sex, guns, and theorems

THE LEGACY OF ÉVARISTE GALOIS

by

DANIEL M. R. BETTENDORF

Honors in Mathematics
Robert S. Johnson, Advisor
Washington and Lee University
Spring, 1991

sex, guns, and theorems

THE LEGACY OF ÉVARISTE GALOIS

by

DANIEL M. R. BETTENDORF

Honors in Mathematics
Robert S. Johnson, Advisor
Washington and Lee University
Spring, 1991

INTRODUCTION

I

Only ignorance of history can allow one to see mathematicians as those who lead boring, uneventful lives, and a brief look at the career of the French mathematician Évariste Galois (1811 - 1832) will put any skeptic to shame. Galois' life was - even without the mythological romanticization which usually surrounds it - unquestionably one of great passion and intrigue. He was haughty, brilliant, a rebel with a cause, and he died gallantly at a young age in a duel over the honor of a certain young woman. Or so the story goes.

Actually, it is not entirely clear what happened to Galois or what the circumstances surrounding the duel were. The highly romanticized version offered by E.T. Bell [2] in which Galois frantically wrote down most of his discoveries the night before the duel is verifiably untrue; yet, Tony Rothman's efforts to render the circumstances of his death commonplace and to underrate tremendously the importance of the letter to Galois' friend August Chevalier written the night before the duel also provide a flawed perspective [7]. At this point I shall try to give what is to my knowledge the most accurate account of the events surrounding his life and death, based largely on remarks by Ian Stewart [8].

Galois was born near Paris at Bourg-la-Reine on October 25, 1811. His father was active in local politics and later became mayor of the town. His mother had a strong classical education and a degree of skepticism regarding established religion. The parents' liberal political sentiments undoubtedly had an influence on Galois' later participation in rebel causes. Galois was educated first by his mother, then at the *lyceé* Louis-le-Grand. He showed himself to be a very good student, but at some point he became bored with his classical studies and obsessed with advanced mathematics, beginning with the original writings of Legendre and Abel. His mathematical genius was evident to him and he wished to pursue a career as a mathematician; consequently, he tried to enter the École Polytechnique. Lacking some basic mathematics, he failed the entrance exam and was forced to attend the École Normale.

By the time he entered this school in 1828, he had already completed some significant mathematical work and tried to have it recognized. In this same year he did publish a minor paper on continued fractions, but he was also upset by the fate of a memoir he had sent to Cauchy. There are various speculative accounts of what happened to the work, but what is certain is that it was never seen again. In 1829 his father committed suicide after a series of village disputes allegedly involving the parish priest. This loss served to augment his already passionate hatred of the royalist government.

In the following year he submitted his researches again, this time as a candidate for the highly coveted Grand Prize in Mathematics from the Academy of Sciences. Galois modestly observed: "I have carried out researches which will halt many savants in theirs" [2, p.371]. The Academy's secretary, Fourier, took them home and died. Galois' papers were not found. By now Galois was convinced there was more than chance involved in the neglect of genius: "Genius is condemned by a malicious social organization to an eternal denial of justice in favor of fawning mediocrity" [Ibid]. In a stroke of incredible illogic he seems to have concluded that the Bourbon regime was somehow at fault.

Bearing witness to the maxim "Hope springs eternal," Galois submitted yet another memoir to the Academy in January of 1831. After hearing nothing, he wrote to the President, but there was still no reply. He then joined the artillery of the National Guard, a republican force, but it was disbanded soon thereafter by royal order. Apparently, however, Galois did not relinquish his uniform, for he was later arrested for wearing it in a Bastille Day demonstration and imprisoned for six months. His participation in this illegal march followed by 10 days the verdict of the Academy concerning his paper: it was too messy to be intelligible and therefore could not properly be considered. News like this must have convinced him that his career lay in furthering the anti-establishment cause. Here public recognition came with greater ease: the official newspapers announced that the government had captured "the dangerous republican, Évariste Galois."

Galois was transferred to a hospital during a cholera epidemic. He was soon paroled, and he then began his one and only love-affair with a woman whose name had remained a mystery until recently. She was Stephanie du Motel, the daughter of a perfectly respectable physician. It seems that she had been trying to break off the affair, and one cannot help but wonder if Galois was not trying to get himself killed. Indeed, while Galois was in prison he predicted - in a drunken stupor forced on him by his less abstemious peers - that he would die in a duel over a woman of little worth. Although the woman was not, as far as any historical evidence indicates, of little worth, Galois did fight a duel ostensibly over the honor of this woman. However, some of his own remarks indicate he was not very happy about it.

We must pause here to consider the two accounts for the circumstances of the duel. It is thought by some that this duel was really a political one and the romantic element was a front, but there is more evidence to support the idea that it was exactly as it appeared: a young man dying for the honor of the woman he is supposed to have loved. His own remarks seem to bear this claim out, and sound scholarship indicates that his opponent was also a republican.

Bell does indeed turn every facet of this tale into full-blown melodrama [2], but it is important to note that Galois did write important discoveries to August Chevalier the night before the duel. These discoveries were in large part already in Galois' intellectual arsenal, but they had not been properly recognized. It is in this document where many of his memorable and pathetic remarks originate, such as "I have no time" and "I die the victim of an infamous coquette." As Galois recorded these researches of his he must have been terribly distraught: it was, after all, only hours before he was to walk 25 paces with a pistol in hand, only to turn and fall to the ground with a bullet in his abdomen. Indeed, it has been observed by some cynical students that Galois might have fared better in his fatal duel had he not spent so much time on abstract mathematics the night before.

II

Now let us consider the mathematical content of his work, the subject of the letter which he did indeed compose the night before his fateful encounter with a fellow rebel. The matter which drives most of his important work considered here surrounds the question of the solubility of the quintic. For a great number of years mathematicians suspected that there was a formula for solving the fifth-degree equation over the rationals, since such formulas had been found for second, third and even fourth-degree equations. However, Lagrange's work with resolvents gave some hint that perhaps there was no general formula, or perhaps there existed some equations which did not admit solutions even with the use of ordinary radicals.

Abel put this question to rest in 1824 (although Ruffini had more or less done so at an earlier date without proper acknowledgment from the mathematical world), but Galois' work is more significant for two reasons: (1) in it lies an enormous body of seminal research in two major branches of modern abstract algebra, and (2) it is the chief subject of this paper.

Also, Galois was primarily concerned with finding the precise conditions under which a given polynomial could be solved by radicals. His approach involved the consideration of the permutation groups of the zeros of polynomials and the idea of a general polynomial, a concept which will be discussed later on. The approach of this paper, however, is a much more modern one, taking into account the work that Galois did and using the theory in its entirety to answer the above question, as well as others, and examine the consequences of his discoveries. This manner of dealing with great theories of the past is not uncommon; indeed, although the name stays with a theorem, the method of proof and the preparation which precedes typically differ from the author's original work.

