n}{r} < n,$$

by our induction hypothesis K is a normal extension of $F(\alpha_1)$.

Let $\theta \in K$ be left fixed by every automorphism$\sigma \in (G(K,F)$; we would like to show that θ is in F. Now, any automorphism in $G(K,F(\alpha_1))$ certainly leaves F fixed, hence leaves θ fixed; by the normality of K over $F(\alpha_1)$, this implies that θ is in $F(\alpha_1)$. Thus

$$\theta = \lambda_0 + \lambda_1\alpha_1 + \lambda_2\alpha_1^2 + \cdots + \lambda_{r-1}\alpha_1^{r-1} \text{ where } \lambda_0, \dots, \lambda_{r-1} \in F \tag{1}$$

By Lemma 3.1.3 there is an automorphism$\sigma_i$of K, $\sigma_i \in G(K,F)$, such that $\sigma_i(\alpha_1) = \alpha_i$; since this σ_i leaves θ and each λ_j fixed, applying it to (1) we obtain

$$\theta = \lambda_0 + \lambda_1\alpha_i + \lambda_2\alpha_i^2 + \cdots + \lambda_{r-1}\alpha_i^{r-1} \text{ for } i = 1,2, \dots, r \tag{2}$$

Thus the polynomial

$$q(x) = \lambda_{r-1}x^{r-1} + \lambda_{r-2}x^{r-2} + \cdots + \lambda_1 + (\lambda_0 - \theta)$$

in $K[x]$, of degree at most $r-1$, has the r distinct roots $\alpha_1, \alpha_2 \dots, \alpha_r$.

This can only happen if all its coefficients are 0; in particular, $\lambda_0 - \theta = 0$whence $\theta = \lambda_0$ so is in F. This completes the induction and proves that K is a normal extension of F. Theorem 3.1.5 is now completely proved.

DEFINITION Let $f(x)$be a polynomial in $F[x]$and let K be its splitting field over F. The *Galois group of* $f(x)$ is the group $G(K,F)$ of all the automorphisms of K, leaving every element of$F$fixed.

Note that the Galois group of $f(x)$can be considered as a group of permutations of its roots, for if $\alpha$is a root of $f(x)$ and if $\sigma \in G(K,F)$, then $\sigma(\alpha)$ is also a root of $f(x)$.

We now come to the result known as the *fundamental theorem of Galois theory.* It sets up a one-to-one correspondence between the subfields of the splitting field of $f(x)$ and the subgroups of its Galois group. Moreover, it gives a criterion that a subfield .of a normal extension itself be a normal extension of F. This fundamental theorem will be used in the next section to derive conditions for the solvability by radicals of the roots of a polynomial.

THEOREM 3.1.6 *Let $f(x)$ be a polynomial in $F[x]$, K its splitting field over$F$, and $G(K,F)$ its Galois group. For any subfield T of K which contains F let $G(K,T) = \{\sigma \in G(K,F) \,|\sigma(t) = t \; for \; every \; t \in T\}$ and for any subgroup H of $G\,(K,F)$ let $K_H = \{x \in K \,|\sigma(x) = x \; for \; every \; \sigma \in H\}$. Then the association of T with $G\,(K,T)$ sets up a one-to-one correspondence of the set of sub fields of K which contain F onto the set of subgroups of $G\,(K,F)$ such that*

1. $T = K_{G(K,T)}$.
2. $H = G(K,K_H)$.
3. $[K:T] = o\big(G(K,T)\big), [T:F] = index \; of \; G(K,T) \; in \; G(K,F)$.
4. *$T$is a normal extension of F if and only if $G\,(K,T)$ is a normal subgroup of$G(K,F)$.*
5. *When T is a normal extension of F, then $G(T,F)$ is isomorphic to$G(K,F)|G(K,T)$.*

Proof. Since $K$is the splitting field of $f(x)$over F it is also the splittingfield of $f(x)$over any subfield Twhich contains F,

Therefore, by Theorem 3.1.5, K is a normal extension of T.

Thus, by the definition of normality, T is the fixed field of $G(K,T)$, that is, $T = K_{G(K,T)}$ proving part 1.

Since K is a normal extension of F, by Theorem 3.1.4, given a subgroup H of $G(K,F)$, then $H = G(K,K_H)$, which is the assertion of part 2. Moreover, this shows that any subgroup of $G(K,F)$ arises in the form $G(K,T)$, whence the association of T with $G(K,T)$ maps the set of all subfields of Kcontaining F *onto* the set of all subgroups of $G(K,F)$. That it is one-to-one is clear, for, if $G(K,T_1) = G(K,T_2)$ then, by part 1, $T_1 = K_{G(K,T_1)}K_{G(K,T_2)} = T_2$.

Since K is normal over T, again using Theorem 3.1.4, $[K:T] = o(G(K,T))$; but then we have $o(G(K,F)) = [K:F] = [K:T][T:F] = o(G(K,T))[T:F]$, whence

$$[T:F] = \frac{o(G(K,F))}{o(G(K,T))} = index\ of\ G(K,T)$$

in $G\ (K,F)$. This is part 3.

The only parts which remain to be proved are those which pertain to normality.

We first make the following observation. T is a normal extension of F if and only if for every $\sigma \in G(K,F), \sigma(T) \subset T$. Why? We know by Theorem 2.2.1 that $T = F(a)$; thus if $\sigma(T) \subset T$, then $\sigma(a) \in T$ for all $\sigma \in G(K,F)$.

But, as we saw in the proof of Theorem 3.1.5, this implies that T is the splitting field of

$$p(x) = \prod_{\sigma \in G(K,F)} (x - \sigma(a))$$

which has coefficients in F.

As a splitting field, T, by Theorem 3.1.5, is a normal extension of F. Conversely, if T is a normal extension of F, then $T = F(a)$, where the minimal polynomial of a, $p(x)$, over F has all its roots in T(Theorem 3.1.5). However, for any $\sigma \in G(K,F)$, $\sigma(a)$ is also a root of $p(x)$,

whence $\sigma(a)$ must be in T. Since T is generated by a over F, we get that $\sigma(T) \subset T$ for every $\sigma \in G(K,F)$.

Thus $T$is a normal extension of F if and only if for any $\sigma \in G(K,F)$,$\tau \in G(K,T)$and $t \in T$, $\sigma(t) \in T$ and so $\tau\big(\sigma(t)\big) = \sigma(t)$; that is, if and only if $\sigma^{-1}\tau\sigma(t) = t$.

But this says that T is normal over F if and only if $\sigma^{-1}G(K,T)\sigma \subset G(K,T)$ for every $\sigma \in G(K,F)$.

This last condition being precisely that which defines $G(K,T)$as a normal subgroup of$G(K,F)$, we see that part 4 is proved.

Finally, if T is normal over F, given $\sigma \in G(K,F)$, since $\sigma(T) \subset T, \sigma$ induces an automorphism $\sigma_*$of Tdefined by $\sigma_*(t) = \sigma(t)$ for every$t \in T$. Because σ_* leaves every element of F fixed, σ_* must be in $G(T,F)$.

Also, as is evident, for any $\sigma, \Psi \in G(K,F)$, $(\sigma\Psi)_* = \sigma_*\Psi_*$whence the mapping of $G(K,F)$into $G(T,F)$ defined by $\sigma \to \sigma_*$ is a homomorphism of $G(K,F)$into $G(T,F)$. What is the kernel of this homomorphism?

It consists of all elements σ in $G\ (K,F)$such that σ_* is the identity map on$T$.

That is, the kernel is the set of all $\sigma \in G(K,F)$such that $t = \sigma_*(t) = \sigma(t)$; by the very definition, we get that the kernel is exactly $G\ (K,T)$.

The image of $G(K,F)$in $G(T,F)$, by Theorem it is isomorphic to $G(K,F)/G(K,T)$, whose order is $o(G(K,F))/o(G(K,T)) = [T\colon F]$ (bypart 3) = $o(G(T,F))$(by Theorem 3.1.4).

Thus the image of $G(K,F)$in $G\ (T,F)$ is all of $G\ (T,F)$ and so we have $G\ (T,F)$ isomorphic to $G(K,F)/G(K,T)$. This finishes the proof of part 5 and thereby completes the proof of Theorem 3.1.6.

UNIT – IV

4.1 FINITE FIELDS

Before we can enter into a discussion of Wedderburn's theorem and finite division rings, it is essential that we investigate the nature of fields having only a finite number of elements. Such fields are called *finite fields.* Finite fields do exist, for the ring $J_p$of integers modulo any prime p, provides us with an example of such. In this section we shall determine all possible finite fields and many of the important properties which they possess.

LEMMA 4.1 .1 *Let F be a finite field with q elements and suppose that $F \subset K$where K is also a finite field. Then K has q^n elements where $n = [K:F]$.*

Proof. $K$is a vector space over $F$and since $K$is finite it is certainly finite dimensional as a vector space over F.

Suppose that $[K:F] = n$; then K has a basis of n elements over F.

Let such a basis be $v_1, v_2, \ldots, v_n$.

Then every element in K has a unique representation in the form $\alpha_1 v_1 + \alpha_2 v_2 + \cdots + \alpha_n v_n$where $\alpha_1, \alpha_2, \ldots, \alpha_n$are all in F.

Thus the number of elements in K is the number of $\alpha_1 v_1 + \alpha_2 v_2 + \cdots + \alpha_n v_n$ as the $\alpha_1, \alpha_2, \ldots, \alpha_n$ range over F.

Since each coefficient can have $q$values Kmustclearly have q^nelements.

COROLLARY 1 *Let F be a finite field; then F has p^m elements where the prime number p is the characteristic of F.*

Proof. Since F has a finite number of elements, by Corollary of Theorem, $f\ 1 = 0$ where f is the number of elements in F.

Thus F has characteristic p for some prime number p.

Therefore F contains a field F_0 isomorphic to J_p. Since F_0 has p elements, F has p^m elements where $m = [F: F_0]$, by Lemma 4.1.1.

COROLLARY 2 *If the finite field F has p^m elements then every $a \in F$ satisfies $a^{p^m} = a$.*

Proof. If $a = 0$ the assertion of the corollary is trivially true.

On the other hand, the nonzero elements of F form a group under multiplication of order $p^m - 1$ thus by Corollary to Theorem, $a^{p^m} - 1$ for all $a \neq 0$ in F.

Multiplying this relation by $a$we obtain that $a^{p^m} = a$.

