The Life of Evariste Galois and his Theory of Field Extension

Felicia Noelle Adams

A Senior Thesis submitted in partial fulfillment
of the requirements for graduation
in the Honors Program
Liberty University
Spring 2010

Acceptance of Senior Honors Thesis

This Senior Honors Thesis is accepted in partial
Fulfillment of the requirements for graduation from the
Honors Program of Liberty University.

_____

Honoré Mavinga, Ph.D.
Thesis Chair

_____

Evangelos Skoumbourdis, Ph.D.
Committee Member

_____

Kristina Schimmels, M.Ed.
Committee Member

_____

James Nutter, D.A.
Honors Director

_____

Date

Abstract

Evariste Galois made many important mathematical discoveries in his short lifetime, yet perhaps the most important are his studies in the realm of field extensions. Through his discoveries in field extensions, Galois determined the solvability of polynomials. Namely, given a polynomial P with coefficients is in the field F and such that the equation $P(x) = 0$ has no solution, one can extend F into a field L with α in L, such that $P(\alpha) = 0$. Whereas Galois Theory has numerous practical applications, this thesis will conclude with the examination and proof of the fact that it is impossible to trisect an angle using only a ruler and compass.

The Life of Evariste Galois and his Theory of Field Extension

One of the great tragedies in the scientific world was the loss of the genius and potential of Evariste Galois (1811-1832). Galois's life, though riddled with rejection and misunderstanding, brought forth one of the most important mathematical works of the nineteenth century. Though never formally presented during his lifetime, his theory of field extensions had revolutionary implications, which still greatly influence the study of mathematics today. Galois's question, "When is an equation solvable by simple radicals?" led him to an entire new world of mathematics. However, his life was not a happy one and – as is true of most genius' lives – and his theories were not accepted nor noticed during his brief lifetime.

History: Galois's short, yet impactful life

Born to a revolutionary family on October 25, 1811, Evariste Galois was the first-born son of Nicolas Gabriel Galois and Adelaide Marie. Galois was the middle child, growing up with an older sister named Nathalie Théodore Galois and a younger brother named Alfred Galois. Galois father, Nicolas, managed a boys' school in Bourg-la-Reine, a suburb of Paris, France. Adelaide, Galois's mother, was the daughter of a jurisconsult in the Paris Faculty of Law and was educated in classical studies. Galois's father, Nicolas was a witty and entertaining man, making him very popular in Bourg-la-Reine. This popularity mingled with good political savvy, won Nicolas the appointment of mayor. Remarkably, he managed to remain mayor of the city throughout the continually changing political atmosphere. France, after Napoleon's final collapse, remained in a state of chaos and polarized into two distinct political camps. One side was identified as the liberals, or republicans, and they were known for their radical ideas; whereas the

other side was branded as the “legitimists” or the “ultras,” and their ideal state was a church-run monarchy (Livio, 2005). The government gave the richer population two-thirds of the vote and the state schools (their public schools) ran with military-like control.

Yet, in the year 1823, just when Paris was teeming with these new ideas and possibilities, twelve-year-old Evariste Galois arrived at the famous *Lycée Louis-le-Grand.* Having been educated at home by his well-informed mother, the *Lycée* must have been a shock to the sheltered Galois. This school was steeped in legitimist values – the students had their own uniforms, very little food to eat, and strict rules regarding when they could speak and exercise. Galois’s life might have turned out differently in a different century, but the strict control and ridiculous rules stifled Galois’s unique creativity. Initially excelling in the classics, (Latin and Greek) due to his mother’s education, and winning a competition in mathematics, the atmosphere of the *Lycée* ultimately took its toll on him and his health and schoolwork started to deteriorate. At this time in Paris, the conservative “ultras” began gaining power and if someone did anything that they could deem a “crime against religion,” they were sentenced to death. This bleak social outlook definitely influenced the students at the *Lycée*. At the age of 15, Galois encountered his first, and certainly not last, setback. The headmaster Laborie held Galois back (despite his grades) from entering the advanced

Figure 1. A picture of Galois during his time at the Lycée (Newman, 2009).

rhetorique class. Laborie claimed that Galois was too young for the advanced class. However demoralizing, this setback introduced Galois to his life-long fascination with mathematics. A new mathematics teacher named a M. Vernier joined the staff of the *Lycée*, and this, along with a new textbook, *Elements of Geometry* by Legendre, led Galois to become interested in the study of mathematics – legend has it that he read the entire book in two days. From that point in his life, Galois lost interest in his other studies – intent on focusing on mathematics – much to the discontent of his teachers. His other teachers described his attitude in their classes as "There is nothing in his work except strange fantasies and negligence," and "He is under the spell of the excitement of mathematics. I think it would be best for him if his parents would allow him to study nothing but this" (Livio, 2005, p. 117).

Only one teacher recognized Galois's giftedness and encouraged his studies; this teacher's name was Louis Paul Emile Richard. It was under Richard's tutelage that Galois published his first paper. This paper dealt with applications of continued fractions and was Galois first foray into his new theories about groups and fields (Livio, 2005). Beginning with introducing the idea of a group, Galois theorized that in order to solve certain polynomials, he would have to create a special "Galois Group" of the polynomial and specific properties of the "Galois Group" would determine whether the polynomial was solvable. During Galois's time at the Lycée, Richard encouraged Galois to submit two papers to the Academy of Science – the most prominent scientific body in France. Richard took these papers to the great mathematician Cauchy, intending for Cauchy to present Galois's manuscripts to the Academy of Sciences. Sadly, Cauchy wrote to the Academy that he was unable to present Galois's theory because he was ill; yet on January

25, Cauchy ended up presenting his own ideas – whether or not this was due to egotism or was an unfortunate oversight is unknown.

Henceforth in Galois's life, problems arose. First, a priest falsely slandered his father, and Nicolas, not able to bear the shame, committed suicide. This tragedy happened in 1829, right in the middle of the struggle between the ultras and the church. Thus, the church did not consider Nicolas, a staunch liberal and the mayor, an ideal person to be in authority. Second, and days after his father's death, Galois re-failed the entrance exam to the greatest scientific college in France, the *Ecole Polytechnique*. There are differing accounts on why the examiner failed him. One account suggests that the examiner asked Galois to detail the theory of "arithmetic logarithms" and Galois informed him that there were no such things as "arithmetic" logarithms (Stewart, 1973). This meant that his only option was to attend the second best college in France, the *Ecole Préparatoire*. Admitted to the *Préparatoire* after obtaining his diploma from the *Lycée* – not an easy thing to do with his focus entirely on mathematics at the cost of his other studies – Galois signed a ten-year contract to remain within the state education system. In February of 1830, Galois again presented his ideas to the Academy of Sciences, attempting to win the Grand Prize in Mathematics – a tremendous mathematical honor. However, yet again ill luck followed Galois and the secretary died before reading his paper. And thus, the Academy never even had the opportunity to consider Galois's paper (Struik, 1986).