It is now appropriate to begin a technical discussion of some of the ideas necessary to understand the Galois theory as presented in this thesis. This presentation assumes a knowledge of the basic concepts of abstract algebra, the theory of groups, rings and fields. What follows is a brief review of some of the fundamentals of the theory of field extensions which shall serve as a point of departure for the material in this paper.

Recall that any field E such that $F \subseteq E$ is called an *extension* of F. An extension E:F can be formed by "attaching" elements not in F to F. For instance, for some $\alpha \notin F$ $F(\alpha)$:F is an extension of F, where the field $F(\alpha)$ is comprised of all rational expressions involving powers of α. $F(\alpha)$:F is said to be a *simple* extension because only it is generated by attaching only one element. If α is a zero of a polynomial over F, these expressions are restricted by the degree of the said polynomial, as we note below. In this case α is said to be *algebraic* over F; in general, an algebraic extension of F is one in which every element is algebraic over F. If α is not algebraic, it is *transcendental* over F; similarly, an extension of F which is not algebraic is called transcendental. Of course, one may attach an element β to $F(\alpha)$ to obtain a simple extension $F(\alpha,\beta)$:$F(\alpha)$ or a double extension $F(\alpha,\beta)$:F, and so forth.

An extension E of a field F can be viewed as a vector space over F; the *degree* [E:F] of E over F is the dimension of this vector space. In the case of a simple algebriac extension $F(\alpha)$:F, every element of $F(\alpha)$ is uniquely expressible in the form $a_{k-1}\alpha^{k-1} + \cdots + a_0$ where $a_i \in F$ and k is the degree of the unique (monic) irreducible polynomial over F for which α is a solution (called the *minimum polynomial for* α). It should be clear that

$[F(\alpha):F]$ is the degree of the minimum polynomial for α over F. A transcendental extension always has infinite degree over F, and an algebraic extension can have infinite degree as well.

In this paper all fields are, unless otherwise indicated, of characteristic zero, and the field over which a given polynomial is written shall be obvious from the context.

Since we are primarily concerned with fields constructed from the zeros of polynomials, we are obviously interested in the *splitting field* of a given polynomial over F: the smallest extension of F containing all the zeros of the polynomial. (Splitting fields are unique up to isomorphism.) Let us familiarize ourselves with these concepts by way of example.

Consider the polynomial $x^2 - 2$ over $\mathbf{Q}$. Its splitting field is quite obviously $\mathbf{Q}(\sqrt{2})$. Clearly, $[\mathbf{Q}(\sqrt{2}):\mathbf{Q}] = 2$. Similarly, we may derive the splitting field $\mathbf{Q}(i)$ for $x^2 + 1$ over $\mathbf{Q}$, where the degree of the extension is also two. It is natural to look at the extension $\mathbf{Q}((\sqrt{2})(i)) = \mathbf{Q}(\sqrt{2},i)$ and recall that the degree of this extension is 4 by the "Tower Rule," that is $[\mathbf{Q}(\sqrt{2}, i):\mathbf{Q}] = [\mathbf{Q}(\sqrt{2}, i)): \mathbf{Q}(\sqrt{2})][\mathbf{Q}(\sqrt{2}):\mathbf{Q}]$. It is interesting to note that $\mathbf{Q}(\sqrt{2}, i)$ can be represented as a simple algebraic extension, $\mathbf{Q}(\frac{\sqrt{2} + \sqrt{2}i}{2})$. Actually, any finite algebraic extension can be reduced to a simple one. In our example this is accomplished by letting $x = \frac{\sqrt{2} + \sqrt{2}i}{2}$ and building up from there: we see that $x^4 + 1$ is the minimum polynomial, determining the irreducibility by considering $(x + 1)^4 + 1$ and using Eisenstein's criterion with $p = 2$. This result shows that $[\mathbf{Q}(\frac{\sqrt{2} + \sqrt{2}i}{2}):\mathbf{Q}] = 4$, which makes the above equivalence believable. If we wish to make it more than believable, we notice that $\mathbf{Q}(\frac{\sqrt{2} + \sqrt{2}i}{2}) \subseteq \mathbf{Q}(\sqrt{2}, i)$. Since each of these fields has the same (finite) degree over $\mathbf{Q}$, they are identical.

This technical review should have sufficiently whetted the reader's appetite, and we shall now begin the formal exploration of the fascinating subject of the theory of field extensions, beginning with the presentation of the Fundamental Theorem.

I. THE FUNDAMENTAL THEOREM

For the moment, let us lay aside the question of the solubility of the quintic and consider wherein lies the real value of the theory behind the work. The idea is to set up a correspondence between the intermediate fields of certain field extensions and the groups of automorphisms which fix these fields: finite groups, especially those of small order, are far more tractable than intermediate fields, as we shall soon see. A few definitions are evidently in order. Recall that an isomorphism is a bijective mapping from one field (or ring) to another which preserves both operations.

Definition An isomorphism from a field K onto itself is called an *automorphism*. Given an extension L of K we define a *K-automorphism of L* to be an automorphism ϕ of L which fixes K; that is, $\phi : L \rightarrow L$ with $\phi(k) = k$ $\forall\ k \in K$.

It should be clear that such automorphisms form a group under function composition and inversion. We call this group for a given field extension the *Galois group* for the extension and usually denote it by the letter G. It will be clear from the context which field extension the Galois group corresponds to; if need be we write $G = \Gamma(F{:}K)$ where F is an extension of K. For a subgroup H of G we may associate a given intermediate field of our extension which H fixes, and that field is called the *fixed field of H*, denoted here by $H^\dagger$. Not surprisingly, for each intermediate field there is a corresponding subgroup of automorphisms which fix that field: just consider the extension to be over the intermediate field and apply the above principle. We shall denote such a group corresponding to the intermediate field I by I^*. Note that these operations are inclusion-reversing; that is, $I \subseteq K$ implies $K^* \subseteq I^*$ and similarly for †. Moreover, $I^{*\dagger} \subseteq I$ and $H^{\dagger *} \subseteq H$. But the real point of interest is to determine under which conditions these relations are inverses of one another.

Before we begin to explore these conditions, it is important to introduce a powerful theorem.

Theorem For a finite field extension $K(\alpha)$:K, where m is the minimum polynomial for α and β is any other zero of m, there is a unique isomorphism from $K(\alpha)$ to $K(\beta)$ leaving K fixed and mapping α to β. Moreover, if α is in some extension of E of K and α is a zero of some polynomial over K, then any K-automorphism of E maps α to a zero of that polynomial.