LEMMA 4.1.2 *If the finite field F has p^m elements then the polynomial $x^{p^m} - x$ in $F[x]$ factors in $F[x]$ as $x^{p^m} - x = \prod_{\lambda \in F}(x - \lambda)$.*

Proof. By Lemma 2.1.2 the polynomial $x^{p^m} - x$ has at most p^{p^m} roots in F.

However, by Corollary 2 to Lemma 4.1.1 we know p^msuch roots, namely all the elements of F. By the corollary to Lemma 2.1.1 we can conclude that $x^{p^m} - x = \prod_{\lambda \in F}(x - \lambda)$.

COROLLARY *If the field F has p^m elements then F is the splitting field of the polynomial $x^{p^m} - x$.*

Proof. By Lemma 4.1.2, $x^{p^m} - x$ certainly splits in F.

However, it cannot split in any smaller field for that field would have to have all the roots of this polynomial and so would have to have at least p^melements. Thus F is the splitting field of $x^{p^m} - x$.

As we have seen in Unit 2 (Theorem 2.1.4) any two splitting fields over a given field of a given polynomial are isomorphic. In light of the corollary to Lemma 4.1.2 we can state

LEMMA 4.1.3 *Any two finite fields having the same number of elements are isomorphic.*

Proof. If these fields havep^melements, by the above corollary they are both splitting fields of the polynomial $x^{P^m} - x$, over $J_p$whence they are isomorphic.

Thus for any integer m and any prime number p there is, up to isomorphism, at most one field having p^melements.

The purpose of the next lemma is to demonstrate that for any prime number p and any integer m there is a field having p^m elements.

When this is done we shall know that there is exactly one field having p^m elements where p is an arbitrary prime and man arbitrary integer.

LEMMA 4.1.4 *For every prime number p and every positive integer m there exists a field having p^m elements.*

Proof. Consider the polynomial $x^{P^m} - x$ in $J_p[x]$, the ring of polynomials in x over J_p, the field of integers $mod\ p$.

Let K be the splitting field of this polynomial.

In K let $F = \{a \in K \mid a^{P^m} - a\}$.

The elements of$F$are thusthe roots of $x^{P^m} - x$, which by Corollary 2 to Lemma 2.2.2 are distinct; whence F has p^melements.

We now claim that F is a field. If $a, b \in F$ then $a^{P^m} = a, b^{P^m} = b$ and so $(ab)^{P^m} = a^{P^m} b^{P^m} = ab;$ thus $ab \in F$.

Also since the characteristic is p, $(a \pm b)p^m = a^{p^m} \pm b^{p^m} = a \pm b$, hence$a \pm b \in F$. Consequently $F$is a subfield of K and so is a field. Having exhibited the field F having p^melements we have proved Lemma 4.1.4.

Combining Lemmas 4.1.3 and 1.1.4 we have the next theorem.

THEOREM 4.1 .1 *For every prime number p and every positive integer m there is a unique field having p^m elements.*

We now return to group theory for a moment. The group-theoretic result we seek will determine the structure of any finite multiplicative subgroup of the group of nonzero elements of any field, and, in particular, it will determine the multiplicative structure of any finite field.

LEMMA 4.1.5 *Let G be a finite abelian group enjoying the property that the relation $x^n = e$ is satisfied by at most n elements of G, for every integer n. Then, G is a cyclic group.*

Proof. If the order of G is a power of some prime number q then the result is very easy.

For suppose that $a \in G$ is an element whose order is aslarge as possible; its order must be q^r for some integer r.

The elements$e, a, a^2, \dots, a^{q^r-1}$ give us q^r distinct solutions of the equation $x^{q^r} = e$, which, by our hypothesis, implies that these are all the solutions of this equation.

Now if $b \in G$ its order is q^s where $s \leq r$, hence $b^{q^r} = \left(b^{q^s}\right)^{q^{r-s}} = e$.

By the observation made above this forces $b = a^i$ for some i, and so Giscyclic.

The general finite abelian group G can be realized as $G = S_{q_1} S_{q_2}, \dots, S_{q_k}$where the q_i are the distinct prime divisors of $o(G)$ and where the S_{q_i} are the Sylow subgroups of G.

Moreover, every element $g \in G$can be writtenin a *unique* way as $g = s_1 s_2, \dots, s_k$where $s_i \in S_{q_i}$.

Anysolution of $x^n = e$ in S_{q_i} is one of $x^n = e$ in Gso that each S_{q_i} inherits the hypothesis we have imposed on G.

By the remarks of the first paragraph of the proof, each $S_{q_i}$is a cyclic group; let $a_i$be a generator of S_{q_i}.

We claim that $c = a_1 a_2, \dots, a_k$is a cyclic generator of G.

To verify this all we must do is prove that $o(G)$divides m, the order of c.

Since $c^m = e$, we have that $a_1^m a_2^m, \dots, a_k^m = e$.

By the uniqueness of representation of an element of Gas a product of elements in the S_{q_i}we conclude that each$a_i^m = e$. Thus $o(S_{q_i}) \mid m$for every i.

Thus $o(G) = o(S_{q_1})o(S_{q_2}), \dots, o(S_{q_k}) \mid m$.However, $m \mid o(G)$and so $o(G) = m$. This proves that $G$is cyclic.

Lemma 4.1.5 has as an important consequence

LEMMA 4.1.6 *Let K be a field and let G be a finite subgroup of the multiplicative group of nonzero elements of K. Then G is a cyclic group.*

Proof. Since K is a field, any polynomial of degree n in $K[x]$ has at most n roots in K.

Thus in particular, for any integer n, the polynomial $x^n - 1$has at most n roots in K, and all the more so, at most n roots in G.

The hypothesis of Lemma 4.1.5 is satisfied, so $G$is cyclic.

Even though the situation of a finite field is merely a special case of Lemma 4.1.6, it is of such widespread interest that we single it out as

THEOREM 4.1.2 *The multiplicative group of nonzero elements of a finite field is cyclic.*

Proof. Let F be a finite field.

By merely applying Lemma 4.1.6 with $F = K$ and $G =$ the group of nonzero elements of F, the result drops out.

We conclude this section by using a counting argument to prove the existence of solutions of certain equations in a finite field. We shall need the result in one proof of the Wedderburn theorem.

LEMMA 4.1.7 *If F is a finite field and $\alpha \neq 0$, $\beta \neq 0$are two elements of F then we can find elements a and b in F such that* $1 + \alpha a^2 + \beta b^2 = 0$.

Proof. If the characteristic of F is 2, F has 2^n elements and every element x in F satisfies $x^{2^n} = x$.

Thus every element in F is a square. In particular $\alpha^{-1} = a^2$ for some $a \in F$.

Using this a and $b = 0$, we have$1 + \alpha a^2 + \beta b^2 = 1 + \alpha\alpha^{-1} + 0 = 1 + 1 = 0$ the last equality being a consequence of the fact that the characteristic of F is 2.

If the characteristic of F is an odd prime p, F has p^n elements.

Let $W_\alpha = \{1 + \alpha x^2 | x \in F\}$. How many elements are there in W_α? We must check how often $1 + \alpha x^2 = 1 + \alpha y^2$.

But this relation forces $\alpha x^2 = \alpha y^2$and so, since $\alpha \neq 0, x^2 = y^2$. Finally this leads to $x = \pm y$.

Thus for $x \neq 0$ we get from each pair x and $-x$ one element in W_α, and for $x = 0$ we get $1 \in W_\alpha$.

Thus W_α has $1 + (p^n - 1)/2 = (p^n + 1)/2$ elements.

Similarly $W_\beta = \{-\beta x^2 | x \in F\}$ has $(p^n + 1)/2$ elements. Since each of W_α and W_β has more than half the elements of F they must have a nonempty intersection.

Let $c \in W_\alpha \cap W_\beta$.

Since $c \in W_\alpha$,$c = 1 + \alpha a^2$ for some $a \in F$; since $c \in W_\beta$, $c = -\beta b^2$ for some $b \in F$.

Therefore $1 + \alpha a^2 = -\beta b^2$, which, on transposing yields the desired result

$$1 + \alpha a^2 + \beta b^2 = 0.$$

4.2 WEDDERBURN'S THEOREM OF FINITE DIVISION RINGS

In 1905 Wedderburn proved the theorem, now considered a classic, that a finite division ring must be a commutative field. This result has caught the imagination of most mathematicians because it is so unexpected, interrelating two seemingly unrelated things, namely the number of elements in a certain algebraic system and the multiplication of that system. Aside from its intrinsic beauty the result has been very important and useful since it arises in so many contexts. To cite just one instance, the only known proof of the purely geometric fact that in a finite geometry the Desargues configuration implies that of Pappus (for the definition of these terms look in any good book on projective geometry) is to reduce the geometric problem to an algebraic one, and this algebraic question is then answered by invoking the Wedderburn theorem. For algebraists the Wedderburn theorem has served as a jumping-off point for a large area of research, in the 1940s and 1950s,concerned with the commutativity of rings.

THEOREM 4.2.1 (WEDDERBURN) *A finite division ring is necessarily acommutative field.*

First Proof. Let K be a finite division ring and let $Z = \{z \in K \mid zx = xz \; for \; all \; x \in K\}$ be its center.

If Z has q elements then, as in the proof of Lemma 4.1.1, it follows that K has q^n elements. Our aim is to prove that $Z = K$, or, equivalently, that $n = 1$.

If $a \in K$ let $N(a) = \{x \in K \mid xa = ax\}$. $N(a)$ clearly contains Z, and, as a simple check reveals, $N(a)$ is a subdivision ring of K.

Thus $N(a)$contains $q^{n(a)}$elements for some integer $n(a)$.

We claim that $n(a) | n$.

For, the nonzero elements of $N(a)$form a subgroup of order $q^{n(a)} - 1$ of the group of nonzero elements, under multiplication, of Kwhich has $q^n - 1$ elements.

By Lagrange's theorem $q^{n(a)} - 1$ is a divisorof$q^n - 1$**;** but this forces $n(a)$to be a divisor of n (see Problem 1 at the end of this section).

In the group of nonzero elements of K we have the conjugacy relation, namely a is a conjugate of b if $a = x^{-1}bx$ for some$x \neq 0$ in K.

By Theorem the number of elements in Kconjugate to a is the index of the normalizer of a in the group of nonzero elements of K.

Therefore the number of conjugates of a in $K$is $(q^n - 1)/(q^{n(a)} - 1)$.