Plagued with trials, the only good thing to come of his time spent at the *Préparatoire,* was his friendship with Auguste Chevalier. Chevalier fostered Galois's fascination with politics. Reformation having entirely taken over Galois's thoughts, he

joined the *Société des Amis du Peuple,* a society consisting of the most radical of the Republican Party. It was during this time in 1830 that Paris erupted in riots over King Charles X's decision to suspend the freedom of the press. Riots broke out and for three days, the streets of Paris were filled with the sound of gunshots and the smell of the dead. Galois desperately wanted to join and fight, but the director of the *Ecole Préparatoire,* Guigniault, sided with the Ultras and threatened to call the troops if the students tried to join the revolution. In the end, after 4,000 people lay dead, the politicians formed a compromise and Charles X left in exile. This revolution severed any ties that Galois might have felt toward Guigniault. Galois considered Guigniault a traitor and coward; consequently, in December of 1830, Galois scathingly responded to a letter that Guigniault had written in a student newspaper. In response, on January 4, 1831, Guigniault expelled Galois from the *Préparatoire* (Livio, 2005). From this point on, Galois's passionate life only deteriorated, ultimately ending in his death.

The Loss of a Brilliant Star that Never Reached Its Peak

After leaving the *Préparatoire,* Galois had no way to support himself. He tried to give math lessons, but his lectures were much too advanced for even his friends to understand. As a result, Galois had to resort to tutoring low-level mathematics. Though in the midst of these trials, the Academy asked him to resubmit his memoir, which he gladly did. Yet again, fate seemed to be against Galois and even after sending a letter inquiring about his submission, he did not receive a response. During this period of his life, Galois's Republican beliefs grew stronger and he joined the National Guard. However, soon after he joined the Republican organization, the King disbanded it. In protest, the members held a banquet. Many famous people attended, including Alexandre

Dumas, Raspail, and Galois. As the dinner grew riotous, history states that Galois was heard giving a toast and saying, “To Louis-Philippe!” brandishing a dagger (Stewart, 1973). His companions obviously saw this as a threat against the King and soldiers arrested Galois the next day. During his trial, Galois protested his arrest, stating that he had said to Louis-Philippe if he turns traitor, but there was too much cheering that no one heard his final words. The jury acquitted Galois and he was free, but only for a short time. His friends, the Chevaliers, wrote an article in a newspaper about Galois and how the Academy never responded to his memoir. In response to this remark, Poisson and Lacroix finally presented their verdict and the news was not encouraging for Galois. They stated that, “His reasonings are neither sufficiently clear, nor sufficiently developed for us to be able to judge their exactness, and we are not in a position that enables us to give an opinion in this report” (Livio, 2005, p. 133). With this sentence, they lost a great genius and the world did not hear of his revolutionary theories for another 15 years when Liouville published most of his work (O’Connor & Robertson, 1996).

July of 1831 was not a good month for Galois. His revolutionary leanings strained his relationship with his family and he moved into to his own apartment. This did not help his violent political position and on July 14, Galois and his friend Ernest Duchatelet led a group of 600 people in protest. The police again arrested Galois and sentenced him to six months in prison. On December 3, the court sent both Galois and Duchatelet to the Saint-Pélagie prison. These months in prison were dreadful for Galois – his low standing due to his lack of financial means and his ill health only increased his depression. Raspail, a compatriot, wrote that a drunk Galois, while in prison, tried to commit suicide. Nathalie-Théodore, his sister, describes him as aging before his time

(Livio, 2005). Yet in the spring of 1832, due to a cholera epidemic, they transferred Galois to a hospital where he met Stéphanie DuMotel. Like all of Galois's emotions, he fell passionately and violently in love. Unfortunately for Galois, the phrase "Love sought is good, but given unsought, is better," did not apply to his own life (Shakespeare, 1994, p. 101).

'Je n'ai pas le temps'

The details of this short affair are shrouded in myth (even Stéphanie's surname is uncertain). However, it is known that she turned his proclamations of love down and he somehow insulted Stéphanie. This misfortune led to the infamous duel. There are many different stories of how Galois came to die in a duel on the 31 of May 1832. The two main ideas are either a lovers' quarrel or a political coupé. Toti Rigatelli's theory concerning the duel is quite interesting; she theorizes that Galois invented the entire story and sacrificed himself, believing that the rebellion needed a corpse to unite (Rigatelli, 1996). Nevertheless, history is not even clear on whom Galois fought or how he got to the hospital, where he died the next day. The only concrete fact that history reveals about Galois's death is that either a peasant or a former military officer carried the wounded Galois to the Cochin Hospital at 9:30 in the morning and only his younger brother Alfred was with him when he died half an hour later (Livio, 2005). While one can never be sure of the reason for the duel, Galois did write a letter to his friend Chevalier the night before his duel, outlining the exciting introduction to the new idea, now known as Galois Theory. Galois asked Chevalier to take his rewritten memoir and ideas to Jacobi or Gauss. This long letter contained what became Galois's most famous quote and one that aptly describes his short life: "'Je n'ai pas le temps' – 'I have no time'" (Livio, 2005, p.

145). While society never honored or recognized his works during his lifetime, today professors around the world teach Galois Theory in graduate programs, influencing new minds to solve the "unsolvable" just as he did.

He found it!

"I hope to interest the Academy in announcing that among the papers of Evariste Galois I have found a solution, as precise as it is profound, of this beautiful problem: whether or not [a polynomial] is solvable by radicals…" This is how Joseph Liouville's presentation of Galois's theories to the Academy on July 4, 1843 began – exactly 12 years after Poisson and Lacroix submitted their report not recommending Galois's papers to be recognized. Years later, Felix Klein used Galois's proof on the solvability of polynomials, which relied on the "classification of equations according to their symmetry properties under permutations of the solutions," to prove "that the icosahedral group and the permutations group are isomorphic" (Livio, 2003, p. 197). This lead to Galois Theory spilling over into other disciplines, especially physics. Einstein used Galois's ideas of symmetry to identify the foundation of the natural laws. Thus, a 21-year-old Frenchman discovered a theory that has ramifications that can ultimately describe the structure of the universe.

What is a Group?

Now what is Galois Theory and why is it important? Before addressing the topic of Galois Theory and the subsequent theory of field extensions, the reader needs a brief definition of groups, fields, and extensions of fields. This will suffice to give him or her a foundation on which to better comprehend the difficult mathematical proofs addressed later. The symmetry of groups is inherent in nature and all created things. The hard part

is to simplify the parts down into the underlying structure. The first mathematician to use the idea of groups as we use it today was Evariste Galois in his search to determine the solvability of polynomials. The definition of a group from J. Fraleigh's Abstract Algebra(2003) states:

A group $\langle \boldsymbol{G}, * \rangle$ is a set **G**, closed under a binary operation *, such that the following axioms are satisfied:

I. For all a,b,c ∈ **R**, we have

$(a * b) * c = a * (b * c)$ associatively of $*$.

II. There is an element e in **G** such that for all $x \in \mathbf{G}$,

$e * x = x * e = x$ identity element e for $*$.

III. Corresponding to each $a \in \mathbf{G}$m there is an element a' in **G** such that

$a * a' = a' * a = e$ inverse a' of a (51-52).

The two good examples of a group are <**Z**,+> and <**Q**,+>. However, notice that <**N**, +> is not a group. Another relatively easy example of a group is the group $\mathbf{Z}_6$. $\mathbf{Z}_6$ is the set {0,1,2,3,4,5,6}. Under addition, the identity of $\mathbf{Z}_6$ is 0 and the inverses of all the elements are clearly seen in figure 2. For example, looking at figure 2, the inverse of 1 is 5, the inverse of 2 is 4, the

+	**0**	**1**	**2**	**3**	**4**	**5**
0	0	1	2	3	4	5
1	1	2	3	4	5	0
2	2	3	4	5	0	1
3	3	4	5	0	1	2
4	4	5	0	1	2	3
5	5	0	1	2	3	4

Figure 2. This table is the group $\mathbf{Z_6}$ under addition.