The proof of this theorem follows immediately from the form of the elements in the extension fields: one merely replaces one zero by another to obtain the 'new' isomorphic field, while fixing the coefficients in K, of course. To verify that this mapping is indeed an isomorphism is tedious and unenlightening, albeit routine. For the second part let f be a polynomial over K with $f(\alpha) = 0$, then $f(\phi(\alpha)) = \phi(f(\alpha)) = 0$, where ϕ is any K-automorphism.

As an example, consider the extension $\mathbf{Q}(\alpha)$:$\mathbf{Q}$ where $\alpha = \sqrt[5]{2}$. Now the Galois group for this extension is evidently $\{e\}$, because we must map zeros of the minimum polynomial to other zeros. In this case m is $x^5 - 2$ and, since $\mathbf{Q}(\alpha) \subseteq \mathbf{R}$, G contains only the identity element, because for any $\phi \in G$, $\phi(\alpha)^5 = \phi(\alpha^5) = 2$, and there is only one real fifth root of 2. Thus $\mathbf{Q}^* = G = \{e\}$ but $G^\dagger = \mathbf{Q}^{*\dagger} = \mathbf{Q}(\alpha)$.

Our goal is to avoid such results and achieve a one-to-one correspondence between the intermediate fields and the subgroups of the Galois group. Our intuition should tell us that in order to achieve such a result, we need to have *all* the roots of the minimum polynomial appear in the extension field under consideration. This guess is indeed correct, and it leads us to define a new term, one which introduces a key concept in the hypotheses of the Fundamental Theorem.

Definition An extension F:K is said to be *normal* if whenever any irreducible polynomial over K has a zero in F then it splits in F.

This definition provides us with the last needed ingredient for the Fundamental Theorem. The reader should suspect that splitting fields for a given polynomial over K are normal extensions of K; indeed, it is true that an extension of K is normal and finite if and only if it is a splitting field for some polynomial over K.[1] We are now ready to present the following theorem.

Theorem The Fundamental Theorem of Galois Theory
Given a field K of characteristic 0, a normal extension F of K, with Galois group G, and the relations *, † as defined above

1. $|\Gamma(F:K)| = [F:K]$;
2. There is a one-to-one, inclusion reversing correspondence - given by * and † - between the intermediate fields of F:K and the subgroups of the Galois group;
3. If M is an intermediate field then $|M^*| = [F:M]$;
4. H is a normal subgroup of G if and only if $H^\dagger$ is a normal extension of K;
5. If an intermediate extension M of K is normal then $\Gamma(M:K)$ is isomorphic to the factor group G/M^*.

The Fundamental Theorem is largely a tool and thus its real beauty lies not so much in its statement as in its application; as one might suspect, the proof, though making use of many techniques in basic abstract algebra, is not intrinsically beautiful. In my judgment Part 1 is the most interesting, and for this reason we shall look at the development of its proof. From this discussion Part 3 will be an apparent consequence of Part 1. Part 2 has already been made credible in a highly informal way, but we shall soon be in a position to prove it rigorously. The proof of Part 5 is given because of its simplicity and its use of basic concepts from elementary group theory.

We begin by stating a theorem whose proof - which we shall omit for reasons of space - relies on some basic group theory and the theorem by Dedekind which shows distinct monomorphisms to be linearly independent over the base field.

Theorem Given a subgroup H of the group of automorphisms on a field K,
$[K:H^\dagger] = |H|$.

[1] It should also be noted that 'separability' - the condition that there be no multiple roots- is a needed hypothesis in the Fundamental Theorem, but since all irreducible polynomials are separable over fields of characteristic 0 and we are dealing largely with such fields, a discussion of this hypothesis is formally omitted from this paper.

We will also need the following technical result.

Lemma If L:K is a finite, normal extension, then every K-monomorphism τ of L is also a K-automorphism of L.

Proof τ is a linear map from the vector space L over K into itself and is injective. Since L is a finite-dimensional vector space over K and we have an injection from it into itself, we know that it is also a surjection. Hence τ is a K-automorphism of L.

We are now in a position to prove the theorem which is the key to parts 1 and 2 of our Theorem above.

Theorem If L:K is a finite, normal extension of degree n, then there are precisely n K-monomorphisms of L.

Proof The proof is by induction on n. The case [L:K] = 1 is obvious. Now choose $\alpha \in L \backslash K$ where m is the minimum polynomial for α over K. There are, by induction, precisely r $K(\alpha)$-monomorphisms ρ_j of L where $r = [L:K(\alpha)] = \dfrac{n}{[K(\alpha):K]}$ by the Tower Law. From the first theorem in this section, there are $[K(\alpha):K] = s$ K-monomorphisms τ_i of L. Combining the two, we have n = rs distinct K- monomorphisms of the form $\tau_i\rho_j$. To see that these monomorphisms exhaust the possibilities, we shall take an arbitrary K-monomorphism $\phi: L \rightarrow L$ and show that it is of the above form. Note that $0 = \phi(m(\alpha)) = m(\phi(\alpha))$. So $\phi(\alpha) = \alpha_k$, where α_k is some zero of m. Then $\tau_k^{-1}\phi$ (where τ_k maps α to α_k) sends α to α and is therefore, by induction, some ρ_j. Then we have $\rho_j = \tau_k^{-1}\phi$ or $\phi = \tau_k\rho_j$.

Now it is clear that Part 1 of the Fundamental Theorem is proved, because each of the above monomorphisms is also an automorphism by the lemma. For similar reasons, Part 2 of the Theorem is now more than just credible, but we shall forego the proof because the technicalities are more cumbersome than interesting. As promised, the proof of Part 5 appears below. First we mention a relevant fact without proof: for a normal extension L:K and an intermediate field M any K-monomorphism from M into L can be extended to a K-automorphism of L.

Proof of part 5

Let G' be the Galois group of an intermediate field M which is a normal extension of K. Define a mapping ϕ from G to G' such that $\phi(\tau) = \tau|_M$ $\forall\ \tau \in G$. Now $\tau|_M$ is a K-automorphism of M by the lemma above, so ϕ is a group homomorphism. It is surjective by the fact above. It should be clear that ker $\phi = M^*$, so by standard group theory we have G' = image of $\phi \approx G/\ker \phi = G/M^*$.

The best way to understand the Theorem and see its real beauty is to look at a specific example. The example which follows is a standard one according to Stewart's book on the Galois theory.