Now $a \in Z$ if and only if $n(a) = n$, thus by the class equation

$$q^n - 1 = q - 1 + \sum_{\substack{n(a)|\, n \\ n(a)\neq n}} \frac{q^n - 1}{q^{n(a)} - 1} \qquad (1)$$

where the sum is carried out over one a in each conjugate class for $a's$ not in the center.

The problem has been reduced to proving that no equation such as (1) can hold in the integers.

Up to this point we have followed the proof in Wedderburn's original paper quite closely. He went on to rule out the possibility of equation (1) by making use of the following number-theoretic result due to Birkhoff and Vandiver: for $n > 1$ there exists a prime numberwhich is a divisor of $q^n - 1$ but is not a divisor of *any* $q^m - 1$ where m is a proper divisor of n, with the exceptions of $2^6 - 1 = 63$ whose prime factors already occur as divisors of $2^2 - 1$ and $2^3 - 1$, and $n = 2$, and q a prime of the form $2^k - 1$.

If we grant this result, how would we finish the proof? This prime number would be a divisor of the left-hand side of (1) and also a divisor of each term in the sum occurring on the right-hand side since it divides $q^n - 1$ but not $q^{n(a)} - 1$; thus this prime would then divide $q - 1$ giving us a contradiction.

The case $2^6 - 1$still would need ruling out but that is simple. In case $n = 2$, the other possibility not covered by theabove argument, there can be no subfield between $Z$and $K$and this forces$Z = K$. (Prove!-See Problem 2.)

However, we do not want to invoke the result of Birkhoff and Vandiver without proving it, and its proof would be too large a digression here.

So we look for another artifice. Our aim is to find an integer which divides $(q^n - 1)/(q^{n(a)} - 1)$, for all divisors $n(a)$ of n except $n(a) = n$, but does not divide $q - 1$. Once this is done, equation (1) will be impossible unless $n = 1$ and, therefore, Wedderburn's theorem will have been proved.

Consider the polynomial $x^n - 1$ considered as an element of $C[x]$ where C is the field of complex numbers. In $C[x]$

$$x^n - 1 = \prod(x - \lambda) \qquad (2)$$

where this product is taken over all λ satisfying $\lambda^n = 1$.

A complex number θ is said to be a *primitive nth root of unity* if $\theta^n = 1$ but $\theta^m \neq 1$ for any positive integer $m < n$.

The complex numbers satisfying $x^n = 1$ form a finite subgroup, under multiplication, of the complex numbers, so by Theorem 4.1.2 this group is cyclic.

Any cyclic generator of this group must then be a primitive *nth* root of unity, so we know that such primitive roots exist. (Alternatively, $\theta = e^{2\pi i/n}$ yields us a primitive *nth* root of unity.)

Let $\Phi_n(x) = \prod(x - \theta)$ where this product is taken over all the primitive *nth* roots of unity.

This polynomial is called a *cyclotomic* polynomial. We list the first few cyclotomic polynomials: $\Phi_1(x) = x - 1, \Phi_2(x) = x + 1, \Phi_3(x) = x^2 + x + 1, \Phi_4(x) = x^2 + 1, \Phi_5(x) = x^4 + x^3 + x^2 + x + 1, \Phi_6(x) = x^2 - x + 1$.

Notice that these are all monic polynomials withinteger coefficients.

Our first aim is to prove that in general $\Phi_n(x)$ is a monic polynomial withinteger coefficients.

We regroup the factored form of $x^n - 1$ as given in (2), and obtain

$$x^n - 1 = \prod_{d|n} \Phi_n(x)$$

By induction we assume that $\Phi_d(x)$is a monic polynomial with integer coefficients for $d|n, d \neq n$.

Thus $x^n - 1 = \Phi_n(x)g(x)$ where $g(x)$ is amonic polynomial with integer coefficients. Therefore,

$$\Phi_n(x) = \frac{x^n - 1}{g(x)},$$

which, on actual division (or by comparing coefficients), tells us that $\Phi_n(x)$ is a monic polynomial with integer coefficients.

We now claim that for any divisor $d$of n, where $d \neq n$,

$$\Phi_n(x) \Big| \begin{matrix} x^n - 1 \\ x^d - 1 \end{matrix}$$

in the sense that the quotient is a polynomial with integer coefficients. To see this, first note that

$$x^d - 1 = \prod_{k|d} \Phi_k(x),$$

and since every divisor of $d$is also a divisor of n, by regrouping terms on the right-hand side of (3) we obtain $x^d - 1$ on the right-hand side; also since $d < n$, $x^d - 1$ does not involve $\Phi_n(x)$. Therefore, $x^n - 1 = \Phi_n(x)(x^d - 1)f(x)$where

$$f(x) = \prod_{\substack{k|n \\ k \nmid d}} \Phi_k(x)$$

has integer coefficients, and so

$$\Phi_n(x) \Big| \begin{matrix} x^n - 1 \\ x^d - 1 \end{matrix}$$

in the sense that the quotient is a polynomial with integer coefficients. This establishes our claim.

For any integer t, $\Phi_n(t)$ is an integer and from the above as an integer divides $(t^n - 1)/(t^d - 1)$.

In particular, returning to equation (1) ,

$$\Phi_n(q) \Big| \begin{matrix} q^n - 1 \\ q^{n(a)} - 1 \end{matrix}$$

and $\Phi_n(q) \mid q^n - 1$; thus by (1), $\Phi_n(q) \mid q - 1$.

We claim, however, that if $n > 1$ then $|\Phi_n(q)| > q - 1$. For $\Phi_n(q) = \prod(q - \theta)$ where θ runs over all primitive nth roots of unity and $|q - \theta| > q - 1$ for all $\theta \neq 1$ a root of unity (Prove!) whence $|\Phi_n(q)| = \prod|q - \theta| < q - 1$.

Clearly, then $\Phi_n(q)$ cannot divide $q - 1$, leading us to a contradiction. We must, therefore, assume that $n = 1$, forcing the truth of the Wedderburn theorem.

Second Proof. Before explicitly examining finite division rings again, we prove some preliminary lemmas.

LEMMA 4.2.1 *Let R be a ring and let $a \in R$. Let T_a be the mapping of Rinto itself defined by $xT_a = xa - ax$. Then*

$$xT_a^m = xa^m - maxa^{m-1} + \frac{m(m-1)}{2}a^2xa^{m-2} - \frac{m(m-1)(m-2)}{3!}a^3xa^{m-3} + \cdots$$

Proof. What is xT_a^2? $xT_a^2 = (xT_a)T_a = (xa - ax)T_a = (xa - ax)a - a(xa - ax) = xa^2 - 2axa + a^2x$.

What about xT_a^3? $xT_a^3 = (xT_a^2)T_a = (xa^2 - 2axa + a^2x)a - a(xa^2 - 2axa + a^2x) = xa^3 - 3axa^2 + 3a^2xa - a^3x$.

Continuing in this way, or by the use of induction, we get the result of Lemma 4.2.1.

COROLLARY *If R is a ring in which $px = 0$ for all $x \in R$, where p is a prime number, then $xT_a^{p^m} = xa^{p^m} - a^{p^m}x$.*

Proof. By the formula of Lemma 4.2.1, if $p = 2$, $xT_a^2 = xa^2 + a^2x$, since $2axa = 0$. Thus, $xT_a^4 = (xa^2 + a^2x)a^2 - a^2(xa^2 + a^2x) = xa^4 - a^4x$, and so on for xT_a^{2m}.

If p is an odd prime, again by the formula of Lemma 4.2.1,

$$xT_a^p = xa^p - paxa^{p-1} + \frac{p(p-1)}{2}a^2xa^{p-2} + \cdots - a^px,$$

and since

$$p \left| \frac{p(p-1)\ldots(p-i+1)}{i!} \right.$$

for $i < p$, all the middle terms drop out and we are left with $xT_a^p = xa^p - a^px = xT_{a^p}$. Now $xT_a^{p^2} = x(T_{a^p})^p = xT_{a^{p^2}}$, and so on for the higher powers of p.

LEMMA 4.2.2 *Let D be a division ring of characteristic $p > 0$ with center Z, and let $P = \{0, 1, 2, \ldots, (p-1)\}$ be the subfield of Z isomorphic to J_p. Suppose that $a \in D$, $a \notin Z$ is such that $a^{p^n} = a$ for some $n \geq 1$. Then there exists an $x \in D$ such that*

1. $xax^{-1} \neq a$.
2. $xax^{-1} \in P(a)$ *the field obtained by adjoining a to P.*

Proof. Define the mapping T_a of D into itself by $yT_a = ya - ay$ for every $y \in D$.

$P(a)$ is a finite field, since a is algebraic over P and has, say, p^m elements.

These all satisfy $u^{p^m} = u$. By the corollary to Lemma 4.2.1, $yT_a^{p^m} = ya^{p^m} - a^{p^m}y = ya - ay = yT_a$, and so $T_a^{p^m} = T_a$.

Now, if $\lambda \in P(a)$, $(\lambda x)T_a = (\lambda x)a - a(\lambda x) = \lambda xa - \lambda ax = \lambda(xa - ax) = \lambda(xT_a)$, since λ commutes with a. Thus the mapping λI of D into itself defined by $\lambda I: y \to \lambda y$ commutes with T_a for every $\lambda \in P(a)$. Now the polynomial

$$u^{p^m} - u = \prod_{\lambda \in P(a)} (u - \lambda)$$

by Lemma 4.2.1.

Since T_a commutes with λI for every $\lambda \in P(a)$, and smce$T_a^{p^m} = T_a$, we have that

$$0 = T_a^{p^m} - T_a = \prod_{\lambda \in P(a)} (T_a - \lambda I)$$

If for every $\lambda \neq 0$ in $P(a)$, $T_a - \lambda I$ annihilates no nonzero element in D(if$y(T_a - \lambda I) = 0$ implies $y = 0$), since $T_a(T_a - \lambda_1 I) \ldots (T_a - \lambda_k I) = 0$, where $\lambda_1, \ldots, \lambda_k$ are the nonzero elements of $P(a)$, we would get $T_a = 0$. That is, $0 = yT_a = ya - ay$ for every $y \in D$ forcing $a \in Z$ contrary to hypothesis.

Thus there is a $\lambda \neq 0$ in $P(a)$ and an $x \neq 0$ in D such that $x(T_a - \lambda I) = 0$.

Writing this out explicitly, $xa - ax - \lambda x = 0$; hence, $xax^{-1} = a + \lambda$ is in $P(a)$ and is not equal to a since $\lambda \neq 0$. This proves the lemma.