+	**1**	**-1**	***i***	***-i***
1	1	-1	*i*	*-i*
-1	-1	1	*-i*	*i*
i	*i*	*-i*	-1	1
-i	*-i*	*i*	1	-1

Figure 3. This table is the group <{1, -1, *i*, *-i*},*>.

inverse of 3 is 3, the inverse of 4 is 2, and the inverse of 5 is 1. Clearly one can see the pattern here. Another example of a group is the set {1,-1, *i*, *-i*} under multiplication. Figure 3 illustrates this group. An interesting aspect of this group is that it is isomorphic to the group $\mathbf{Z_4}$ and is thus cyclic with a generator of < *i* >.

While studying groups, Galois noticed that sometimes a group's structure could capture the inherent and abstract structure of a geometric square. However, innate in geometry are many groups of symmetry other than squares; for example, the permutations of the geometrical shapes of either a rectangle or an equilateral triangle both can be represented by a group. Let me elaborate on the example of the dihedral group $\mathbf{D_4}$ of permutations. The group is also known as the group of symmetries of a square, or the octic group (Fraleigh, 2003). This group contains all the permutations that correspond to the rotations, mirror images, and reflections that act on the square (seen in figure 2), leaving it in the same position as it began. Let us refer to rotations as ρ_i, mirror images as σ_i, and diagonal flips as δ_i. Let $\rho_0 = \binom{1\,2\,3\,4}{1\,2\,3\,4}$, $\rho_1 = \binom{1\,2\,3\,4}{2\,3\,4\,1}$, $\rho_2 = \binom{1\,2\,3\,4}{3\,4\,1\,2}$, $\rho_3 = \binom{1\,2\,3\,4}{4\,1\,2\,3}$, $\sigma_0 = \binom{1\,2\,3\,4}{2\,1\,4\,3}$, $\sigma_1 = \binom{1\,2\,3\,4}{4\,3\,2\,1}$, $\delta_0 = \binom{1\,2\,3\,4}{3\,2\,1\,4}$,and $\delta_1 = \binom{1\,2\,3\,4}{1\,4\,3\,2}$. Obviously, ρ_0 refers to the

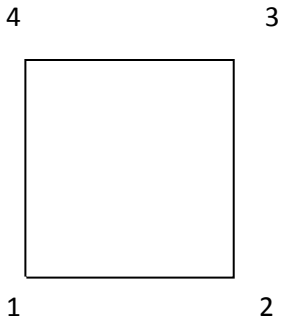

Figure 4. The square.

identity permutation, or in other words, the square does not change at all. ρ_1 moves the squares vertices – vertices 1 to 2, 2 to 3, 3 to 4, and 4 to 1. This is a rotation of 90 degrees. ρ_2 is a rotation of 180 degrees, and ρ_3 is a rotation of 270 degrees. σ_0 is the reflection across the perpendicular bisector of the sides, permuting the vertices 1 to 2, 2 to 1, 3 to 4, and 4 to 3. σ_1 reflects the vertices across the horizontal bisector of the sides, permuting the vertex from 1 to 4, from 2 to 3, from 3 to 2, and from 4 to 1. δ_0 flips the vertices across a diagonal line drawn from vertices 2 to 4, while δ_1 permutes them across a diagonal line from vertices 1 to 3. Looking at table 3, several beautiful properties shine forth. First of all, note that $\mathbf{D_4}$ is nonabelian. Also, look at all of the subgroups. Figure 5 shows the subgroup diagram for $\mathbf{D_4}$.

$*$	$\boldsymbol{\rho_0}$	$\boldsymbol{\rho_1}$	$\boldsymbol{\rho_2}$	$\boldsymbol{\rho_3}$	$\boldsymbol{\sigma_0}$	$\boldsymbol{\sigma_1}$	$\boldsymbol{\delta_0}$	$\boldsymbol{\delta_1}$
$\boldsymbol{\rho_0}$	ρ_0	ρ_1	ρ_2	ρ_3	σ_0	σ_1	δ_0	δ_1
$\boldsymbol{\rho_1}$	ρ_1	ρ_2	ρ_3	ρ_0	δ_0	δ_1	σ_1	σ_0
$\boldsymbol{\rho_2}$	ρ_2	ρ_3	ρ_0	ρ_1	σ_1	σ_0	δ_1	δ_0
$\boldsymbol{\rho_3}$	ρ_3	ρ_0	ρ_1	ρ_2	δ_1	δ_0	σ_0	σ_1
$\boldsymbol{\sigma_0}$	σ_0	δ_1	σ_1	δ_0	ρ_0	ρ_2	ρ_3	ρ_1
$\boldsymbol{\sigma_1}$	σ_1	δ_0	σ_0	δ_1	ρ_2	ρ_0	ρ_1	ρ_3
$\boldsymbol{\delta_0}$	δ_0	σ_0	δ_1	σ_1	ρ_1	ρ_3	ρ_0	ρ_2
$\boldsymbol{\delta_1}$	δ_1	σ_1	δ_1	σ_0	ρ_3	ρ_1	ρ_2	ρ_0

Figure 5. The group $\mathbf{D_4}$.

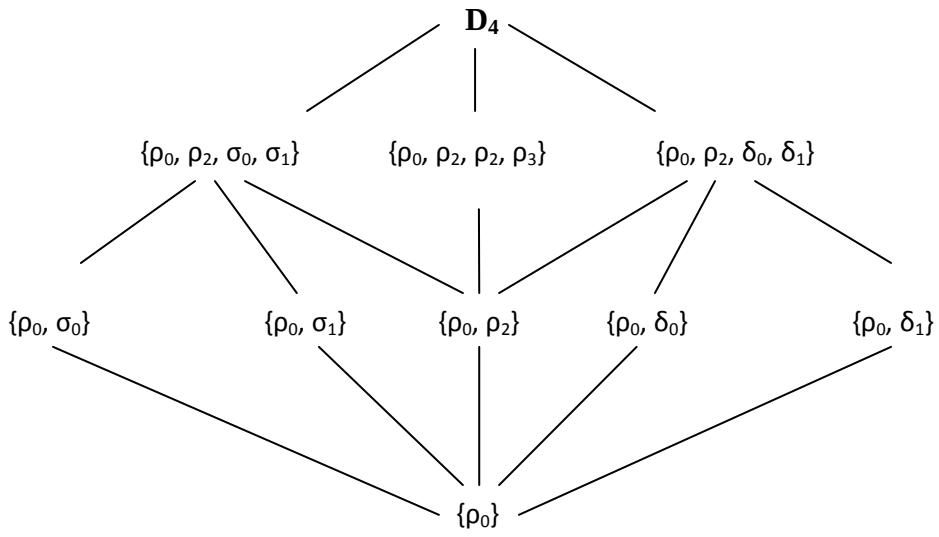

Figure 6. The subgroup diagram for $\mathbf{D_4}$.