Consider the polynomial $t^4 - 2$ over **Q**. It is easy enough to see that the roots of the polynomial are $\pm \sqrt[4]{2}$ and $\pm i\sqrt[4]{2}$. With the notation $\alpha = \sqrt[4]{2}$, it should be clear that the splitting field for this polynomial is K = **Q**(α,i). Now we explore the Galois correspondence. The degree of K over **Q** is, by the Tower Rule, equal to [**Q**(α,i):**Q**(α)][**Q**(α):**Q**]. Now [**Q**(α):**Q**] is obviously 4, since $t^4 - 2$ is the minimum polynomial for α over **Q**, and $t^2 + 1$ is still irreducible over **Q**(α) and hence is the minimum polynomial for i over **Q**(α). So the degree of the splitting field over **Q** is $2 \cdot 4 = 8$. By the Theorem, we should hope to find that there are precisely eight **Q**-automorphisms of K. These **Q**-automorphisms can be found by considering two obvious 'root' automorphisms, namely ρ which sends i to -i and leaves α fixed, and τ which sends α to iα and leaves i fixed. We then build up the others by taking suitable combinations, and, as is indicated in the table below, there are exactly 8 of them.

Automorphism	*Effect on α*	*Effect on i*
e	α	i
τ	$i\alpha$	i
τ^2	$-\alpha$	i
τ^3	$-i\alpha$	i
ρ	α	-i

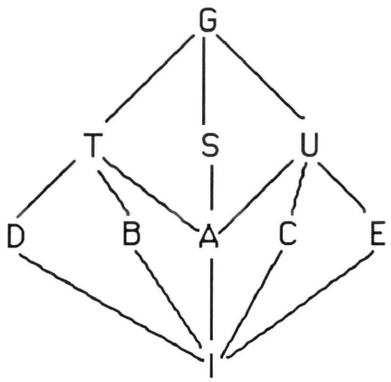
$\tau\rho$	$i\alpha$	$-i$
$\tau^2\rho$	$-\alpha$	$-i$
$\tau^3\rho$	$-i\alpha$	$-i$

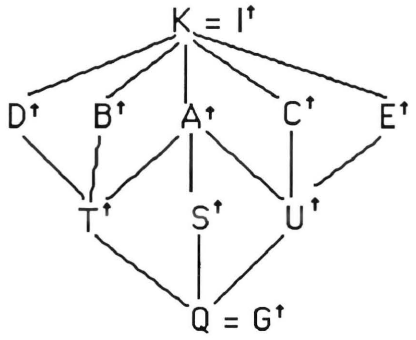
Other products do not give new automorphims since $\tau^4 = \rho^2 = e$ and $\tau^3\rho = \rho\tau$. In fact, these relations serve as a complete description of the abstract structure of the Galois group. They tell us how to multiply two elements in the group by showing how to move τ's 'to the left' and ρ's 'to the right.' From this generator-relation description we deduce that the Galois group is the dihedral group $\mathbf{D}_4$ of permutations on a square. It should seem reasonable that the Galois group be some kind of permutation group; after all, the idea is to find automorphisms which permute the zeros of given polynomials irreducible over the base field. Were it a simple case like the five fifth-roots of unity, one would expect it to be an abelian group, the rotations of a regular pentagon, for instance. This is exactly the case. In our current example, we have two zeros with different minimum polynomials; hence we expect complications. These complications arise in the structure of the group by adding in the 'flips' with the rotations to take into account the interplay between the zeros.

Now we shall find the subgroups of the Galois group. They are

Order 8:	$G \approx \mathbf{D}_4$
Order 4:	$S = \{e, \tau, \tau^2, \tau^3\} \approx \mathbf{Z}_4$
	$T = \{e, \tau^2, \rho, \tau^2\rho\} \approx \mathbf{Z}_2 \times \mathbf{Z}_2$
	$U = \{e, \tau^2, \tau\rho, \tau^3\rho\} \approx \mathbf{Z}_2 \times \mathbf{Z}_2$
Order 2:	$A = \{e, \tau^2\} \approx \mathbf{Z}_2$
	$B = \{e, \rho\} \approx \mathbf{Z}_2$
	$C = \{e, \tau\rho\} \approx \mathbf{Z}_2$
	$D = \{e, \tau^2\rho\} \approx \mathbf{Z}_2$
	$E = \{e, \tau^3\rho\} \approx \mathbf{Z}_2$
Order 1:	$\{e\}$

We make a few observations before we juxtapose two lattice diagrams which graphically exhibit the connection between the intermediate fields and the subgroups of the Galois group. First, we note that the index of the subgroup in the Galois group is identical to the degree of the corresponding extension. This fact follows directly from Part 3 of the Fundamental Theorem. Second, notice that one diagram will appear to be 'same' as the other one yet inverted. This connection is obvious but no less important to note because of that. Third, notice that at this point we do not yet know what the intermediate fields are, but we know they must exist by the Theorem. It is very difficult in general to find intermediate fields, hence the usefulness of the Theorem.





Despite the neat categorization of fields the graphic representation above appears to provide, we must look at how to find these intermediate fields in order to illustrate the value of the theorem. Note that corresponding to the three subgroups of order four there are three fairly obvious subfields of K with degree two over **Q**, namely $\mathbf{Q}(\sqrt{2})$, $\mathbf{Q}(i)$, and $\mathbf{Q}(i\sqrt{2})$. These subfields correspond to the fixed fields $U^\dagger$, $S^\dagger$, and $T^\dagger$, and it is clear enough that this is true. Consider $S^\dagger$, for instance. The elements of S are all powers of τ which all leave i fixed but change α, so $S^\dagger$ is evidently $\mathbf{Q}(i)$. There are similarly transparent explanations for the other fields of degree 2.

The case of the remaining intermediate fields is another matter. We shall find one of them, namely $C^\dagger$, in order to suggest an approach for finding them in general. Note that any element x in K can be expressed in the form

$$x = a_0 + a_1\alpha + a_2\alpha^2 + a_3\alpha^3 + a_4 i + a_5 i\alpha + a_6 i\alpha^2 + a_7 i\alpha^3$$

where $a_i \in \mathbf{Q}$.

Then $\tau\rho(x) = \tau\rho(a_0 + a_1\alpha + a_2\alpha^2 + a_3\alpha^3 + a_4 i + a_5 i\alpha + a_6 i\alpha^2 + a_7 i\alpha^3)$

$$= a_0 + a_5\alpha - a_2\alpha^2 - a_7\alpha^3 - a_4 i + a_1 i\alpha + a_6 i\alpha^2 - a_3 i\alpha^3$$

And so x is fixed by $\tau\rho$ (and hence by C) if and only if the following relations hold.