COROLLARY *In Lemma 4.2.2, $xax^{-1} = a^i \neq a$ for some integer i.*

Proof. Let a be of order s; then in the field $P(a)$ all the roots of thepolynomial $u^s - 1$ are $1, a, a^2, \ldots, a^{s-1}$since these are all distinct roots and they are s in number.

Since$(xax^{-1})^s = xa^s x^{-1} = 1$, and since $xax^{-1} \in P(a), xax^{-1}$ is a root in $P(a)$ of $u^s - 1$, hence $xax^{-1} = a^i$.

We now have all the pieces that we need to carry out our second proof of Wedderburn's theorem.

Let D be a finite division ring and let Z be its center. By induction we may assume that any division ring having fewer elements than $D$is acommutative field.

We first remark that if $a, b \in D$ are such that $b^t a = ab^t$ but $ba \neq ab$, then $b^t \in Z$.

For, consider $N(b^t) = \{x \in D | b^t x = xb^t\}$. $N(b^t)$ is a subdivision ring of $D;$ if it were not D, by our induction hypothesis, it would be commutative.

However, both a and b are in $N(b^t)$and these do not commute; consequently, $N(b^t)$ is not commutative so must be all of D. Thus $b^t \in Z$.

Every nonzero element in D has finite order, so some positive power of it falls in Z. Given $w \in D$ let the *order if w relative to Z* be the smallest positive integer $m(w)$ such that $w^{m(w)} \in Z$.

Pick an element a in D but not in Z having minimal possible order relative to Z, and let this order be r.

We claim that r is a prime number, for if $r = r_1 r_2$with $1 < r_1 < r$ then a^{r_1} is not in Z. Yet $(a^{r_1})^{r_2} = a^r \in Z$, implying that a^{r_1}has an order relative to Z smaller than that of a.

By the corollary to Lemma 4.2.2 there is an $x \in D$ such that $xax^{-1} = a^i \neq a;$ thus $x^2 ax^{-2} = x(xax^{-1})x^{-1} = xa^i x^{-1} = (xax^{-1})^i = \left(a^i\right)^i = a^{i^2}$.

Similarly, we get $x^{r-1} ax^{-(r-1)} = a^{i^{r-1}}$.

However, r is a prime number, thus by the little Fermat theorem (corollary to Theorem 2.4 .1), $i^{r-1} = 1 + u_0 r$, hence $a^{i^{r-1}} = a^{1+u_0 r} = aa^{u_0 r} = \lambda a$ where $\lambda = a^{u_0 r} \in Z$. Thus$x^{r-1} a = \lambda a x^{r-1}$.

Since $x \notin Z$, by the minimal nature of r, x^{r-1}cannot bein Z.

By the remark of the earlier paragraph, since $xa \neq ax, x^{r-1}a \neq ax^{r-1}$ and so$\lambda \neq 1$.

Let $b = x^{r-1};$ thus $bab^{-1} = \lambda a;$ consequently, $\lambda^r a^r = (bab^{-1})^r = ba^r b^{-1} = a^r$since $a^r \in Z$. This relation forces $\lambda^r = 1$.

We claim that if $y \in D$ then whenever $y^r = 1$, then $y = \lambda^i$for some i,for in the *field* $Z(y)$ there are at most $r$roots of the polynomial $u^r - 1$;the elements $1, \lambda, \lambda^2, \ldots, \lambda^{r-1}$ in Z are all distinct since λ is of the prime order r and they already account for r roots of $u^r - 1$ in $Z(y)$, in consequence of which $y = \lambda^i$.

Since $\lambda^r = 1, b^r = \lambda^r b^r = (\lambda b)^r = (a^{-1}ba)^r = a^{-1}b^r a$ from which we get $ab^r = b^r a$.

Since a commutes with b^r but does not commute with b, by the remark made earlier, b^rmust be in Z.

By Theorem 4.1.2 the multiplicative group of nonzero elements of Z is cyclic; let $\gamma \in Z$ by a generator.

Thus $a^r = \gamma^j, b^r = \gamma^k$;if $j = sr$then $a^r = \gamma^{sr}$, whence$(a/\gamma^s)^r = 1$; thiswould imply that $a/\gamma^s = \lambda^i$, leading to $a \in Z$, contrary to $a \notin Z$.

Hence,$r \nmid j;$ similarly $r \nmid k$. Let $a_1 = a^k$and$b_1 = b^j;$ a direct computation from $ba = \lambda ab$leads to $a_1 b_1 = \mu b_1 a_1$where$\mu = \lambda^{-jk} \in Z$.

Since the prime number r which is the order of λ does not divide $j$or k,$\lambda^{jk} \neq 1$ hence$\mu \neq 1$. Note that $\mu^r = 1$.

Let us see where we are. We have produced two elements a_1, b_1 such that

1. $a_1^r = b_1^r = \alpha \in Z$.
2. $a_1 b_1 = \mu b_1 a_1 with \mu \neq 1$ *in* Z.
3. $\mu^r = 1$.

We compute $(a_1^{-1}b_1)^r; (a_1^{-1}b_1)^2 = a_1^{-1}b_1 a_1^{-1}b_1 = a_1^{-1}(b_1 a_1^{-1})b_1 = a_1^{-1}(\mu a_1^{-1}b_1)b_1 = \mu a_1^{-2}b_1^2$. If we compute $(a_1^{-1}b_1)^3$ we find it equal to$\mu^{1+2}a_1^{-3}b_1^3$. Continuing, we obtain

$(a_1^{-1}b_1)^r = \mu^{1+2+\cdots+(r+1)}a_1^{-r}b_1^r = \mu^{1+2+\cdots+(r+1)} = \mu^{r(r-1)/2}$.If $r$is an odd prime, since $\mu^r = 1$, we get$\mu^{r(r-1)/2} = 1$, whence $(a_1^{-1}b_1)^r = 1$.

Being a solution of $y^r = 1, a_1^{-1}b_1 = \lambda^i$ so that $b_1 = \lambda^i a_1;$ but then $\mu b_1 a_1 = a_1 b_1 = b_1 a_1$, contradicting$\mu \neq 1$.

Thus if $r$is an odd prime number, the theorem is proved.

We must now rule out the case $r = 2$. In that special situation we have two elements $a_1, b_1 \in D$ such that $a_1^2 = b_1^2 = \alpha \in Z, a_1 b_1 = \mu b_1 a_1$ where$\mu^2 = 1$ and $\mu \neq 1$.

Thus $\mu = -1$ and $a_1 b_1 = -b_1 a_1 \neq b_1 a_1;$ in consequence, the characteristic of *D* is *not* 2. By Lemma 4.1.7 we can find elements $\zeta, \eta \in Z$ such that $1 + \zeta^2 - \alpha\eta^2 = 0$.

Consider $(a_1 + \zeta b_1 + \eta a_1 b_1)^2$; on computing this out we find that

$$(a_1 + \zeta b_1 + \eta a_1 b_1)^2 = \alpha(1 + \zeta^2 - \alpha\eta^2) = 0.$$

Being in a division ring this yields that $a_1 + \zeta b_1 + \eta a_1 b_1 = 0$; thus $0 \neq 2a_1^2 = a_1(a_1 + \zeta b_1 + \eta a_1 b_1) + (a_1 + \zeta b_1 + \eta a_1 b_1)a_1 = 0$.

This contradiction finishes the proof and Wedderburn's theorem is established.

This second proof has some advantages in that we can use parts of it to proceed to a remarkable result due to Jacobson, namely,

UNIT – V

5.1 SOLVABILITY BY RADICALS

Given the specific polynomial $x^2 + 3x + 4$ over the field of rationalnumbers F_0 , from the quadratic formula for its roots we know that its roots are $(-3 \pm \sqrt{-7})/2$; thus the field $F_0(\sqrt{7i})$ is the splitting field of $x^2 + 3x + 4$ over F_0.Consequently there is an element $\gamma = -7$ in F_0such that the extension field $F_0(\omega)$ where $\omega^2 = \gamma$is such that it contains all the roots of $x^2 + 3x + 4$.

From a slightly different point of view, given the *general* quadratic polynomial $p(x) = x^2 + a_1x + a_2$over F, we can consider it as a *particular* polynomial over the field $F(a_1, a_2)$of rational functions .in the two variables a_1 and a_2 over F*;* in the extension obtained by adjoining ω to $F(a_1, a_2)$ where $\omega^2 = a_1^2 - 4a_2 \in F(a_1, a_2)$, we find all the roots of $p(x)$. There is a formula which expresses the roots of $p(x)$ in terms of a_1, a_2 and square roots of rational functions of these.

For a cubic equation the situation is very similar; given the general cubic equation $p(x) = x^3 + a_1x^2 + a_2x + a_3$ an explicit formula can be given, involving combinations of square roots and cube roots of rational functionsin a_1, a_2, a_3. While somewhat messy, they are explicitly given by *Cardan' s formulas:*

Let $p = a_2 - (a_1^2/3)$ and $q = \frac{2a_1^2}{27} - \frac{a_1a_2}{3} + a_3$

and let

$$P = \sqrt[3]{-\frac{q}{2} + \sqrt{\frac{p^3}{27} + \frac{p^2}{4}}}$$

And

$$Q = \sqrt[3]{-\frac{q}{2} - \sqrt{\frac{p^3}{27} + \frac{p^2}{4}}}$$

(with cube roots chosen properly); then the roots are $P + Q - (a_1/3)$,$\omega P + \omega^2 Q - (a_1/3)$, and $\omega^2 P + \omega Q - (a_1/3)$, where $\omega \neq 1$ is a cuberoot of 1. The above formulas only serve to illustrate for us that by adjoining a certain square root and then a cube root to $F(a_1, a_2, a_3)$ wereach a field in which $p(x)$has its roots.

For fourth-degree polynomials, which we shall not give explicitly, by using rational operations and square roots, we can reduce the problem to that of solving a certain cubic, so here too a formula can be given expressing the roots in terms of combinations of radicals (surds) of rational functions of the coefficients.

For polynomials of degree five and higher, no such universal radical formula can be given, for we shall prove that it is impossible to express their roots, in general, in this way.