Subgroups

Subgroups are very important in our discussion of groups. The definition of a subgroup, found in Fraleigh's *Abstract Algebra* (2003), states that

"A subset **H** of a group **G** is a subgroup of **G** iff the following axioms are met:

I. **H** is closed under the binary operation of **G,**

II. the identity element *e* of **G** is in **H**,

III. for all a ∈ **H** it is true that $a^{-1} \in \mathbf{H}$ also" (p. 66).

From this definition, it should be clear that the sets listed in figure 6 are indeed the subgroups of $\mathbf{D_4}$. Not all proper groups have subgroups; however, all non-proper groups have at least two subgroups – the groups itself and the identity group. Joseph-Louis Lagrange (1736-1813) discovered a theorem that proves if subset is in fact a subgroup. Aptly named Lagrange's Theorem:

Theorem 1: Let **H** be a subgroup of the group **G**. The order **H**, divides the order of the group **G.**

Proof: Let n be the order of the group **G**, and m be the order of the subgroup **H**. We know that every left (or right) coset of **H** has the order as **H**. This implies that every coset of **H** has m elements. Let q be the number of cosets in the partition of **G** into the left cosets of **H**. Then n=m(q). And thus, m is a divisor of n (Fraleigh, 2003, p. 114).

Note that the order of a group is just how many elements are in the group (Borowski & Borwein, 2007). For example, let us examine the group $\langle \boldsymbol{z_6}, + \rangle$ again and try to find its subgroups. Looking at figure 2, we see that the subgroups of $\boldsymbol{z_6}$ are {0,3} and {0,2,4} and the trivial subgroup {0}. Notice Lagrange's theorem at work: the order of the subgroups divide the order of the group. Lagrange's theorem, while it may seem simple, actually allows mathematicians to prove countless theorems and without which, group theory would be infinitely more difficult.

Cosets are another important aspect of subgroups and Quotient groups:

Definition 2: Let **H** be a subgroup of a group **G** and let a be an element of **G**. The subset a**H** = {ah| h is an element of **H**} of **G** is left coset of **H**. The subset **H**a is the right coset of **H** (Borowski & Borwein, 2007, p. 123).

These cosets form a partition of **G**. For example, the left cosets of the subgroup $\{\rho_0,\sigma_1\}$ = **H** of the group **D4** are: $\rho_1\mathbf{H} = \delta_1\mathbf{H} = \{\rho_1,\delta_1\}$, $\rho_2\mathbf{H} = \sigma_0\mathbf{H} = \{\rho_2,\sigma_0\}$, $\rho_3\mathbf{H} = \delta_0\mathbf{H} = \{\rho_3,\delta_0\}$, $\sigma_1\mathbf{H} = \mathbf{H} = \{\rho_0,\sigma_1\}$. From the definition of cosets and Lagrange's theorem, we form one more definition that is important and one more theorem:

Theorem 3: The order of an element of a group **G** divides the order of the group when the group is finite.

Proof: We know that the order of an element is the same as the order of the cyclic group that the element generates. Let m be the order of the element. Thus, m also is the order of a cyclic subgroup. Thus from theorem 1, m divides the order of the group.

Definition 4: Let **H** be a subgroup of a group **G**. The *index* (G:H) is the number of the left cosets of **H** in **G** (Fraleigh, 2003, p. 115).

We might hypothesize here that if an integer m divides the order of a group **G**, then **G** must have a subgroup of order m. Well, this is true in the case where the group **G** is abelian; however, if **G** is not abelian, we cannot make this conjecture.

Now that we have a suitable understanding of basic groups, subgroups, and cosets, we can discuss the special types of groups called factor groups, or quotient groups:

Definition 5: A factor group, **G/H**, is a group whose members are the cosets of the invariant subgroup **H**. Note, any member of the factor group is a set of the elements of a**H**, for all a ∈ **G (**Fraleigh, 2003, p. 151).

We can construct a theorem that states that the cosets form a quotient group by using just coset multiplication. First we must prove that left coset multiplication is well-defined; however, while that proof is straightforward, it is too long and will detract from the point:

Theorem 6: Let **H** be a subgroup of the group **G**. Then the left coset multiplication is well defined for the equation (a**H**)(b**H**) = (ab)**H** if and only if **H** is a invariant subgroup **H** of **G** (Fraleigh, 2003, p. 152).

Fields

While fields were implicit in Galois's work, it was Leopold Kronecker and Richard Dedekind who actually defined a field. Their definition of a field is foundational to Galois Theory:

Definition 7: A field consists of a set **F** with two binary operations <**F**, +,∗>, such that

I. For <**F**, +>, **F** is an abelian group under addition with identity $e = 0$.

II. The set $\mathbf{F} - \{0\}$ is a group, with an identity $e = 1$.

III. And the distributive law holds for all elements; i.e., for all $a,b,c \in \mathbf{F}$, $a * (b + c) = (a * b) + (a * c)$ and $(a + b) * c = (a * c) + (b * c)$ (Borowski & Borwein, 2007, p. 211).

Two examples of fields are the rational and the real number systems; however, the integers **Z** do not form a field. This is because, for example, 2 has no multiplicative inverse, also called a unit. $\mathbf{Z_p}$ is a field, for every prime p – the proof follows on the following page. The fields $\mathbf{Z_p}$ and **Q** are called prime fields – in fact, they are the minimal fields.

Theorem 8: The ring $\mathbf{Z_p}$ is a field if and only if p is a prime number.

Proof: I will prove this by contradiction. Assume that p is not a prime number. If p=1, then $\mathbf{Z_p} = \mathbf{Z}/\mathbf{Z}$ (the quotient group) has only one member and thus cannot be a field. If p>0, then $p = ab$, such that a and b are integers less than p. Let $I = p\mathbf{Z}$, implies that $(I + a)(I + b) = I + ab = I$. However, I is the zero element of $\mathbf{Z}/I$, while $I + a$ and $I + b$ are both greater than zero. This implies that, since the product of two non-zero elements in a field is non-zero, $\mathbf{Z}/I$ cannot be a field.

Now the converse: assume that p is prime. Let $I + a$ be a non-zero element of $\mathbf{Z}/I$. Since $\gcd(a,p)=1$, there exist integers r and s, such that $ra + sp = 1$. Then $(I + r)(I + a) = (I + 1) - (I + p)(I + s) = I + 1$ and also $(I + a)(I + r) = I + 1$. Since $I + 1$ is the identity of $\mathbf{Z}/I$, we have found the multiplicative inverse (the unit) for $I + a$. Thus all non-zero elements of $\mathbf{Z}/I$ have inverses. Therefore $\mathbf{Z}_p = \mathbf{Z}/I$ is a field (Stewart, 1973, p. 56).

*	0	1	2	3	4	5
0	0	0	0	0	0	0
1	0	1	2	3	4	5
2	0	2	4	1	2	4
3	0	3	0	3	0	3
4	0	4	2	0	4	2
5	0	5	4	3	2	1

Figure 7. $\mathbf{Z_6}$ under multiplication.

Now let the reader examine the $\mathbf{Z}_6$ under the binary operation of multiplication. Figure 7, on the right, contains this group. Figure 7 shows that the identity of $\mathbf{Z}_6$ under multiplication is 1, the inverse of 1 is 0, and the inverse of 5 is 5. Since 2, 3, and 4 do not have inverses in $\mathbf{Z}_6$ under multiplication, this implies that $\mathbf{Z}_6$ is not a group under multiplication, thus $\mathbf{Z}_6$ is not a field. This is where the idea of field extensions comes into play; however, let us finish discussing fields.