$a_0 = a_0$, $a_1 = a_5$, $a_2 = -a_2$, $a_3 = -a_7$, $a_4 = -a_4$, $a_5 = a_1$, $a_6 = a_6$, and $a_7 = -a_3$

So a_0 and a_6 are arbitrary, while $a_4 = a_2 = 0$ and $a_3 = -a_7$, whence it follows that

$$\begin{aligned} x &= a_0 + a_1\alpha + a_3\alpha^3 + a_1 i\alpha + a_6 i\alpha^2 - a_3 i\alpha^3 \\ &= a_0 + a_1(\alpha + i\alpha^2) + a_3(\alpha^3 - i\alpha^3) + a_6 i\alpha^2 \\ &= a_0 + a_1(1+i)\alpha + \frac{a_6}{2}\{(1+i)\alpha\}^2 - \frac{a_3}{2}\{(1+i)\alpha\}^3 \end{aligned}$$

Thus $C^\dagger = \mathbf{Q}((1 + i)\alpha)$.

Now it is also easy enough to use this example to illustrate the last two parts of the Fundamental Theorem, but the primary focus of this paper is on the first three parts and shall remain so. In any event, the above should make the importance of the theorem as a tool quite clear.

II. THE INSOLUBILITY OF THE QUINTIC

Recall that the motivation for the invention of the Galois theory was to answer the question of the solubility of a polynomial of fifth degree. Although Abel (and Ruffini) had proved before Galois that there was no general formula for the zeros of a quintic, it was Galois' work which determined the precise conditions under which the zeros of a polynomial could be expressed by radicals. The purpose of this section is to discuss what those conditions are and prove the quintic to be insoluble.

Before embarking on this journey we must consider exactly what we mean by saying the quintic is 'insoluble.' There are really two approaches, one involving the so-called 'general polynomial,' a term whose highly specialized significance renders it a misnomer, and another which displays a particular polynomial over **Q** whose zeros cannot be expressed as radicals. The first result is in some sense stronger because it will show that there is no general formula for all polynomials of any degree greater than 4; however, it is weaker in that it does not show that the zeros of some given polynomial are not expressible by radicals.

In order to consider both of these approaches it is necessary to make all these notions rigorous. The strategy will be to look at how to define 'expressible by radicals' and then move on to the question of using such definitions and some facts about soluble groups to determine, with the help of the Fundamental Theorem, which polynomials are soluble.

Definition A *radical extension* of a field K is one of the form $K(\alpha_1, \alpha_2, \ldots, \alpha_k)$ where $\alpha_i^{n(i)} \in K(\alpha_1, \alpha_2, ..., \alpha_{i-1})$, for some positive integer n(i).

A zero of a polynomial is therefore *expressible by radicals* if it is in some radical extension of the base field. It should be clear that this definition is the equivalent of the ordinary sense of the phrase "expressible by radicals." Consider an example of a zero expressible by radicals over a field K. Such a zero would be a combination of elements of K under the operations of addition, subtraction, multiplication, division and the extraction of roots. For instance, $\sqrt[5]{1 - \sqrt[3]{2+\sqrt{7}}}$ is expressible by radicals over **Q**, and the following series of extensions ends in the necessary radical extension of **Q**.

$$\mathbf{Q} \subseteq \mathbf{Q}(\sqrt{7}) \subseteq \mathbf{Q}(\sqrt{7}, \sqrt[3]{2 + \sqrt{7}}) \subseteq \mathbf{Q}(\sqrt{7}, \sqrt[3]{2 + \sqrt{7}}, \sqrt[5]{1 - \sqrt[3]{2+ \sqrt{7}}})$$

It is also important to note that if an irreducible polynomial has one root expressible by radicals then the other roots are also. To see this we need the following.

Lemma If $K(\alpha_1, \alpha_2, ..., \alpha_r)$ is a radical extension of the field K, then any normal closure of this extension (i.e., the smallest normal extension of K) is also radical.

Proof Let $L = K(\alpha_1, \alpha_2, ..., \alpha_r)$ be a radical extension with $\alpha_i^{n(i)} \in K(\alpha_1, ..., \alpha_{i-1})$. Let f_i be the minimum polynomial for α_i. Clearly the normal closure N of L:K is the splitting field of $\Pi_{i=1}^{r} f_i$. So $N = K(\alpha_1, \beta_{11}, \beta_{12}, ..., \beta_{1m(1)}, \ldots, \alpha_r, \beta_{r1}, \ldots, \beta_{rm(r)})$ where β_{ik} are the other zeros of f_i. Now by an earlier theorem $\beta_{ik}{}^{n(i)} = \phi(\alpha_i)^{n(i)} = \phi(\alpha_i{}^{n(i)}) \in K(\alpha_1, ..., \alpha_{i-1})$ for some $K(\alpha_1, ..., \alpha_{i-1})$- automorphism ϕ. Hence N is a radical extension of K.

Now consider an irreducible polynomial f with a zero θ expressible by radicals over K. Then θ is in some radical extension of K, and, since the normal closure of such an extension is radical (by the above lemma), all other zeros are expressible by radicals.
It should be clear how the next definition represents the appropriate condition under which the zeros of a polynomial can said to be expressible by radicals.

Definition A polynomial over a field K is said to be *soluble by radicals* if its zeros lie in a radical extension of K.

Thus a polynomial is soluble by radicals if its zeros are merely combinations of roots of any degree using the normal algebraic operations of a field.

We now turn to look at soluble groups before we draw the connection between them and radical extensions.

Definition A group G is said to be *soluble* if there exists a series of subgroups

$\{e\} = N_1 \subseteq N_2 \subseteq \ldots \subseteq N_k = G$, each normal in the one following it, such that each factor group N_i/N_{i-1} is abelian.

Clearly every abelian group is soluble. Also, subgroups of soluble groups are soluble. (That claim does not follow directly from the definitions, but its proof is too far afield to discuss in this paper.) It can be shown that S_3 and S_4 are both soluble, but it is an extremely important fact that S_n is not soluble for $n \geq 5$; indeed, it is the key to answering the question central to the origin of the Galois theory. We shall show this to be true before developing a relationship between the solubility of Galois groups and the solubility of polynomials by radicals. In order to do this a more manageable criterion is needed for the solubility of a group.

Definition Let a, b be elements in a group G. The *commutator* of two elements a and b of G is the element $a^{-1}b^{-1}ab$. We may take all elements of this form and generate a subgroup of G which we call the *commutator subgroup* G' of G.

We note that G' is a normal subgroup of G, the factor group G/G' is abelian, and that any normal subgroup M of G such that G/M is abelian is a supergroup of G'. Also, $G^{(k)}$, the commutator subgroup of $G^{(k-1)}$, is normal in G as well. (The zealous reader can verify these facts quite easily from the definitions.) It turns out these ideas provide us with a simple criterion for the solubility of a group.

Theorem G is soluble if and only if $G^{(k)} = \{e\}$ for some k.