Given a field $F$and a polynomial $p(x) \in F[x]$, we say that $p(x)$ *is solvable by radicals over* F if we can find a finite sentence of fields $F_1 = F(\omega_1), F_2 = F_1(\omega_2), \ldots, F_k = F_{k-1}(\omega_k)$ such that $\omega_1^{r_1} \in F, \omega_2^{r_2} \in F_1, \ldots, \omega_k^{r_k} \in F_{k-1}$ such that the roots of $p(x)$all lie in F_k.

If K is , the splitting field of $p(x)$ over F, then $p(x)$ is solvable by radicals over F if we can find a sequence of fields as above such that $K \subset F_k$. An important remark, and one we shall use later, in the proof of Theorem 5.1.2, is that if such an F_k can be found, we can, without loss of generality, assume it to be a *normal* extension of F*;* we leave its proof as a problem (Problem 1).

By the *general polynomial of degree n over* F, $p(x) = x^n + a_1 x^{n-1} + \cdots + a_n$We mean the following: Let $F(a_1, \ldots, a_n)$be the field of rational functions, in the n variables $a_1, \ldots, a_n$over F, and consider the particular polynomial $p(x) = x^n + a_1 x^{n-1} + \cdots + a_n$ over the field $F(a_1, \ldots, a_n)$· We say that it is solvable by radicals if it is solvable by radicals over $F(a_1, \ldots, a_n)$. This really expresses the intuitive idea of "finding a formula" for the roots of $p(x)$ involving combinations of *m*th roots, for various *m's*, of rational functions in $a_1, a_2, \ldots, a_n$ For

$n = 2, 3$, and 4, we pointed out that this can always be done. For $n \geq 5$, Abel proved that this cannotbe done. However, this does not exclude the possibility that a given polynomial over F may be solvable by radicals. In fact, we shall give a criterion for this in terms of the Galois group of the polynomial. But first we must develop a few purely group-theoretical results.

DEFINITION A group G is said to be *solvable* if we can find a finite chain of subgroups $G = N_0 \supset N_1 \supset N_2 \supset \cdots \supset N_k = (e)$, where each N_i is anormal subgroup of N_{i-1} and such that every factor group N_{i-1}/N_i is abelian.

Every abelian group is solvable, for merely take $N_0 = G$ and $N_1 = (e)$ to satisfy the above definition. The symmetric group of degree 3, S_3, is solvable for take $N_1 = \{e, (1,2,3), (1,3,2)\}$; N_1 is a normal subgroup ofS_3 and S_3/N_1 and $N_1/(e)$ are both abelian being of orders 2 and 3, respectively. It can be shown that S_4 is solvable (Problem 3). For $n \geq 5$ weshow in Theorem 5.1.1 below that S_n is *not* solvable.

We seek an alternative description for solvability. Given the group G and elements a, b in G, then the *commutator* of a and b is the element $a^{-1}b^{-1}ab$. The *commutator subgroup*, G', of $G$is the subgroup of G generated by all the commutators in G. (It is *not* necessarily true that the set of commutators itself forms a subgroup of G.) It was an exercise before that G' is a normal subgroup of G. Moreover, the group $G/G'$is abelian, for, given any two elements in it, aG', bG', with $a, b \in G$, then

$$(aG')(bG') = abG' = ba(a^{-1}b^{-1}ab)G'$$

$$= (since\ a^{-1}b^{-1}ab \in G')baG' = (bG')(aG').$$

On the other hand, if M is a normal subgroup of G such that G/M is abelian, then $M \supset G'$, for, given $a, b \in G$, then $(aM)(bM) = (bM)(aM)$, from which we deduce $abM = baM$ whence *a- 1b- 1abM = M* and so $a^{-1}b^{-1}ab \in M$. Since M contains all commutators, it contains the group these generate, namely G'.

G' is a group in its own right, so we can speak of its commutator subgroup$G^{(2)} = (G')'$. This is the subgroup of Ggenerated by all elements$(a')^{-1}(b')^{-1}a'b'$ where $a', b' \in G'$. It is easy

to prove that not only is $G^{(2)}$a normal subgroup of G' but it is also a normal subgroup of G(Problem 4).We continue this way and define the higher commutator subgroups $G^{(m)}$by$G^{(m)} = (G^{(m-1)})'$. Each $G^{(m)}$is a normal subgroup of G (Problem 4) and$G^{(m-1)}/G^{(m)}$ is an abelian group.

In terms of these higher commutator subgroups of G, we have a very succinct criterion for solvability, namely,

LEMMA 5.1.3 *Suppose that the field F has all nth roots of unity (for some particular n) and suppose that $a \neq 0$ is in F. Let $x^n - a \in F[x]$ and let K be its splitting field over F. Then*

1. $K = F(u)$*where u is any root of* $x^n - a$.
2. *The Galois group of* $x^n - a$ *over* F *is abelian.*

Proof. Since Fcontains all nth roots of unity, it contains $\xi = e^{2\pi i/n}$; note that $\xi^n = 1$ but $\xi^m \neq 1$ for $0 < m < n$.

If $u \in K$ is any root of $x^n - a$, then $u, \xi u, \xi^2 u, \ldots, \xi^{n-1}u$ are all the roots of $x^n - a$.

That they are roots is clear; that they are distinct follows from: $\xi^i = \xi^u$with $0 \leq i < j < n$, then since $u \neq 0$, and $(\xi^i - \xi^j)u = 0$,we must have $\xi^i = \xi^j$, which is impossible since $\xi^{j-i} = 1$, with $0 < j - i < n$.

Since $\xi \in F$, all of $u, \xi u, \xi^2 u, \ldots, \xi^{n-1}u$ are in $F(u)$, thus $F(u)$ splits $x^n - a$; since no proper subfield of $F(u)$which contains F also contains u, no proper subfield of $F(u)$ can split $x^n - a$. Thus $F(u)$ is the splitting field of $x^n - a$, and we have proved that $K = F(u)$.

If σ, τ are any two elements in the Galois group of $x^n - a$, that is, if σ, τ are automorphisms of $K = F(u)$ leaving every element of F fixed, then since both $\sigma(u)$ and $\tau(u)$ are roots of $x^n - a$, $\sigma(u) = \xi^i(u)$ and $\tau(u) = \xi^j(u)$ for some i and j.

Thus $\sigma\tau(u) = \sigma(\xi^j u) = \xi^j \sigma(u)$ (since $\xi^j \in F$)$= \xi^i \xi^j u = \xi^{i+j}u$; similarly, $\tau\sigma(u) = \xi^{i+j}u$.

Therefore, $\sigma\tau$ and $\tau\sigma$ agree on u and on F hence on all of $K = F(u)$.

But then $\sigma\tau = \tau\sigma$, whence the Galois group is abelian.

Note that the lemma says that when F has all nth roots of unity, then adjoining one root of $x^n - a$ to F, where $a \in F$, gives us the whole splitting field of $x^n - a$; thus this must be a normal extension of F.

We assume for the rest of the section that F is a field which contains all nth roots of unity for every integer n. We have

THEOREM 5.1.2 *If $p(x) \in F[x]$ is solvable by radicals over F, then the Galois group over F of $p(x)$ is a solvable group.*

Proof. Let K be the splitting field of $p(x)$ over F; the Galois group of $p(x)$ over F is $G(K, F)$. Since $p(x)$ is solvable by radicals, there exists a sequence of fields

$$F \subset F_1 = F(\omega_1) \subset F_2 = F(\omega_2) \subset \cdots \subset F_k = F_{k-1}(\omega_k),$$

where $\omega_1^{r_1} \in F, \omega_2^{r_2} \in F_1, \ldots, \omega_k^{r_k} \in F_{k-1}$ and where $k \subset F_k$.

As we pointed out, without loss of generality we may assume that $F_k$is a normal extension of F. As a normal extension of F, F_k is also a normal extension of any intermediate field, hence F_k is a normal extension of each F_i.

By Lemma 5.1.3 each F_i is a normal extension of F_{i-1} and since F_k is normal over F_{i-1}, by Theorem 3.1.6, $G(F_k, F_i)$is a normal subgroup in$G(F_k, F_{i-1})$.

Consider the chain

$$G(F_k, F) \supset G(F_k, F_1) \supset G(F_k, F_2) \supset \cdots \supset G(F_k, F_{k-1}) \supset (e) \qquad (1)$$

As we just remarked, each subgroup in this chain is a normal subgroup in the one preceding it. Since $F_i$is a normal extension of F_{i-1}, by the fundamental theorem of Galois theory (Theorem 3.1.6) the group of F_i over F_{i-1} , $G(F_i, F_{i-1})$ is isomorphic to $G(F_k, F_{i-1})/G(F_k, F_i)$.

However, by Lemma 5.1.3, $G(F_i, F_{i-1})$ is an abelian group. Thus each quotient group $G(F_k, F_{i-1})/G(F_k, F_i)$of the chain (1) is abelian.

Thus the group $G(F_k, F)$is solvable! Since $K \subset F_k$ and is a normal extension of F(being a splitting field), by Theorem 3.1.6, $G(F_k, F)$is a normal subgroup of $G(F_k, F)$and $G\ (K, F)$ is isomorphic to $G(F_k, F)/G(F_k, K)$. Thus $G(K, F)$is a homomorphic image of $G(F_k, F)$, a solvable group; by the corollary to Lemma 5.1.1, $G(K, F)$ itself must then be a solvable group.

Since $G\ (K, F)$is the Galois group of $p(x)$over F the theorem has been proved.

We make two remarks without proof.

1. The converse of Theorem 5.1.2 is also true; that is, if the Galois group of $p(x)$ over F is solvable then $p(x)$is solvable by radicals over F.
2. Theorem 5.1.2 and its converse are true even if Fdoes not containroots of unity.

Recalling what is meant by the general polynomial of degree $n$over F, $p(x) = x^n + a_1x^{n-1} + \cdots + a_n$and what is meant by solvable by radicals, we close with the great, classic theorem of Abel:

THEOREM 5.1.3 *The general polynomial of degree $n \geq 5$ is not solvable by radicals.*

Proof. In Theorem 3.1.3 we saw that if $F(a_1, \ldots, a_n)$ is the field of rational functions in the n variables $a_1, \ldots, a_n$ then the Galois group of the polynomial $p(t) = t^n + a_1t^{n-1} + \cdots + a_n$ over $F(a_1, \ldots, a_n)$ was S_n, the symmetric group of degree n. By Theorem 5.1.1, $S_n$is not a solvable group when $n \geq 5$, thus by Theorem 5.1.2, $p(t)$ is not solvable by radicals over $F(a_1, \ldots, a_n)$ when $n \geq 5$.