One important invariant of a field is its characteristic, which is defined below in theorem 9:

Theorem 9: Let **F** be a field. For all positive integers n, we set $n*1 = 1+1+1+\ldots+1$, n times. We have two cases:

Case 1) $n * 1 \neq 0$ for all n in $\mathbf{Z}^+$.

This implies that since $n * 1 \neq 0$, $(n * 1)^{-1}$ exists. This, in turn, implies that for any $\frac{p}{q} \in \mathbf{Q}$, this rational number can be identified with $(p*1)(q * 1)^{-1}$. So that $\mathbf{Q} \subseteq F$. The field **F** is then is said to be of characteristic zero.

Case 2) There exists a n in $\mathbf{Z}^+$, such that $n * 1 = 0$.

If n is the smallest integer such that $n*1 = 0$, then p is a prime. Suppose that $p = k * l = 0$, for $k, l \in \mathbf{Z}$. $(n * 1) = (k * 1)(l * 1) = 0$.

This implies that $(k * 1) = 0$ or $(l * 1) = 0$. But this contradicts the fact that p is the smallest integer n such that $n*1 = 0$. Thus, $n * 1 = 0$.

Because **F** is a field, we can say that $\mathbf{Z_p}$ is a subfield of **F**. Therefore, **F** is said to be of characteristic p (Borowski & Borwein, 2007, p. 76).

Every science uses the field of real numbers and most use the field of complex numbers. Electrical engineers would not have a job if complex numbers did not exist. However, what about Galois and why did he use and define groups and fields? Remember that he was trying to prove that it is not possible to solve a polynomial of n^{th} order by radicals. To achieve this, Galois created something mathematicians now call field extensions.

Field Extensions

Galois originally wrote his theory of solving polynomials in the complex field (Stewart, 1973). However, mathematicians today use arbitrary fields:

Definition 10: A field **L** is an extension of a field **F** if $\mathbf{F} \leq \mathbf{L}$ (Fraleigh, 2003, p. 279).

For example, any field **F** is an extension of **Q**, if **F** is of characteristic 0; otherwise **F** is an extension of $\mathbf{Z_p}$ if **F** is of characteristic *p*. Also, take for example, the field of real numbers **R** and the field of complex numbers **C**. We denote the extension of **R** by **C** as $\mathbf{R} \leq \mathbf{C}$. Remember that there are two minimal fields, **Q** and $\mathbf{Z_p}$. While the extension of **Q** is relatively easy to construct, the construction of a field extension of $\mathbf{Z_p}$, requires a review of polynomials.

Polynomials

Taught in every middle school in the world, polynomials are the backbone of algebra and without which, mathematics would be indescribable:

Definition 11: We define a polynomial as

$a_0 + a_1x + \cdots + a_nx^n$, where $a_0, \ldots, a_n \in \boldsymbol{R}, 0 \leq n \in \boldsymbol{Z}$, and x is undefined.

The elements $a_0, \ldots, a_n$ are called the coefficients of the polynomial (Borowski & Borwein, 2007, p. 436).

The sum of a polynomial is again a polynomial. Let f(x) = $a_0 + a_1x + \cdots + a_nx^n$ and g$(x) = b_0 + b_1x + \cdots + b_nx^n$. Adding f($x$) and g($x$) gives the new polynomial, h(x) = f(x) + g(x) = $(a_0 + b_0) + (a_1 + b_1)x + \cdots + (a_n + b_n)x^n$. In polynomial addition, one just adds the coefficients; however, polynomial multiplication is not as nice. Yet, the product of a polynomial is still another polynomial, since polynomials are closed under their binary operators. Let f(x) = $a_0 + a_1x + \cdots + a_nx^n$ and g$(x) = b_0 + b_1x + \cdots + b_nx^n$. Multiplying f($x$) and g($x$) produces the new polynomial, k(x) = f(x) g(x) = $d_0 + d_1x + \cdots + d_nx^n$, where $d_0 = \sum_{i=0}^{n} a_i b_{n-i}$. When the coefficients of two different

polynomials of the same degree are equal, we defined the polynomials as equal. Finally, we define **F**[x] as the set of all the polynomials with coefficients in the field **F**. Thus, $\langle \mathbf{F}[x], +, * \rangle$ satisfies all the axioms of a field, except that not all of the elements have multiplicative inverses. Nevertheless, this set, called a ring, is very important:

> **Definition 12: "**A ring $\langle \mathbf{R}, +, * \rangle$ is a set **R** together with two binary operations + and *, which we call *addition* and *multiplication*, defined on **R** such that the following axioms are satisfied:
>
> - $\langle \mathbf{R}, + \rangle$ is an abelian group
> - Multiplication is associative
> - For all $a,b,c \in \mathbf{R}$, the *left distributive law*, $a * (b + c) = (a * b) + (a * c)$ and the *right distributive law* $(a + b) * c) = (a * c) + (b * c)$ hold" (Fraleigh, 2003, p. 181).

A few examples of rings are $\langle \mathbf{Z}, +, * \rangle$, $\langle \mathbf{Q}, +, * \rangle$, and $\langle \mathbf{C}, +, * \rangle$. As stated earlier, **Z** does not have multiplicative inverses under multiplication, so **Z** is not a field, yet it is a ring. **F**[x] is a ring for any field **F**; for example, **Q**[x] is a ring.

Although I defined a polynomial, the question still may arise of how polynomials relate to an ordered set of numbers. Take the $\mathbf{Z_5} = \{0,1,2,3,4\}$. These are the possible remainders when **Z** is divided by 5. In other words, $\mathbf{Z_5}$ is the field equal to the quotient field **Z**/5**Z**. Just as the integers have remainders when divided, polynomials also have long division and remainders. This 'division' is commonly referred to as factoring; in other words, f(x)=q(x) h(x) + r(x), where the degree of the remainder, r(x), is less than the degree of q(x).

Factoring Polynomials: (Easy?) Think again

Finding the zeros of a polynomial is extremely important in every scientific realm imaginable. In fact, this was the purpose of Galois's theory. The factorization of polynomials immensely simplifies the process of finding zeros:

> **Theorem 13:** Any element $\alpha \in \mathbf{F}$ (a field) is a zero of $f(x) \in \mathbf{F}[x]$ if and only if $x - \alpha$ is a factor of $f(x)$ in $\mathbf{F}[x]$ (Steward, 1973, p. 78).

For example, the polynomial $f(x) = x^4 + 4$, can be factored into linear factors in $\mathbf{Z_5}[x]$. Let $\alpha = 1$. Using long division, we see that that $x - 1 = x + 4$ is a factor of $f(x)$. We continuing with $\alpha = 2$, $\alpha = 3$, and $\alpha = 4$. Finally, $f(x) = (x+1)(x+2)(x+3)(x+4)$. Thus, by Theorem 13, we know that $\alpha = 1, 4, 2, 3$ are the zeros of $f(x)$ in $\mathbf{Z_5}$. Obviously, the Factor Theorem makes solving polynomials much easier.