Proof If $G^{(k)} = \{e\}$ for some k then we may let the chain of commutator subgroups serve as the series of normal subgroups. It follows directly from the above that such a series produces factor groups which are abelian. Now suppose G is soluble. Then there is a series of normal subgroups $\{e\} = N_0 \subseteq N_1 \subseteq \ldots \subseteq N_k = G$ such that N_i/N_{i-1} is abelian. Thus $N_i' \subseteq N_{i-1}$, and we may write $G' = N_k' \subseteq N_{k-1}, \ldots, G^{(i)} = N'_{k-i+1} \subseteq N_{k-i}, \ldots, G^{(k)} = N_1' \subseteq N_0 = \{e\}$, and the claim follows.

Corollary The homomorphic image of a soluble group is soluble.

Now we use these facts to show the following.

Lemma If H is a subgroup of S_n $(n \geq 5)$ containing every 3-cycle, N is a normal subgroup of H and H/N is abelian, then N contains every 3-cycle.

Proof Let f be the natural homomorphism from H to H/N. Now let $x = (r,s,t)$ and $y = (t,u,v)$ be elements of H. Then $f(x^{-1}y^{-1}xy) = (x')^{-1}(y')^{-1}x'y' = 1$ so $x^{-1}y^{-1}xy \in N$. But $x^{-1}y^{-1}xy = (t,s,r)(v,u,t)(r,s,t)(t,u,v) = (t,u,r)$, and this is the case for any t, u, and r, so N contains every 3-cycle.

Theorem S_n is not soluble for $n \geq 5$.

Proof If S_n were soluble there would be a series of normal subgroups producing abelian factor groups, but these subgroups would always contain 3-cycles by the above lemma and could never be the trivial subgroup.

The connection between radical extensions and soluble Galois groups is the next step in our journey towards proving the quintic insoluble. First we need to prove a technical lemma.

Lemma The Galois group G of the polynomial[2] $p(x) = x^n - a$ over K, $a \in K$, is abelian.

Proof It is clear that the splitting field for p over K is $K(\sqrt[n]{a}, \omega)$ where ω is the primitive n-th root of unity. Any element ϕ of G maps one root to another, so we may classify all elements of G as $\phi_i(\sqrt[n]{a}\omega) = \sqrt[n]{a}\omega^i$. Then $\phi_i\phi_j(\sqrt[n]{a}\omega) = (\sqrt[n]{a}\omega^j)^i = (\sqrt[n]{a}\omega^{j+i}) = (\sqrt[n]{a}\omega^i)^j = \phi_j\phi_i(\sqrt[n]{a}\omega)$. Hence G is abelian.

Now we are ready for the main theorem linking solubility of polynomials with the solubility of their corresponding Galois groups. Although the theorem states that these are equivalent conditions, we shall prove only that the group must be soluble if the polynomial is, since that is all that is necessary for the given task (and because it is a great deal less complicated). There is one assumption which is necessary to make the proof cleaner, namely that the base field K has all the "necessary" roots of unity. Once the proof is

[2] The Galois group G of a polynomial p over K has the obvious meaning; that is, G is the group of K-automorphisms of the splitting field of p over K.

finished the reader should note that such an assumption is harmless since the method could be extended to account for these roots of unity were they not already in the base field.

Theorem A polynomial p over a field K is soluble by radicals if and only if its Galois group is soluble.

Proof (Necessity only.) Let F be the splitting field for the polynomial p over K. Now F is a radical extension of K, thus there is a chain of fields $K = F_0 \subseteq F_0(\alpha_1) = F_1 \subseteq F_1(\alpha_2) = F_2 \subseteq \ldots \subseteq F_k(\alpha_{k+1}) = F$ such that $\alpha_i^{n(i)} \in F_{i-1}$ for some $n(i) \in \mathbf{N}$. Note that each intermediate extension is normal since it is a splitting field over K and therefore, by the Fundamental Theorem, each of the corresponding subgroups of the Galois group is normal in G and normal in the one preceding it. Also by the Fundamental Theorem we have $\Gamma(F:F_i)/\Gamma(F:F_{i+1}) \approx \Gamma(F_{i+1}:F_i)$, where $\Gamma(F_{i+1}:F_i)$ is abelian by the technical lemma above. Thus we have produced a chain of normal subgroups yielding abelian factor groups, so the group G is soluble.

Finally we are in a position to tackle the main question which motivated the theory and thereby to crown years of mathematical achievement. As mentioned before, first we shall look at the so-called general polynomial of degree n.

Suppose we have a (monic) polynomial p over K. If we write this polynomial as a product of linear factors, we have

$$p(x) = (x - t_1)(x - t_2)....(x - t_n),$$

where the t_k are the zeros. Since this represents all possible polynomials of degree n over K, we view the t_k as "indeterminates." We note that p(x) in unfactored form is

$$p(x) = x^n - s_1x^{n-1} + s_2x^{n-2} - \ldots +\ldots+(-1)^n s_n$$

where s_i is the i-th symmetric polynomial in the n indeterminates; that is, the sum of all possible products of n indeterminates chosen i at a time. A brief look at a polynomial of degree 3 will lend credibility to this. Consider $f(x) = (x - t_1)(x - t_2)(x - t_3) = x^3 - (t_1 + t_2 +$

$t_3)x^2 + (t_1t_2 + t_2t_3 + t_1t_3)x - t_1t_2t_3$ These non-leading coefficients are clearly s_1, s_2, and s_3, respectively, for three indeterminates t_1, t_2, and t_3.

The polynomial p above is called the *general polynomial* over $K(s_1, s_2, ..., s_n)$. Notice that this polynomial is not over K, even though a specific polynomial which this 'general' form represents would be over K. It is important to realize at this point that p is a polynomial with purely symbolic zeros, so $K(s_1, s_2, ..., s_n)$ is a transcendental extension of K. But the splitting field for p over $K(s_1, s_2, ..., s_n)$ is evidently $K(t_1, t_2, ... , t_n)$, and we are interested in the Galois group of this field over $K(s_1, s_2, ..., s_n)$. If we discover that this Galois group is insoluble, then we have shown that the general polynomial is not soluble by radicals 'over K.' The alert reader may have noticed that we are home free, because S_n is obviously a subgroup of the said Galois group - it certainly fixes the symmetric polynomials - and a subgroup of a soluble group is soluble. If the Galois group *were* soluble, then S_n would be soluble, a contradiction for $n \geq 5$.

This result tells us that there does not exist a general 'radical' formula for all n-th degree polynomials, $n \geq 5$. However, it does not tell us that any specific polynomial is not soluble by radicals. One must think of it in this way: if there were a general formula, it would solve the general polynomial. But the general polynomial is not soluble by radicals, so there is no general formula. However, the general polynomial is actually a highly specialized kind of polynomial: it is one with symbols as its zeros and thus does not truly represent any given polynomial with actual zeros. So in order to show that it is impossible to solve the quintic by radicals even with ad hoc methods, we must find a given polynomial which has an insoluble Galois group over **Q**. This result is in an important sense stronger than the other: it settles all the questions at once. That is, if a given polynomial of degree 5 is not soluble by radicals then there is no general formula. Also, the polynomials of higher degree (over **Q**) are also shown to be not all soluble by radicals, for if they were, one could solve the fifth degree polynomial as well. We now turn our attention to finding a specific polynomial of degree 5 over **Q** which is not soluble by radicals.

