THE KRONECKER WEBER THEOREM AND CONCEPTS IN ALGEBRAIC NUMBER THEORY

by

Marla Schnall
A Thesis
Submitted to the
Graduate Faculty
of
George Mason University
in Partial Fulfillment of
The Requirements for the Degree
of
Master of Science
Mathematics

Committee:

	Dr. Jay Shapiro, Thesis Director
	Dr. Flavia Colonna, Committee Member
	Dr. John Kulesza, Committee Member
	Dr. David Walnut, Department Chairperson
	Dr. Richard Diecchio, Interim Associate Dean for Student and Academic Affairs, College of Science
	Dr. Peggy Agouris, Interim Dean, College of Science

Date: 4/28/14

Spring Semester 2014
George Mason University
Fairfax, VA

The Kronecker Weber Theorem and Concepts in Algebraic Number Theory

A thesis submitted in partial fulfillment of the requirements for the degree of Master of Science at George Mason University

By

Marla Schnall
Bachelor of Arts
Yale College, 1986

Director: Dr. Jay Shapiro, Professor
Department of Mathematics

Spring Semester 2014
George Mason University
Fairfax, VA

Table of Contents

Abstract

THE KRONECKER WEBER THEOREM AND CONCEPTS IN ALGEBRAIC NUMBER THEORY

Marla Schnall, MS

George Mason University, 2014

Thesis Director: Dr. Jay Shapiro

The Kronecker-Weber Theorem states that all abelian extensions are subfields of cyclotomic fields. This paper considers a proof based on foundational concepts in algebraic number theory that was presented by Greenberg in the 1970s. These concepts include rings of integers as Dedekind domains, finite fields and residue extensions, ramified primes, properties of cyclotomic extensions, the norm of an element and the discriminant of an extension.

The proof shows that all abelian extensions are subfields of cyclotomic extensions by breaking the problem down to cases of prime power order. An argument is made that is analagous to the Chinese Remainder Theorem that the Galois group of the compositum of two field extensions is direct product of the Galois group of each field extension. The proof breaks down further into two cases, odd primes and powers of 2. The result then relies on theorems pertaining to the ramified prime in any given extension. It can be shown that for the odd primes only one prime not dividing the order is ramified in an abelian extension or the only ramified prime in the extension divides the order. Then it can be shown that this extesion is a subfield of a cyclotomic extension. A inductive argument based on valuation theory is used to prove the power of 2 case.

Chapter 1: Basics of Galois Theory

1.1 Introduction

Everiste Galois was born in 1811 and died 20 short years later in a duel. While there has been a great deal written about Galois' turbulent and short life, it is the mathematics that he created that overshadows the drama of his romantic and political activities . The focus of Galois' research was finding a general formula for solutions of all polynomials with rational coefficients by radicals. The key result of his research was that there is no general solution by radicals for polynomials of degree greater than or equal to five. In establishing this result, he created the machinery of Galois Theory, which explores the structure of the automorphism groups of splitting fields of polynomials.

The Inverse Galois problem breaks down into two important questions. First, given a group G and a field F, is there a Galois extension L of F whose Galois group is G. In addition, once we have identified the extension, how do we find the polynomial with coefficients in F whose splitting field is L. This is still an open question for every group over every field. Also, there is current work being done to determine generic forms of polynomials whose splitting field is a Galois group G over $\mathbb{Q}$. The focus of the thesis will be on abelian extensions, polynomials whose Galois groups are abelian. The key theorem concerning these extensions is the Kronecker-Weber theorem, which states that all abelian extensions of $\mathbb{Q}$ are subfields of cyclotomic extensions: extensions created by adjoining roots of unity. After establishing some important concepts in abstract algebra and algebraic number theory, this thesis will conclude with a proof of this theorem.

1.2 Field Extensions and Splitting Fields of Polynomials

For a given field K, we can construct an extension of the field L such that K is a subfield of L and L is a finitely generated vector space over K. An algebraic extension of K is an extension where every element is a root of a polynomial with coefficients in K. As an example, consider $L = \mathbb{Q}[\sqrt[3]{2}]$. This field contains all elements of the form $q + r\sqrt[3]{2} + s\sqrt[3]{4}, q, r, s \in \mathbb{Q}$. Clearly this field can be considered a vector space over $\mathbb{Q}$ with basis $\{1, \sqrt[3]{2}, \sqrt[3]{4}\}$. The dimension of this vector space is the degree of the field extension, three. This extension is clearly algebraic. The dimension of the vector space is known as the degree of the extension and is denoted as $[L : \mathbb{Q}]$.

In this thesis we will be considering field extensions which are created by adjoining roots of a given polynomial $p(x)$ with coefficients in $\mathbb{Q}$. A *splitting field* of a polynomial with coefficient in $\mathbb{Q}$ is the smallest field contained in the algebraic closure of $\mathbb{Q}$ over which a given polynomial can be split into linear factors. Every splitting field is algebraic since, by the Fundamental Theorem of Algebra, a polynomial of degree n has at most n roots and all finite extensions are algebraic. [1, p. 521] A separable polynomial is a polynomial with no repeated roots. An extension L of $\mathbb{Q}$ is called Galois if the field is a splitting field of a separable polynomial $p(x)$. Every irreducible polynomial over $\mathbb{Q}$ is separable. [1, p. 547] Consider our example field L above. This extension of $\mathbb{Q}$ is not Galois, because there is no polynomial with coefficients in $\mathbb{Q}$ that factors completely into linear factors whose elements are in L. Clearly, the simplest polynomial with coefficients in $\mathbb{Q}$ that would factor over this extension would be $x^3 - 2$. This factors as $(x - \sqrt[3]{2})(x^2 + \sqrt[3]{2} + \sqrt[3]{4})$. The roots of the second factor are complex so in order to factor this polynomial completely we will need i, but $i \notin L$.