However, a problem arises of what to do in the case of an irreducible polynomial. A polynomial $f(x)$ is irreducible over $\mathbf{F}$ if $f(x)$ cannot be expressed as a product $g(x)\,h(x)$ of two polynomials $g(x)$ and $h(x)$ in $\mathbf{F}[x]$ where both $g(x)$ and $h(x)$ are of lower degree than the degree of $f(x)$. In other words, an irreducible polynomial is a polynomial over a field $\mathbf{F}$ that is unable to be factored in $\mathbf{F}$ into a product of polynomials of lower degree (Borowski & Borwein, 2002). Also, note that the irreducible polynomial is analogous to the prime numbers. However, just because a polynomial is irreducible over $\mathbf{F}$ does not mean that it is not reducible over a larger field $\mathbf{E}$ containing $\mathbf{F}$. For example, $f(x) = x^2 + 1$ is irreducible over the Real numbers, yet it is reducible over the Complex number system. $f(x) = x^2 + 1$ factors into $(x - i)(x + i)$, where i is the imaginary number such that $i = \sqrt{-1}$:

> **Theorem 14:** Let f(x) □ **F**[x], and let f(x) be of degree 2 or 3. Then f(x) is reducible over **F** if and only if f(x) has a zero in **F**. In other words, if a polynomial of degree 2 or 3 is factorable, then it has zeros or conversely, if a polynomial of degree 2 or 3 has zeros in **F**, then it is reducible (Fraleigh, 2003, p. 228).

Polynomials in **F**[x] can be factored into a product of irreducible polynomials in **F**[x] in an essentially unique way.

> **Theorem 15:** Let p(x) be an irreducible polynomial in **F**[x]. If p(x) divides r(x)s(x) for r(x), s(x) □ **F**[x], then either p(x) divides r(x) or p(x) divides s(x) (Fraleigh, 2003, p. 228)

Looking at the example above, let p(x) = $x - i$. Thus p(x) is irreducible and also divides (x^2 +1)(x + 1). This generalizes into Theorem 16:

> **Theorem 16**: If **F** is a field, then every nonconstant polynomial f(x) ∈ **F**[x] can be factored in **F**[x] into a product of irreducible polynomials that are unique except for order and for unit (that is, nonzero constant) (Fraleigh, 2003, p. 231).

Overall, understanding how to factor polynomials is imperative to comprehending field extensions. After all, this was the problem that Galois faced and ultimately solved.

Returning to Field Extensions

We can now discuss the extension of $\mathbf{Z_p}$. Let p(x) be an irreducible polynomial in **F**[x]. This means that there is no element α in **F**[x] such that p(α) = 0. Now, ⟨p(x)⟩ are all the polynomials that have p(x) as a factor; this is called an "ideal". Just as we can find a field by taking a quotient of a field and an ideal, we can use the same idea with polynomials. Just as in the earlier example $\mathbf{Z_5} = \mathbf{Z}/5\mathbf{Z} = \mathbf{Z}/\langle \mathbf{5} \rangle$, so is the field extension

E = **F**[x]/⟨p(x)⟩. In other words, if there is an irreducible polynomial p(x) ∈ **F**[x], then there is a field extension **E** of **F**, such that there exists an α ∈ **E**, such that p(α) = 0.

However, what exactly did Galois theorize and what is a Galois field? While the whole, exhaustive explanation of Galois Theory is too advanced to include in this paper, I will still give an example of a Galois group. Let **F** be a field, such that **F**=$\mathbf{Z}_2$ and let p(x) = $x^2 + x + 1$ which is an element of $\mathbf{Z}_2[x]$. Using the rational roots test, it is obvious to see that p(x) is irreducible over $\mathbf{Z}_2[x]$. Therefore, we must extend $\mathbf{Z}_2$. The extension **E** of $\mathbf{Z}_2$ is $\mathbf{Z}_2[x]/\langle x^2 + x + 1\rangle$. The class of x mod(p(x)) = α. This implies that the remainders are 0, 1, α, 1 + α. These remainders create a Galois field, **GF**(4) ={0, 1, α, 1+α}. Since we know that $\alpha^2 + \alpha + 1 = 0$, we can form a table for this field (figures 8 and 9). Remember that $\alpha^2 = \alpha + 1$.

+	0	1	α	1+α
0	0	1	α	1+α
1	1	0	1+α	α
α	α	1+α	0	1
1+α	1+α	A	1	0

Figure 8. The group of the **GF**(4) under addition.

*	0	1	α	1+α
0	0	0	0	0
1	0	1	α	1+α
α	0	A	1+α	1
1+α	0	1+α	1	α

Figure 9. The group of the **GF**(4) under multiplication.

In general, this system creates an extension **E** of $\mathbf{Z}_p$, such that $\mathbf{E} = \mathbf{GF}(p^r)$, where p is the prime modulus of the field raised to a power $r \in \mathbf{Z}$ of the irreducible polynomial.

For the sake of understanding, let us examine another example. The problem is how to extend $\mathbf{Z_3}$ to allow $f(x) = x^2 + 1$ to have solutions. Factoring $f(x)$, we find the roots are $\sqrt{2}$. Looking at figure 10 and figure 11 on the following page, the field $\mathbf{Z_3}$ appears in the top right corner of both figures. Obviously the square root of two is not a member of $\mathbf{Z_3}$ nor are the square root of two's inverses. Thus, we must extend $\mathbf{Z_3}$ to $\mathbf{Z_3}(\alpha)$, where $\alpha = \sqrt{2}$. The remainders are $\{0, 1, 2, \alpha, 1 + \alpha, 2 + \alpha, 2\alpha, 1 + 2\alpha, 2 + 2\alpha\}$. This field extension **F** is illustrated in figures 10 and 11.

+	**0**	1	2	$\sqrt{2}$	$\sqrt{2}+1$	$\sqrt{2}+2$	$2\sqrt{2}$	$2\sqrt{2}+1$	$2\sqrt{2}+2$
0	0	1	2	$\sqrt{2}$	$\sqrt{2}+1$	$\sqrt{2}+2$	$2\sqrt{2}$	$2\sqrt{2}+1$	$2\sqrt{2}+2$
1	1	2	0	$\sqrt{2}+1$	$\sqrt{2}+2$	$\sqrt{2}$	$2\sqrt{2}+1$	$2\sqrt{2}+2$	$2\sqrt{2}$
2	2	0	1	$\sqrt{2}+2$	$\sqrt{2}$	$\sqrt{2}+1$	$\sqrt{2}$	$2\sqrt{2}$	$2\sqrt{2}+1$
$\sqrt{2}$	$\sqrt{2}$	$\sqrt{2}+1$	$\sqrt{2}+2$	$2\sqrt{2}$	$2\sqrt{2}+1$	$2\sqrt{2}+2$	0	1	2
$\sqrt{2}+1$	$\sqrt{2}+1$	$\sqrt{2}+2$	$\sqrt{2}$	$2\sqrt{2}+1$	$2\sqrt{2}+2$	$2\sqrt{2}$	1	2	0
$\sqrt{2}+2$	$\sqrt{2}+2$	$\sqrt{2}$	$\sqrt{2}+1$	$2\sqrt{2}+2$	$2\sqrt{2}$	$2\sqrt{2}+1$	2	0	1
$2\sqrt{2}$	$2\sqrt{2}$	$2\sqrt{2}+1$	$2\sqrt{2}+2$	0	1	2	$\sqrt{2}$	$\sqrt{2}+1$	$\sqrt{2}+2$
$2\sqrt{2}+1$	$2\sqrt{2}+1$	$2\sqrt{2}+2$	$2\sqrt{2}$	1	2	0	$\sqrt{2}+1$	$\sqrt{2}+2$	$\sqrt{2}$
$2\sqrt{2}+2$	$2\sqrt{2}+2$	$2\sqrt{2}$	$2\sqrt{2}+1$	2	0	1	$\sqrt{2}+2$	$\sqrt{2}$	$\sqrt{2}+1$

Figure 10. This figure refers to the extension of $\mathbf{Z_3}$, or $\mathbf{Z_3}(\sqrt{2})$ under addition. This is also **GF**(9) under addition.