First we need a technical fact about the Galois group of certain polynomials of prime degree. Before presenting this lemma, we must recognize that all Galois groups are subgroups of the group of permutations. Permutating the roots are the only possibilities for the automorphisms, so this relation should be evident.

Lemma If an irreducible polynomial f over **Q** has prime degree p and precisely two non-real zeros, then the Galois group G of f is S_p.

Proof If the splitting field of f is $\Sigma \subseteq$ **C**, and if α is a zero of f then $\mathbf{Q}(\alpha) \subseteq \Sigma$. Thus $p = [\mathbf{Q}(\alpha):\mathbf{Q}]$ so $p \mid [\Sigma:\mathbf{Q}] = |G|$. So there is an element of order p in $G \subseteq S_p$. Complex conjugation is a **Q**-automorphism of Σ which leaves the real roots fixed, so there is a 2-cycle in G. But it is a well-known fact in group theory that a 2-cycle and a p-cycle generate all of S_p.

Now we are ready to answer the main question of the text.

Theorem $f(t) = t^5 - 6t + 3$ over **Q** is not soluble by radicals.

Proof f is irreducible by Eisenstein. Now we need to show that f has exactly 3 real zeros. Note that $f(-2) = -17$; $f(-1) = 8$; $f(0) = 3$; $f(1) = -2$; and $f(2) = 23$. By Rolle's Theorem the zeros are separated by zeros of the derivative of f, and $Df = 5t^4 - 6$ which has $t = \pm \sqrt[4]{6}$ as its real roots. So there are precisely 3 real roots, leaving 2 non-real roots. 5 is prime, so the Galois group of the polynomial is S_5, which is insoluble.

III. APPLICATIONS

In his *Apology* G.H. Hardy made the following remark concerning the mark of truly worthy mathematics[3]:

> A significant mathematical idea, a serious mathematical theorem, should be 'general' in some such sense as this. The idea should be one which is a constituent in many mathematical constructs, which is used in the proof of theorems of many different kinds. The theorem should be one which, even if stated originally (like Pythagoras's theorem) in a quite special form, is capable of considerable extension and is typical of a whole class of theorems of its kind. The relations revealed by the proof should be such as connect many different mathematical ideas.

These observations are particularly germane to the theory of field extensions developed by Galois. In this section I shall make an attempt to demonstrate the appropriateness of Hardy's criterion to determine the greatness of the theory by means of example. Unfortunately, the applications offered in this text reveal the limitations of my mathematical expertise, but they should give the reader some idea of the wide applicability of Galois' theory of field extensions.

The first example is a relatively simple result given by D.G. Mead in a recent article in the *American Mathematical Monthly* [6]. It involves the idea that there is no parallel for field extensions of Cauchy's theorem for groups. That is, unlike groups where if a prime p divides the order of the group then there is a subgroup of order p, not every extension contains subfields with prime extension degree where the prime divides the degree of the original extension. The best way to see this is to look directly at the result.

Theorem For any positive integer n, there is an extension K of **Q** of degree n such that there is no intermediate extension.

Proof Let f be a polynomial over **Q** whose Galois group is S_n. (It is known that such a construction is possible.) Let L be the splitting field for f over **Q**. If K is the fixed field of S_{n-1}, then $[K:Q] = [L:Q]/[L:K] = |S_n| / |S_{n-1}| = n$ by the Fundamental Theorem. Also by the Fundamental Theorem, if there were an extension of **Q** between K and **Q** then its corresponding group of

[3] Hardy, G.H. *A Mathematician's Apology*. Cambridge University Press, New York: 1967. p. 104

automorphisms would be a group properly between S_n and S_{n-1}, and basic group theory shows this to be a contradiction.

Actually, the above theorem is not surprising at all. If it were not true, the Fundamental Theorem would be rather uninteresting in that the correspondence between subfields and subgroups would be automatic without the extra hypotheses of normality and separability. However, what is interesting in the above result is the way in which the Fundamental Theorem asserts itself as important. That is to say, one uses the theorem to demonstrate its own necessity.

The next application is an alternate proof of the so-called Fundamental Theorem of Algebra. Of course, Gauss proved this before the birth of the Galois theory and in a manner wholly different from the present one. But the point here is not to offer a superior proof; rather, it is to show how the Galois theory *can* verify this familiar result in a new fashion.[4] First we need an important tool.

Lemma If for a field K of characteristic 0 every finite extension has degree divisible by a prime p, then every finite extension of K has degree a power of p.

Proof Let M be a finite extension of K. By passing to a normal closure we may assume that M:K is normal. Now take the Sylow p-subgroup of $\Gamma(M{:}K)$ and call it P. By the Fundamental Theorem $[P^\dagger{:}K]$ is equal to the index of P in $\Gamma(M{:}K)$ which is prime to p. Then p does not divide $[P^\dagger{:}K]$ which implies $P^\dagger = K$ so $P = \Gamma(M{:}K)$.

Theorem The Fundamental Theorem of Alegbra
Every polynomial over **Q** splits in **C**.

Proof Our strategy is to show that the splitting field of any polynomial over **R** is contained in**R**(i) = **C**. Let K be an arbitrary finite extension of degree > 1. Then [K:**R**] cannot be odd, for if it were we would have $\alpha \in K \backslash \mathbf{R}$ with minimum polynomial over **R** of odd degree. But we know from analysis that a polynomial of odd degree has at least one zero in **R**, whence comes a

[4] It is really not all that new, since it was first done this way by Legendre; however, his proof had gaps which are here filled by the Galois theory.