Problems

1. If $p(x)$ is solvable by radicals over F, prove that we can find a sequence of fields
$$F \subset F_1 = F_1(\omega_1) \subset F_2 = F_1(\omega_2) \subset \cdots \subset F_k = F_{k-1}(\omega_k),$$
where$\omega_1^{r_1} \in F, \omega_2^{r_2} \in F_1, \ldots, \omega_k^{r_k} \in F_{k-1}, F_k$ containing all the roots of $p(x)$, such that $F_k$is *normal* over F.

2. Prove that a subgroup of a solvable group is solvable.
3. Prove that S_4 is a solvable group.
4. If $G$is a group, prove that all $G^{(k)}$ are normal subgroups of G.
5. If $N$is a normal subgroup of Gprove that N'must also be a normalsubgroup of G.
6. Prove that the alternating group (the group of even permutations inS_n) $A_n$has no nontrivial normal subgroups for $n \geq 5$.

5.2 A THEOREM OF FROBENIUS

In 1877 Frobenius classified all division rings having the field of real numbers in their center and satisfying, in addition, one other condition to be described below. The aim of this section is to present this result of Frobenius.

FACT 1 Every polynomial of degree n over the field of complex numbers has all its n roots in the field of complex numbers.

FACT 2 The only irreducible polynomials over the field of real numbers are of degree 1 or 2.

DEFINITION A division algebra D is said to be *algebraic over a field F* if

1. F is contained in the center of D;
2. every$a \in D$ satisfies a nontrivial polynomial with coefficients in F.

If D, as a vector space, is finite-dimensional over the field F which is contained in its center, it can easily be shown that D is algebraic over F (seeProblem 1, end ofthis section). However, it can happen that $D$is algebraic over F yet is not finite-dimensional over F.

We start our investigation of division rings algebraic over the real field by first finding those algebraic over the complex field.

LEMMA 5.2.1 *Let C be the field of complex numbers and suppose that the division ring D is algebraic over C. Then $D = C$.*

Proof. Suppose that $a \in D$. Since $D$is algebraic over C, $a^n + \alpha_1 a^{n-1} + \cdots + \alpha_{n-1} a + \alpha_n = 0$ for some $\alpha_1, \alpha_2, \ldots, \alpha_n$in C.

Now the polynomial $p(x) = x^n + \alpha_1 x^{n-1} + \cdots + \alpha_{n-1}x + \alpha_n$in $C[x]$,by Fact 1, can be factored, in $C\,[\,x]$, into a product of linear factors; that is, $p(x) = (x - \lambda_1)(x - \lambda_2) \ldots (x - \lambda_n)$ where $\lambda_1, \lambda_2, \ldots, \lambda_n$are all in C.

Since C is in the center of D, every element of Ccommutes with a, hence $p(a) = (a - \lambda_1)(a - \lambda_2) \ldots (a - \lambda_n)$.

But, by assumption, $p(a) = 0$, thus $(a - \lambda_1)(a - \lambda_2) \ldots (a - \lambda_n) = 0$.

Since a product in a divisionring is zero only if one of the terms of the product is zero, we conclude that $a - \lambda_k = 0$ for some k, hence $a = \lambda_k$, from which we get that $a \in C$.

Therefore, every element of D is in C; since $C \subset D$, we obtain $D = C$.

We are now in a position to prove the classic result of Frobenius, namely,

THEOREM 5.2.1 (FROBENIUs) *Let D be a division ring algebraic over F the field of real numbers. Then D is isomorphic to one of the field of real numbers, the field of complex numbers, or the division ring of real quaternions.*

Proof. The proof consists of three parts. In the first, and easiest, we dispose of the commutative case; in the second, assuming that D is not commutative, we construct a replica of the real quaternions in D; in the third part we show that this replica of the quaternions fills out all of D.

Suppose that $D \neq F$ and that a is in Dbut not in F.

By our assumptions, a satisfies some polynomial over F, hence some irreducible polynomial over F.

In consequence of Fact 2, a satisfies either a linear or quadratic equation over F.

If this equation is linear, a must be in Fcontrary to assumption.

So we may suppose that $a^2 - 2\alpha a + \beta = 0$ where $\alpha, \beta \in F$.

Thus$(a-\alpha)^2=\alpha^2-\beta;$ we claim that $\alpha^2-\beta<0$ for, otherwise, it would have a real square root δ and we would have $a-\alpha=\pm\delta$ and so a would be in F.

Since $\alpha^2-\beta<0$ it can be written as $-\gamma^2$where $\gamma\in F$.

Consequently $(a-\alpha)^2=-\gamma^2,$ whence $[(a-\alpha)/\gamma]^2=-1.$ *Thus if* $a\in D$,$a\notin F$ *we can find real* a, y *such that* $[(a-\alpha)/\gamma]^2=-1.$

If D is commutative, pick $a\in D, a\notin F$ and let $i=(a-\alpha)/\gamma$ where α,γ in F are chosen so as to make $i^2=-1.$

Therefore D contains $F(i)$, a field isomorphic to the field of complex numbers.

Since $D$is commutative andalgebraic over Fit is, all the more so, algebraic over $F(i)$.

By Lemma 5.2.1we conclude that $D=F(i)$. Thus if D is commutative it is either F*or* $F(i)$.

Assume, then, that D is *not* commutative.

We claim that the center of D must be exactly F.

If not, there is an $a$in the center, a not in F. But then for some $\alpha,\gamma\in F$,$[(a-\alpha)/\gamma]^2=-1$ so that the center contains a field isomorphic to the complex numbers. However, by Lemma 5.2.1 if the complex numbers (or an isomorph of them) were in the center of D then $D=C$ forcing D to be commutative.

Hence $F$is the center of D.

Let $a\in D$, $a\notin F;$ for some $\alpha,\gamma\in F$,$i=(a-\alpha)/\gamma$ satisfies $i^2=-1.$

Since $i\notin F$, i is not in the center of F. Therefore there is an element $b\in D$ such that $c=bi-ib\neq 0.$

We compute $ic+ci; ic+ci=i(bi-ib)+(bi-ib)i=ibi-i^2b+bi^2-ibi=0$ since $i^2=-1.$

Thus $ic = -ci$; from this we get $ic^2 = -c(ic) = -c(-ci) = c^2 i$, and so c^2 commutes with i. Now c satisfies some quadratic equation over F, $c^2 + \lambda c + \mu = 0$. Since c^2 and μ commute with i, λc must commute with i; that is, $\lambda ci = i\lambda c = \lambda ic = -\lambda ci$, hence $2\lambda ci = 0$, and since $2ci \neq 0$ we have that $\lambda = 0$.

Thus $c^2 = -\mu$; since $c \notin F$ (for $ci = -ic \neq ic$) we can say, as we have before, that μ is positive and so $\mu = \nu^2$ where $\nu \in F$. Therefore $c^2 = -\nu^2$;let$j = c/\nu$. Then j satisfies

1. $j^2 = \frac{c^2}{\nu^2} = -1$.
2. $ji + ij = \frac{c}{\nu} i + i\frac{c}{\nu} = \frac{ci+ic}{\nu} = 0$.

Let $k = ij$. The i, j, k we have constructed behave like those for the quaternions,whence $T = \{\alpha_0 + \alpha_1 i + \alpha_2 j + \alpha_3 k \mid \alpha_0, \alpha_1, \alpha_2, \alpha_3 \in F\}$ forms asubdivision ring of Disomorphic to the real quaternions. We have produced a replica, T, of the division ring of real quaternions in D!

Our last objective is to demonstrate that $T = D$.

If $r \in D$satisfies $r^2 = -1$ let $N(r) = \{x \in R \mid xr = rx\}$. $N(r)$ is a subdivision ring of D; moreover r, and so all $\alpha_0 + \alpha_1 r, \alpha_0, \alpha_1 \in F$are in the center of $N(r)$.

By Lemma 5.2.1 it follows that $N(r) = \{\alpha_0 + \alpha_1 r \mid \alpha_0, \alpha_1 \in F\}$. Thus if $xr = rx$ then $x = \alpha_0 + \alpha_1 r$ for some α_0, α_1 in F.

Suppose that $u \in D$, $u \notin F$. For some$\alpha, \beta \in F, w = (u - \alpha)/\beta$ satisfies $w^2 = -1$.

We claim that $wi + iw$ commutes with both i and w; for $i(wi + iw) = iwi + i^2 w = iwi + wi^2 = (iw + wi)i$since $i^2 = -1$.

Similarly $w(wi + iw) = (wi + iw)w$. By the remark of the preceding paragraph, $wi + iw = \alpha_0' + \alpha_1' i = \alpha_0 + \alpha_1 w$.

If $w \notin T$this last relation forces $\alpha_1 = 0$ (for otherwise we could solve for $w$in terms of i). Thus$wi + iw = \alpha_0 \in F$.

Similarly $wj + jw = \beta_0 \in F$and $wk + kw = \gamma_0 \in F$.Let

$$z = w + \frac{\alpha_0}{2}i + \frac{\beta_0}{2}j + \frac{\gamma_0}{2}k.$$

Then

$$zi + iz = wi + iw + \frac{\alpha_0}{2}(i^2 + i^2) + \frac{\beta_0}{2}(ji + ij) + \frac{\gamma_0}{2}(ki + ik)$$

$$= \alpha_0 - \alpha_0 = 0$$

similarly $zj + jz = 0$ and $zk + kz = 0$.

We claim these relations force z to be 0.

For $0 = zk + kz = zij + ijz = (zi + iz)j + i(jz - zj) = i(jz - zj)$ since $zi + iz = 0$.

However $i \neq 0$, and since we are in adivision ring, it follows that $jz - zj = 0$. But $jz + zj = 0$.

Thus $2jz = 0$, and since $2j \neq 0$ we have that $z = 0$. Going back to the expression for z we get

$$w + \frac{\alpha_0}{2}i + \frac{\beta_0}{2}j + \frac{\gamma_0}{2}k = 0$$

hence $w \in T$, contradicting $w \notin T$.

Thus, indeed, $w \in T$. Since $w = (u - \alpha)/\beta, u = \beta w + \alpha$ and so $u \in T$.

We have proved that any element in $D$is in T. Since $T \subset D$ we conclude that $D = T;$ because T is isomorphic to the real quaternions we now get that D is isomorphic to the division ring of real quaternions. This, however, is just the statement of the theorem.

Problems

1. If the division ring $D$is finite-dimensional, as a vector space, over the field Fcontained in the center of D, prove that D is algebraic over F.