*	**0**	1	2	$\sqrt{2}$	$\sqrt{2}+1$	$\sqrt{2}+2$	$2\sqrt{2}$	$2\sqrt{2}+1$	$2\sqrt{2}+2$
0	0	0	0	0	0	0	0	0	0
1	0	1	2	$\sqrt{2}$	$\sqrt{2}+1$	$\sqrt{2}+2$	$2\sqrt{2}$	$2\sqrt{2}+1$	$2\sqrt{2}+2$
2	0	2	1	$2\sqrt{2}$	$2\sqrt{2}+2$	$2\sqrt{2}+1$	$\sqrt{2}$	$\sqrt{2}+2$	$\sqrt{2}+1$
$\sqrt{2}$	0	$\sqrt{2}$	$2\sqrt{2}$	2	$\sqrt{2}+2$	$2\sqrt{2}+2$	1	$\sqrt{2}+1$	$2\sqrt{2}+1$
$\sqrt{2}+1$	0	$\sqrt{2}+1$	$2\sqrt{2}+2$	$\sqrt{2}+2$	$2\sqrt{2}$	1	$2\sqrt{2}+1$	2	$\sqrt{2}$
$\sqrt{2}+2$	0	$\sqrt{2}+2$	$2\sqrt{2}+1$	$2\sqrt{2}+2$	1	$\sqrt{2}$	$\sqrt{2}+1$	$2\sqrt{2}$	2
$2\sqrt{2}$	0	$2\sqrt{2}$	$\sqrt{2}$	1	$2\sqrt{2}+1$	$\sqrt{2}+1$	2	$2\sqrt{2}+2$	$\sqrt{2}+2$
$2\sqrt{2}+1$	0	$2\sqrt{2}+1$	$\sqrt{2}+2$	$\sqrt{2}+1$	2	$2\sqrt{2}$	$2\sqrt{2}+2$	$\sqrt{2}$	1
$2\sqrt{2}+2$	0	$2\sqrt{2}+2$	$\sqrt{2}+1$	$2\sqrt{2}+1$	$\sqrt{2}$	2	$\sqrt{2}+2$	1	$2\sqrt{2}$

Figure 11. This table refers to the extension of $\mathbf{Z_3}$, or $\mathbf{Z_3}(\sqrt{2})$ under multiplication. It is also **GF**(9) under multiplication.

With this field extension, the polynomial f(x) = x^2 + 1 is reducible over $\mathbf{Z_3}(\sqrt{2})$. In other words, $\mathbf{Z_3}(\sqrt{2})$ is a simple algebraic extension over $\mathbf{Z_3}$ (to be explained later) and is of characteristic 3. The nine remainders of $\mathbf{Z}_3[x]/\langle x^2 + 1\rangle$ form the Galois field **GF**(9). Referring to figures 10 and 11, the reader should be able to tell that with $\alpha = \sqrt{2}$, these two figures illustrate **GF**(9). This is the genius of Galois. He proved how to solve any polynomial.

Finite and Infinite Field Extensions

Understanding finite and infinite field extensions is imperative to understanding Galois groups – our ultimate goal. Beginning with finite field extensions, let **E** be a field extension of a field **F**. We can say that **E** is a vector space over **F**. For example let us examine the field **GF**(9), specifically, $\mathbf{Z_3}(\sqrt{2}\,)$. Using linear algebra, we determine that the basis of this extension is $\{1, \sqrt{2}\,\}$. This means that (a)(1) + (b) ($\sqrt{2}$), where a and b are elements of $\mathbf{Z_3}$, constructs all of the elements in $\mathbf{Z_3}(\sqrt{2}\,)$. It is important to notice that while **E** is a finite extension of **F**, this does not imply that the field **E** is a finite field. Also notice that finite fields **F** have characteristic $p > 0$, when p is prime. In the case of infinite field extensions, the basis is infinite. For example, the real numbers **R** are an infinite extension of the rational numbers **Q**, $\mathbf{Q < R < C}$. Whereas the extension from **R** to **C** is finite with a basis of $\{1, i\}$. This discussion leads to two very important elements of extensions – algebraic and transcendental elements:

Definition 16: Assume that $\mathbf{F} \leq \mathbf{E}$ is a simple extension and $\alpha \in \mathbf{E}$. We say that α is algebraic over **F** if some nonzero polynomial $f(x) \in \mathbf{F}[x]$ factors in $\mathbf{F}[x]$, so that $f(x) = g(x)h(x)$ for $g(x), h(x) \in \mathbf{F}[x]$. Now for the evaluation homomorphism φ_α, such that φ_α: $\mathbf{F}[x] \rightarrow \mathbf{E}$, we have $f(\alpha) = \varphi_\alpha(f(x)) = \varphi_\alpha(g(x)\, h(x)) = \varphi_\alpha(g(x))\, \varphi_\alpha(h(x)) = g(\alpha)\, h(\alpha)$. Thus, if $\alpha \in \mathbf{E}$, then $f(\alpha) = 0$ if and only if either $g(\alpha) = 0$ or $h(\alpha) = 0$.

Otherwise, when $f(x) \neq 0$, α is transcendental over **F** (Stewart, 1973, p. 112)

It is a well-known fact that π and e are transcendental over **Q**; however, this is not easy to prove. Just because π and e are transcendental over **Q** does not sufficient to prove that π and e are transcendental over any field. In fact, they both are algebraic over **R**, for π is a zero of $(x - \pi) \in \mathbf{R}$. This leads to another definition:

Definition 17: An algebraic number is an element of **C** that is algebraic over **Q**. An element of **C** that is transcendental over **Q** is a transcendental number (Fraleigh, 2003, p. 282).

For example, to prove that $1 + 2i \in \mathbf{C}$ is algebraic over **Q**, we must find a $f(x) \in \mathbf{Q}[x]$ such that $f(1 + 2i) = 0$. The polynomial $f(x) = x^2 - 2x + 5$ has as a root, $1 + 2i$. Therefore, $1 + 2i$ is algebraic over **Q**. This theory of beginning with an irreducible polynomial over a field **F** and extending the field to some field extension **E**, is what Galois theorized.

Galois Group of an Extension

All of this prior discussion leads us to the culmination of Galois's theory - the Galois group of an extension. A definition of a homomorphism is required:

Definition 18: A homomorphism on a field **F** is a mapping φ such that for all x and y elements in **F**, $\varphi(x+y) = \varphi(x) + \varphi(y)$ and $\varphi(xy) = \varphi(x)\varphi(y)$ (Fraleigh, 2003, p. 43).

°	**Z**	$\bar{z}$
z	**Z**	$\bar{z}$
$\bar{z}$	$\bar{z}$	**Z**

Figure 12. The table representing $\mathbf{G(C{:}R)} \cong \mathbf{Z_2}$.

The Galois group of an extension **G**[**E**,**F**], is the set of all homomorphisms φ: **E** → **E** that leave **F** pointwise fixed. In other words, φ is an automorphism of **E**. For example, consider the extension **C:R** and assume that φ is an automorphism of **C**. This means that $\varphi(r) = r$ for all r in **R**.