contradiction. So 2 divides every finite extension and, by the lemma above, every finite extension is a power of 2. Now consider a splitting field Σ for a polynomial irreducible over $\mathbf{R}$. Assume $\Sigma \not\subseteq \mathbf{C}$. $\Gamma(\Sigma:\mathbf{R})$ is a 2-group as we have shown above. By the Galois correspondence there exists an extension M of $\mathbf{R}(i) = \mathbf{C}$, with $M \subseteq \Sigma$, such that $[M:\mathbf{C}] = 2$. So there is an element $\beta \in M\backslash\mathbf{C}$ with minimum polynomial n of degree 2. Since $\mathbf{C}(\beta) \subseteq M$ and $[\mathbf{C}(\beta):\mathbf{C}] = 2$ we know that $M = \mathbf{C}(\beta)$. Since $[\mathbf{C}(\beta):\mathbf{C}] = 2$, we have $\beta^2 + e\beta + f = 0$, for e and f in $\mathbf{C}$. By the quadratic formula, $\beta \in \mathbf{C}(\gamma)$ where $\gamma = \sqrt{e^2 - 4f}$. But $\gamma^2 \in \mathbf{C}$ and so $M = \mathbf{C}(\beta) = \mathbf{C}(\gamma)$. Also, since $\gamma^2 \in \mathbf{C}$, we have $\gamma^2 = a + bi$, where $a,b \in \mathbf{R}$ and $\gamma = \sqrt{a + bi} = \sqrt{\frac{a + \sqrt{a^2 + b^2}}{2}} + i\sqrt{\frac{-a + \sqrt{a^2 + b^2}}{2}}$, by Demoivre's Theorem. So β is in $\mathbf{C}$ and $M = \mathbf{C}$, a contradiction. Thus $\Sigma \subseteq \mathbf{C}$.

The remaining portion of this chapter will be the preparation for and demonstration of Gauss' famous theorem concerning the possibility constructibility of regular polygons of an arbitrary number of sides. In order to begin we need to introduce a useful though non-standard definition found in Stewart.

Definition A number n is said to be *constructive* if the n-gon can be constructed.

Note that whether the n-gon is constructible really reduces to whether one can construct the angle $2\pi/n$ or, equivalently, whether the number $\cos(2\pi/n)$ or $\sin(2\pi/n)$ is constructible in the conventional sense of that word. From these observations a few results follow rather easily.

Lemma If m is constructive and $d|m$, then d is constructive. If n is constructive and m and n are relatively prime, then mn is constructive. 2^r is constructive for any positive integer r.

Corollary $n = 2^r p_1^{\alpha_1} p_2^{\alpha_2} \dots p_k^{\alpha_k}$ (where the p_i are distinct primes) is constructive if and only if each $p_i^{\alpha_i}$ is constructive.

At this point recall that constructible numbers must lie in an extension of degree a power of 2 over **Q**. This fact is important for our next result.

Theorem If p^n is constructive then the p^n-th root of unity has splitting field degree a power of 2 over **Q**.

Proof Let $\alpha = \cos(2\pi/p^n)$ and $\beta = \sin(2\pi/p^n)$. These numbers are constructible by hypothesis so $[\mathbf{Q}(\alpha, \beta):\mathbf{Q}] = 2^r$, for some r. For ω the primitive p^n-th root of unity, $\mathbf{Q}(\omega) \subseteq \mathbf{Q}(\alpha,\beta,i)$ and $[\mathbf{Q}(\alpha,\beta,i):\mathbf{Q}] = 2^{r+1}$ so $\mathbf{Q}(\omega)$ has degree a power of 2 over **Q**.

We also need two technical lemmas whose proof amounts to showing that the given polynomials are irreducible over **Q**.

Lemma For a prime p, the minimum polynomial of the p-th root of unity is $f(t) = 1 + t + ...+ t^{p-1}$.

Lemma For a prime p, the minimum polynomial for the p^2-th root of unity is $f(t) = 1 + t^p + ... + t^{p(p-1)}$.

One last definition is pertinent.

Definition A *Fermat prime* is one of the form $2^{2^r} + 1$ for a positive integer r.

It is a well-known fact that any prime of the form $2^s + 1$ is a Fermat prime.

We are now ready for Gauss' theorem on the constructibility of the n-gon. Gauss proved the more difficult part - sufficiency, but he said he could also prove necessity. The proof which follows has many details relying on the lemmas directly preceding it, so careful attention is required.

Theorem A number n is constructive if and only if n has the form $2^r p_1 p_2 . . . p_k$ where the p_i's are distinct Fermat primes.

Proof Suppose $n = 2^r p_1^{\alpha_1} p_2^{\alpha_2} \ldots p_k^{\alpha_k}$ is constructive. Assume some $\alpha_i \geq 2$. Then p_i^2 is also constructive. Hence $[\mathbf{Q}(\omega):\mathbf{Q}] = 2^r$ for ω the primitive p_i^2-th root of unity. But $[\mathbf{Q}(\omega):\mathbf{Q}] = p_i(p_i - 1)$ by our lemma above, and this cannot be the case since $p_i > 2$. Therefore each $\alpha_i = 1$. Now each p_i is constructive, and by our lemma $p_i - 1 = 2^r$ so p_i is a Fermat prime.

For sufficiency we need only show that the Fermat primes are constructive. Let $p = 2^{2^r} + 1$. Then $p - 1 = 2^s$. Now consider the p-th root of unity, ω. It is clear that $[\mathbf{Q}(\omega):\mathbf{Q}] = 2^s$ (from the above lemma) and that $G = \Gamma(\mathbf{Q}(\omega):\mathbf{Q})$ is not only a 2-group but an abelian one as well. We want to look at $K = \mathbf{Q}(\omega) \cap \mathbf{R}$. Now K is obviously a field and $\cos(2\pi/p) = (\omega + \omega^{-1})/2 \in K$. From the Galois correspondence we have that $|\Gamma(\mathbf{Q}(\omega):K)| = [\mathbf{Q}(\omega):K] = 2$, and $\Gamma(\mathbf{Q}(\omega):K)$ is a normal subgroup of G since G is abelian. Then $K:\mathbf{Q}$ is a normal extension of degree a power of 2 and has a series of intermediate fields of degree 2 over the previous one by the Galois correspondence (because a p-group has a series of subgroups of every power of p and G is abelian). Therefore $\cos(2\pi/p)$ is constructible, so p is constructive.

Works Consulted

1. Artin, Emil. *Galois Theory.* Notre Dame Mathematical Lectures, Number 2, Second Edition. North State Press, Hammand, IN: 1964.

2. Bell. E.T. *Men of Mathematics.* Simon and Schuster, New York: 1965.

3. Ehrlich, Gertrude. *Fundamental Concepts of Abstract Algebra.* PWS-KENT Publishing Company, Boston: 1991.

4. Gallian, Joseph A. *Contemporary Abstract Algebra.* Second Edition. D.C. Heath and Company, Lexington, MA: 1990.

5. Herstein, I. N. *Topics in Algebra.* Blaisdell Publishing Company, New York: 1964.

6. Mead, D.G. "The Missing Fields." *American Mathematical Monthly.* Vol 94, Number 9. November, 1987, pp. 871-2.

7. Rothman, A. "The Short life of Évariste Galois." *Scientific American.* Vole 246, April, 1982, pp. 112-20.

8. Stewart, Ian. *Galois Theory.* Second Edition. Chapman and Hall, New York: 1989.