2. Give an example of a field K algebraic over another field F but not finite-dimensional over F.
3. If A is a ring algebraic over a field $F$and A has no zero divisors prove that A is a division ring.

5.3 INTEGRAL OUATERNIONS AND THE FOLLT-SQUARE THEOREM

When the results about this class of rings were applied to the ring of Gaussian integers, we obtained, as a consequence, the famous result of Fermat that every prime number of the form $4n + 1$is the sum of two squares.

We shall now consider a particular subring of the quaternions which, in all ways except for its lack of commutativity, will look like a Euclidean ring. Because of this it will be possible to explicitly characterize all its left-ideals. This characterization of the left-ideals will lead us quickly to a proof of the classic theorem of Lagrange that every positive integer is a sum of four squares.

DEFINITION For $x = \alpha_0 + \alpha_1 i + \alpha_2 j + \alpha_3 k$ in Q the *adjoint* of x, denoted by x^*, is defined by $x^* = \alpha_0 - \alpha_1 i - \alpha_2 j - \alpha_3 k$.

LEMMA 5.3.1 *Theadjoint in Q satisfies*

1. $x^{**} = x;$
2. $(\delta x + \gamma y)^* = \delta x^* + \gamma y^*;$
3. $(xy)^* = y^* x^*;$

for all x, y in Q and all real δ and γ.

Proof. If $x = \alpha_0 + \alpha_1 i + \alpha_2 j + \alpha_3 k$ then $x^* = \alpha_0 - \alpha_1 i - \alpha_2 j - \alpha_3 k$, whence $x^{**} = (x^*)^* = \alpha_0 + \alpha_1 i + \alpha_2 j + \alpha_3 k$, proving part 1.

Let $x = \alpha_0 + \alpha_1 i + \alpha_2 j + \alpha_3 k$ and $y = \beta_0 + \beta_1 i + \beta_2 j + \beta_3 k$ be in Q and let δ and γ be arbitrary real numbers.

Thus $\delta x + \gamma y = (\delta\alpha_0 + \gamma\beta_0) + (\delta\alpha_1 + \gamma\beta_1)i + (\delta\alpha_2 + \gamma\beta_2)j + (\delta\alpha_3 + \gamma\beta_3)k$; therefore by the definitionof the $*$, $(\delta x + \gamma y)^* = (\delta\alpha_0 + \gamma\beta_0) - (\delta\alpha_1 + \gamma\beta_1)i - (\delta\alpha_2 + \gamma\beta_2)j - (\delta\alpha_3 + \gamma\beta_3)k = \delta(\alpha_0 + \alpha_1 i + \alpha_2 j + \alpha_3 k) + \gamma(\alpha_0 - \alpha_1 i - \alpha_2 j - \alpha_3 k) = \delta x^* + \gamma y^*$. This, of course, proves part 2.

In light of part 2, to prove 3 it is enough to do so for a basis of Q over the reals.

We prove it for the particular basis 1, i, j, k. Now $ij = k$, hence$(ij)^* = k^* = -k = ji = (-j)(-i) = j^* i^*$.

Similarly $(ik)^* = k^* i^*, (jk)^* = k^* j^*$. Also $(i^2)^* = (-1)^* = -1 = (i^*)^2$, and similarly for j and k. Since part 3 is true for the basis elements and part 2 holds, 3 is true for all linear combinations of the basis elements with real coefficients, hence 3 holds for arbitrary x and$y$ in Q.

DEFINITION If $x \in Q$then the *norm* of x, denoted by $N(x)$, is defined by $N(x) = xx^*$.

Note that if $x = \alpha_0 + \alpha_1 i + \alpha_2 j + \alpha_3 k$ then

$$N(x) = xx^* = (x = \alpha_0 + \alpha_1 i + \alpha_2 j + \alpha_3 k)(\alpha_0 - \alpha_1 i - \alpha_2 j - \alpha_3 k)$$

$$= \alpha_0^2 + \alpha_1^2 + \alpha_2^2 + \alpha_3^2;$$

therefore $N(0) = 0$ and $N(x)$is a *positive* real number for $x \neq 0$ in Q. In particular, for any real number $\alpha, N(\alpha) = \alpha^2$. If$x \neq 0$ note that $x^{-1} = [1/N(x)]\, x^*$.

LEMMA 5.3.2 *For all* $x, y \in Q, N(xy) = N(x)N(y)$.

Proof. By the very definition of norm, $N(xy) = (xy)(xy)^*$; by part 3 of Lemma 5.2.1, $(xy)^* = y^* x^*$and so $N(xy) = xyy^* x^*$.

However, $yy^* = N(y)$is a real number, and thereby it is in the center of Q; in particular it must commute with x^*.

Consequently $N(xy) = x(yy^*)x^* = (xx^*)(yy^*) = N(x)N(y)$.

As an immediate consequence of Lemma 5.3.2 we obtain

LEMMA 5.3.3 ***(LAGRANGE IDENTITY)*** *If* $\alpha_0, \alpha_1, \alpha_2, \alpha_3$ *and* $\beta_0, \beta_1, \beta_2, \beta_3$ *are real numbers then* $(\alpha_0^2 + \alpha_1^2 + \alpha_2^2 + \alpha_3^2)(\beta_0^2 + \beta_1^2 + \beta_2^2 + \beta_3^2) = (\alpha_0\beta_0 - \alpha_1\beta_1 - \alpha_2\beta_2 - \alpha_3\beta_3)^2 + (\alpha_0\beta_1 + \alpha_1\beta_0 + \alpha_2\beta_3 - \alpha_3\beta_2)^2 + (\alpha_0\beta_2 - \alpha_1\beta_3 + \alpha_2\beta_0 + \alpha_3\beta_1)^2 + (\alpha_0\beta_3 + \alpha_1\beta_2 - \alpha_2\beta_1 + \alpha_3\beta_0)^2$.

Proof. Of course there is one obvious proof of this result, namely, multiply everything out and compare terms.

However, an easier way both to reconstruct the result at will and, at the same time, to prove it, is to notice that the left-hand side is $N(x)N(y)$while the right-hand side is $N(xy)$ where $x = \alpha_0 + \alpha_1 i + \alpha_2 j + \alpha_3 k$ and $y = \beta_0 + \beta_1 i + \beta_2 j + \beta_3 k$. By Lemma 5.3.2, $N(x)N(y) = N(xy)$, ergo the Lagrange identity.

The Lagrange identity says that the sum of four squares times the sum of four squares is again, in a very specific way, the sum of four squares.

A very striking result of Adolf Hurwitz says that if the sum of n squares times the sum of n squares is again a sum of n squares, where this last sum has terms computed bilinearly from the other two sums, then $n = 1, 2, 4,$ or 8.

There is, in fact, an identity for the product of sums of eight squares but it is too long and cumbers some to write down here.

Now is the appropriate time to introduce the Hurwitz ring of integral quaternions.

Let $\zeta = \frac{1}{2}(1 + i + j + k)$and let

$$H = \{m_0\zeta + m_1 i + m_2 j + m_3 k \mid m_0, m_1, m_2, m_3 \text{ integers}\}.$$

LEMMA 5.3.4 H *is a subring of* Q. *If* $x \in H$ *then* $x^* \in H$ *and* $N(x)^*$ is *a positive* integer *for every nonzero* x *in* H.

We leave the proof of Lemma 5.3.4 to the reader. It should offer no difficulties.

In some ways H might appear to be a rather contrived ring. Why use the quaternions ζ? Why not merely consider the more natural ring $Q_0 = \{m_0 + m_1 i + m_2 j + m_3 k \mid m_0, m_1, m_2, m_3 \ integers\}$? The answer is that $Q_0$is not large enough, whereas H is, for the key lemma which follows tohold in it. But we want this next lemma to be true in the ring at our disposal for it allows us to characterize its left-ideals. This, perhaps, indicates why we (or rather Hurwitz) chose to work in H rather than in Q_0.

LEMMA 5.3.5 ***(LEFT-DIVISION ALGORITHM)*** *Let a and b be in H with $b \neq 0$. Then there exist two elements c and d in H such that $a = cb + d$ and $N(d) < N(b)$.*

Proof. Before proving the lemma, let's see what it tells us.

With Euclidean rings, we can see that Lemma 5.3.5 assures us that except for its lack of commutativity H has all the properties of a Euclidean ring.

The fact that elements in H may fail to commute will not bother us. True, we must be a little careful not to jump to erroneous conclusions; for instance $a = cb + d$ but we have no right to assume that $a$is also equal to $bc + d$, for b and c might not commute. But this will not influence any argument that we shall use.

In order to prove the lemma we first do so for a very special case, namely, that one in which a is an arbitrary element of H but b is a positive integer$n$.

Suppose that $a = t_0\zeta + t_1 i + t_2 j + t_3 k$ where t_0, t_1, t_2, t_3 are integers and that $b = n$ where n is a positive integer.

Let $c = x_0\zeta + x_1 i + x_2 j + x_3 k$where x_0, x_1, x_2, x_3 are integers yet to be determined. We want to choose them in such a manner as to force $N(a - cn) < N(n) = n^2$.