Let $z=x+iy$, so $\varphi(z)=\varphi(x) + \varphi(i)\varphi(y)$.

Since $\varphi(r) = r$, $\varphi(z)= x + \varphi(i)y$. We know that $i^2 = -1$, and since -1 is an element of **R**, $\varphi(i^2) = \varphi(i)\varphi(i) = \varphi^2(i) = -1$. We also know that $\varphi(i)=\pm i$. Thus, $\varphi(z)= x + \varphi(i)y$ either equals $x + iy = z$ or $x - iy = \bar{z}$ (the complex conjugate of z). One can create a Galois group **G**[**C**:**R**] with z and $\bar{z}$ as the elements. This group is isomorphic to $\mathbf{Z_2}$ and is illustrated in figure 12. At first glance, this may not seem important or at all thrilling; yet, the properties of this group reflect the solvability of a polynomial. Galois used this theory to prove that a quintic is not solvable by radicals. However, as that discussion is beyond the scope of this paper, we will discuss a geographical result of Galois Theory.

The Trisection of an Angle

All of this prior theory is nice; however, one may ask how it relates to the physical world. In 1937, Pierre Wantzel proved a practical example using Galois's Theory (Fraleigh, 2003). Since the Greek mathematics of the fourth century, mathematicians have spent years devoted to proving that certain constructions are

impossible; for example, the construction of trisecting an angle. By 1937, everyone knew that trisecting any angle was impossible, yet no one had been able to prove this accepted fact. This assumption can be proved based on Wantzel's proof:

Definition 19: Trisecting any angle is impossible.

Proof: Assume that the angle φ we are trying to construct is a 20 degrees from a 60 degree angle. So let φ = 20. We know that in order to construct an angle of φ, we have to be able to construct the length |cos (φ)|. Using a ruler and compass, it is possible to construct the angle of 60 degress. Remember that $\cos(3\varphi) = \cos(2\varphi + \varphi) = \cos(2\varphi)\cos(\varphi) - \sin(2\varphi)\sin(\varphi) = (2\cos^2(\varphi) - 1)\cos(\varphi) - 2\sin(\varphi)\cos(\varphi)\sin(\varphi) = (2\cos^2(\varphi) - 1)\cos(\varphi) - 2\cos(\varphi)(1 - \cos^2(\varphi)) = 4\cos^3(\varphi) - 3\cos(\varphi)$. Letting φ = 20, entails that cos(3φ) = ½. Let cos(20) = δ and let $4\cos^3(\varphi) - 3\cos(\varphi) = \cos(3\varphi)$. This implies that $4\delta^3 - 3\delta = ½$. We know that the function $f(x) = 4x^3 - 3x - 1/2 = 8x^3 - 6x - 1$ is irreducible over **Q**. The rational roots test proves that none the possible roots, $\pm 1, \pm\frac{1}{2}, \pm\frac{1}{4}, \pm\frac{1}{8}$, is a zero of $8x^3 - 6x - 1$. This implies that the degree of $\mathbf{Q}(\delta):\mathbf{Q} = 3$. In order for δ to be constructible, the degree of the extension must be a power of 2. Since $\mathbf{Q}(\delta):\mathbf{Q} = 3 \neq 2^r$, is means that δ is not constructible. Therefore, a 60-degree angle cannot be trisected (Fraleigh, 2003, p. 311).

Using this same method, it is possible to prove that many other such constructions, like the fact that one cannot use a ruler and compass to duplicate a cube, are impossible. While mathematicians before Galois certainly were aware of the idea of field extensions, Galois was the first to concretely use them to prove his theorems. In

fact, Gauss had asserted “anyone who attempted to find a geometric construction for a *p*-gon where $p - 1$ is not a power of 2 would ‘spend his time uselessly’” (Fraleigh, 2003, 312). When Watzel proved that the trisection of angles was impossible, his theorems relied on the theorems of field extensions that Galois had clearly demonstrated a few years before.

Conclusion

Approximately 180 years ago, Evariste Galois devised a structure to determine whether a polynomial is solvable by radicals. The world still feels ramifications of Galois’s theory today. We saw how useful his theorems were in the example that proved that any angle is unable to be trisected using a ruler and compass. Mathematicians also use Galois Theory to study geometry, physics, chemistry, and many other realms of study. The world is indebted to Galois and the question remains: what else would we know if Galois’s life had not ended so tragically?

References

Adamson, I. T. (1964). *Introduction to field theory.* Edinburgh: Oliver and Boyd.

Artin, E. (1948). *Galois theory.* Notre Dame: University of Notre Dame Press.

Borowski, E.J. & Borwein, J. M. (2007). *Collins dictionary of mathematics.* London: HarperCollins Publishers.

Burton, D. M. (2007). *Elementary number theory.* New York: McGraw-Hill Companies.

Fraleigh, J. B. (2006). *A first course in abstract algebra*. New York: Pearson Education.

Gokhan, S., Demirci, M., Ikikardes, N. Y., & Cangul, I. N. (2007). Rational Points on Elliptic Curves $y^2 = x^3 + a^3$ in $\mathbf{F}_p$, where $p \equiv 5 (\mathrm{mod}\ 6)$ is Prime. *International Journal of Mathematics Sciences, 1*(4), 247 – 250.

Hardy, G.H. (1979). *An introduction to the theory of numbers.* Oxford: Clarendon Press.

Jacobson, N. (1964). *Lectures in abstract algebra : Volume 3 – Theory of fields and galois theory.* Princeton: Van Nostrand.

Kaplansky, I. (1969). *Fields and rings.* Chicago: University of Chicago Press.

Kline, M. (1972). *Mathematical thought from ancient to modern times.* New York: Oxford Universal Press. *Evariste Galois.* MacTutor History of Mathematics. Found from http://www-history.mcs.st-andrews.ac.uk/Biographies/Galois.html.

Livio, M. (2005). *The equation that couldn't be solved.* New York: Simon and Schuster.

Martini, L. (1999). The First Lectures in Italy on Galois Theory: Bologna, 1886–1887. *Historia Mathematica, 26,* 201 – 223.

Neumann, P. M. (2006). The concept of primitivity in group theory and the second memoir of Galois. *Archive for History of Exact Sciences, 60*(4), 379 – 429.

Newman, P. (2009). The memoirs of Evariste Galois. Retrieved from http://sites.google .com/site/algcomb/2009-semester-1/neumann

O'Connor, J.J. & Robertson, E.F. (1996). Evariste Galois. MacTutor. Retrieved from http://www-history.mcs.st-andrews.ac.uk/Biographies/Galois.html

Poole, D. (2006). *Linear algebra: A modern introduction*. Belmont, CA: Thomson.

Radloff, I. (2002). Évariste Galois: Principles and Applications. *Historia Mathematica: 29*(2), 114 – 137.

Rigatelli, L. T. (1996). *Evariste Galois*, Basel: Birkhauser.

Rotmanm J. (1998). *Galois theory.* New York: Springer.

Shakespeare, W. (1968). *Twelfth Night.* London: Penguin Books.

Stewart, I. (1973). *Galois theory.* London: Chapman and Hall Ltd.

Tignol, J. P. (2001). *Galois's theory of algebraic equations.* Singapore: World Scientific.

Van der Waerden, B. L. (1953). *Modern algebra.* New York: Ungar.