But $a - cn = \left(t_0\left(\frac{1+i+j+k}{2}\right) + t_1 i + t_2 j + t_3 k\right)$

$$-nx_0\left(\frac{1+i+j+k}{2}\right) - nx_1 i - nx_2 j - nx_3 k$$

$$= \frac{1}{2}(t_0 - nx_0) + \frac{1}{2}(t_0 + 2t_1 - n(t_0 + 2x_1))i$$

$$+ \frac{1}{2}\big(t_0 + 2t_1 - n(t_0 + 2x_2)\big)j + \frac{1}{2}(t_0 + 2t_3 - n(t_0 + 2x_3))k$$

If we could choose the integers x_0, x_1, x_2, x_3 in such a way as to make

$$|t_0 - nx_0| \leq \tfrac{1}{2}n, |t_0 + 2t_1 - n(t_0 + 2x_1)| \leq n, |t_0 + 2t_1 - n(t_0 + 2x_2)| \leq n, \text{and}$$
$$|t_0 + 2t_3 - n(t_0 + 2x_3)| \leq n$$

then we would have

$$N(a - cn) = \frac{(t_0 - nx_0)^2}{4} + \frac{\big(t_0 + 2t_1 - n(t_0 + 2x_1)\big)^2}{4} + \cdots$$

$$\leq \frac{1}{16}n^2 + \frac{1}{4}n^2 + \frac{1}{4}n^2 + \frac{1}{4}n^2 < n^2 = N(n),$$

which is the desired result. But now we claim this can always be done:

1. There is an integer x_0 such that $t_0 = x_0 n + r$ where $-\frac{1}{2}n \leq r \leq \frac{1}{2}n;$ for this x_0, $|t_0 - x_0 n| = |r| \leq \frac{1}{2}n.$
2. There is an integer k such that $t_0 + 2t_1 = kn + r$ and $0 \leq r \leq n$. If $k - t_0$ is even, put $2x_1 = k - t_0;$ then $t_0 + 2t_1 = (2x_1 + t_0)n + r$ and $|t_0 + 2t_1 - (2x_1 + t_0)n| = r < n.$ If, on the other hand, $k - t_0$ is odd, put $2x_1 = k - t_0 + 1;$ thus $t_0 + 2t_1 = (2x_1 + t_0 - 1)n + r = (2x_1 + t_0)n + r - n,$ whence $|t_0 + 2t_1 - (2x_1 + t_0)n| = |r - n| \leq n$ since $0 \leq r < n.$ Therefore we can find an integer x_1 satisfying $|t_0 + 2t_1 - (2x_1 + t_0)n| \leq n.$
3. As in part 2, we can find integers $x_2$and x_3 which satisfy $|t_0 + 2t_2 - (2x_2 + t_0)n| \leq n$ and $|t_0 + 2t_3 - (2x_3 \mp t_0)n| \leq n,$ respectively.

In the special case in which a is an arbitrary element of H and b is a positive integer we have now shown the lemma to be true.

We go to the general case where in a and b are arbitrary elements of H and $b \neq 0$. By Lemma 5.3.4, $n = bb^*$ is a positive integer; thus there exists $ac \in H$such that $ab^* = cn + d_1$ where $N(d_1) < N(n)$.

Thus $N(ab^* - cn) < N(n)$; but $n = bb^*$ whence we get $N(ab^* - cbb^*) < N(n)$, and so $N((a - cb)b^*) < N(n) = N(bb^*)$.

By Lemma 5.3.2 this reduces to $N(a - cb)N(b^*) < N(b)N(b^*)$; since $N(b^*) > 0$ we get $N(a - cb) < N(b)$

.Putting $d = a - cb$ we have $a = cb + d$ where $N(d) < N(b)$. This completely proves the lemma.

As in the commutative case we are able to deduce from Lemma 5.3.5.

LEMMA 5.3.6 *Let L be a left-ideal of H. Then there exists an element $u \in L$ such that every element in L is a left-multiple of u; in other words, there exists$u \in L$ such that every $x \in L$ is of the form $x = ru$ where $r \in H$.*

Proof. If $L = (0)$ there is nothing to prove, merely put $u = 0$.

Therefore we may assume that L has nonzero elements. The norms of the nonzero elements are positive integers (Lemma 5.3.4) whence there is an element $u \neq 0$ in L whose norm is minimal over the nonzero elements of L.

If $x \in L$, by Lemma 5.3.5, $x = cu + d$ where $N(d) < N(u)$.

However d is in L because both x and u, and so cu, are in Lwhich is a left-ideal. Thus $N(d) = 0$ and so $d = 0$. From this $x = cu$ is a consequence.

Before we can prove the four-square theorem, which is the goal of this section, we need one more lemma.

LEMMA 5.3.7 *If $a \in H$ then $a^{-1} \in H$ if and only if $N(a) = 1$.*

Proof. If both $a$and a^{-1} are in H, then by Lemma 5.3.4 both $N(a)$and $N(a^{-1})$ are positive integers.

However, $aa^{-1} = 1$, hence, by Lemma 5.3.2, $N(a)N(a^{-1}) = N(aa^{-1}) = N(1) = 1$.

This forces $N(a) = 1$. On the other hand, if $a \in H$ and $N(a) = 1$, then $aa^* = N(a) = 1$ andso $a^{-1} = a^*$. But, by Lemma 5.3.4, since $a \in H$ we have that $a^* \in H$, and so $a^{-1} = a^*$ is also in H.

We now have determined enough of the structure of H to use it effectively to study properties of the integers. We prove the famous classical theorem of Lagrange,

THEOREM 5.3.1 *Every positive integer can be expressed as the sum of squares of four integers.*

Proof. Given a positive integer n.

we claim in the theorem that $n = x_0^2 + x_1^2 + x_2^2 + x_3^2$ for four integers x_0, x_1, x_2, x_3.

Since every integer factors into a product of prime numbers, if every prime number were realizable as a sum of four squares, in view of Lagrange's identity (Lemma 5.3.3) every integer would be expressible as a sum of four squares.

We have reduced the problem to consider only prime numbers n. Certainly the prime number 2 can be written as $1^2 + 1^2 + 0^2 + 0^2$ as a sum of four squares.

Thus, without loss of generality, we may assume that $n$is an *odd prime number.* As is customary we denote it by p.

Consider the quaternions $W_p$over J_p, the integers $mod\ p$; $W_p = \{\alpha_0 + \alpha_1 i + \alpha_2 j + \alpha_3 k \mid \alpha_0, \alpha_1, \alpha_2, \alpha_3 \in J_p\}$. $W_p$is a finite ring; moreover, since $p \neq 2$ it is not commutative for$ij = -ji \neq ji$. Thus, by Wedderburn's theorem it cannot be a division ring, hence it must have a left-ideal which is neither (0) nor *wp:*

But then the two-sided ideal V in H defined by $V = \{x_0\zeta + x_1 i + x_2 j + x_3 k \mid p \; divides \; all \; of \; x_1, x_1, x_2, x_3\}$ cannot be a maximal left-ideal of H,since H/V is isomorphic to W_p. (Prove!) (If Vwere a maximal left-idealin $H, H/V$, and so W_p, would have no left-ideals other than (0) and$H/V)$.

Thus there is a left-ideal L of H satisfying: $L \neq H, L \neq V$, and $L \supset V$.

By Lemma 5.3.6, there is an element $u \in L$ such that every element in L is a left-multiple of u.

Since $p \in V$, $p \in L$, whence $p = cu$ for some $c \in H$. Since $u \notin V$, c cannot have an inverse in H, otherwise $u = c^{-1}p$ would be in V.

Thus $N(c) > 1$ by Lemma 5.3.7. Since $L \neq H, u$ cannot have an inverse in H, whence $N(u) > 1$. Since $p = cu, p^2 = N(p) = N(cu) = N(c)N(u)$. But $N(c)$and $N(u)$ are integers, since both $c$and u are in H, both are larger than 1 and both divide p^2. The only way this is possible is that $N(c) = N(u) = p$.

Since $u \in H$, $u = m_0\zeta + m_1 i + m_2 j + m_3 k$ where m_0, m_1, m_2, m_3 are integers; thus $2u = 2m_0\zeta + 2m_1 i + 2m_2 j + 2m_3 k = (m_0 + m_0 i + m_0 j + m_0 k) + 2m_1 i + 2m_2 j + 2m_3 k$

$$= m_0 + (2m_1 + m_0)i + (2m_2 + m_0)j + (2m_3 + m_0)k.$$

Therefore $N(2u) = m_0^2 + (2m_1 + m_0)^2 + (2m_2 + m_0)^2 + (2m_3 + m_0)^2$

But $N(2u) = N(2)N(u) = 4p$ since $N(2) = 4$and $N(u) = p$.

We have shown that $4p = m_0^2 + (2m_1 + m_0)^2 + (2m_2 + m_0)^2 + (2m_3 + m_0)^2$.

We are almost done.

To finish the proof we introduce an old trick of Euler's: If $2a = x_0^2 + x_1^2 + x_2^2 + x_3^2$ where a, x_0, x_1, x_2 and x_3 are integers, then $a = y_0^2 + y_1^2 + y_2^2 + y_3^2$ for some integers y_0, y_1, y_2, y_3.

To see this note that, since $2a$ is even, the x's are all even, all odd or two are even and two are odd. At any rate in all three cases we can renumber the $x's$ and pair them in such a way that

$$y_0 = \frac{x_0 + x_1}{2}, y_1 = \frac{x_0 - x_1}{2}, y_2 = \frac{x_2 + x_3}{2} \; and \; y_3 = \frac{x_2 - x_3}{2}$$

are all integers. But

$$y_0^2 + y_1^2 + y_2^2 + y_3^2 = \left(\frac{x_0 + x_1}{2}\right)^2 + \left(\frac{x_0 - x_1}{2}\right)^2 + \left(\frac{x_2 + x_3}{2}\right)^2 + \left(\frac{x_2 - x_3}{2}\right)^2$$

$$= \frac{1}{2}(x_0^2 + x_1^2 + x_2^2 + x_3^2)$$

$$= \frac{1}{2}(2a)$$

$$= a.$$

Since $4p$ is a sum of four squares, by the remark just made $2p$ also is; since $2p$ is a sum of four squares, p also must be such a sum.

Thus $p = a_0^2 + a_1^2 + a_2^2 + a_3^2$ for some integers $a_0, a_1, a_2, a_3$and Lagrange's theorem is established.

This theorem itself is the starting point of a large research area in number theory, the so-called *Waring problem.* This asks if every integer can be written as a sum of a fixed number of kth powers. For instance it can be shown that every integer is a sum of nine cubes, nineteen fourth powers, etc. The Waring problem was shown to have an affirmative answer, in this century, by the great mathematician Hilbert.

Problems

1. Prove Lemma 7.4.4.
2. Find all the elements $a$in Q_0such that a^{-1} is also in Q_0.

3. Prove that there are exactly 24 elements $a$in Hsuch that a^{-1} is alsoin H. Determine all of them.
4. Give an example of an $a$and b, $b \neq 0$, in Q_0such that it is impossibleto find $c$and $d$in Q_0satisfying $a = cb + d$where $N(d) < N(b)$.
5. Prove that if $a \in H$then there exist integers α, βsuch that$\alpha^2 + \alpha a + \beta = 0$.
6. Prove that there is a positive integer which cannot be written as thesum of three squares.
7. * Exhibit an infinite number of positive integers which cannot be written as the sum of three squares.

Study Learning Material Prepared by

Dr. S.N. Leena Nelson, M.Sc., M.Phil., Ph.D.

Associate Professor & Head, Department of Mathematics,

Women's Christian College, Nagercoil – 629 001,

Tamil Nadu, India.