1.3 Degree of Splitting Fields and Primitive Elements

There is an important relationship between the dimension of a splitting field L over K as a vector space and the degree of the polynomial for which L is the splitting field.

Let us consider again our example, $f(x) = x^3 - 2$. The solution set of $f(x) = 0$ is $\{\sqrt[3]{2}, \sqrt[3]{2}(\frac{-1+i\sqrt{3}}{2}), \sqrt[3]{2}(\frac{-1-i\sqrt{3}}{2})\}$ from which it follow that $\mathbb{Q}[i\sqrt{3}]$ is in the splitting field of $f(x)$. What is the dimension of the splitting field of this polynomial as a vector space over $\mathbb{Q}$ and how can we characterize a set of elements that form a basis of this vector space? Consider first the subfield, $L = \mathbb{Q}[i\sqrt{3}]$ of the splitting field. Now we can show that $\{1, i\sqrt{3}\}$ is a basis of this as a vector space over $\mathbb{Q}$. Because the field must be closed under addition, the field must contain all possible products and sums of all elements in the field. Consider two elements, $a + bi\sqrt{3}$ and $c + di\sqrt{3}$. Their sums clearly are linear combinations of the elements. Their product would be $ac - 3bd + (bc + ad)i\sqrt{3}$. So, the set $\{1, i\sqrt{3}\}$ spans $\mathbb{Q}[i\sqrt{3}]$ as a vector space over $\mathbb{Q}$. Clearly, the elements are linearly independent. Therefore, by definition, the degree of the extension is 2.

Now consider the splitting field of $x^3 - 2$. So, we have $K = L[\sqrt[3]{2}]$. The elements $1, i\sqrt{3}, \sqrt[3]{2}, \sqrt[3]{4}$ are clearly in K but do they form a basis? Again, since the splitting field must be closed under multiplication, it must also include $(i\sqrt{3})(\sqrt[3]{2}) = i\sqrt[6]{108}$ and $(i\sqrt{3})(\sqrt[3]{4}) = i\sqrt[6]{432}$. Clearly, these elements are linearly independent. The question is: would they span the vector space. If they do, then, as a vector space over $\mathbb{Q}$ this splitting field has dimension 6, so the degree of the extension is 6. We can see that multiplying any pair of these elements together will yield another element that can be expressed in terms of another of these elements. In order to make this more apparent, we can express our basis in terms of sixth roots: $\{\sqrt[6]{4}, \sqrt[6]{16}, i\sqrt[6]{27}, i\sqrt[6]{108}, i\sqrt[6]{432}\}$

$$
\begin{aligned}
i\sqrt[6]{432} \times i\sqrt[6]{27} &= -3\sqrt[6]{16} \\
i\sqrt[6]{432} \times \sqrt[6]{4} &= 2i\sqrt[6]{27} \\
i\sqrt[6]{432} \times \sqrt[6]{16} &= 2i\sqrt[6]{108} \\
i\sqrt[6]{432} \times i\sqrt[6]{108} &= -6 \\
i\sqrt[6]{108} \times i\sqrt[6]{27} &= -3\sqrt[6]{4} \\
i\sqrt[6]{108} \times \sqrt[6]{4} &= i\sqrt[6]{432} \\
i\sqrt[6]{108} \times \sqrt[6]{16} &= 2i\sqrt[6]{27}
\end{aligned}
$$

So, it would seem that these six elements span the splitting field of $f(x)$ and therefore form a basis as a vector space over $\mathbb{Q}$. The next two theorems will show us that the dimension of this extension cannot be more than 6, so then we can be certain that the dimension of this splitting field is 6.

Theorem 1.1. *Let $F \subseteq K \subseteq L$ be fields. Then $[L : F] = [L : K][K : F]$.*

Proof. Suppose that $[L : K] = m$ and $[K : F] = n$. Define $\{\alpha_1, ...\alpha_n\}$, a basis for the extension K/F as a vector space and $\{\beta_1, ...\beta_m\}$, a basis for L/K as a vector space. Clearly, the set $S = \{\alpha_i\beta_j : 1 \leq i \leq n, 1 \leq j \leq m\}$ spans L. It remains to show that the elements of S are linearly independent. Suppose that they are not. Then, there exists $b_{ij} \neq 0$ for some i, j and

$$\sum_{i \leq n, j \leq m} b_{ij}\alpha_i\beta_j = 0.$$

Now, we can express this sum as

$$\alpha_1 \sum_{j=1}^{m} b_{1j}\beta_j + ...\alpha_n \sum_{j=1}^{m} b_{nj}\beta_j.$$

Since the α_i are linearly independent, then each $\sum_{j=1}^{m} b_{ij}\beta_j = 0$. But, since the β_j are also linearly independent, then each $b_{ij} = 0$. So we have a contradiction and the dimension of the vector space is mn.[1, p.523] □

Definition 1.2. *A* primitive element *of a field extension L of F is an element θ such that $L = F[\theta]$.*

Now we can state an important connection between the field generated by one root of a polynomial and the degree of that polynomial.

Theorem 1.3. *If θ is a root of $p(x) \in F[x]$, and p(x) is irreducible, then $[F[\theta] : F]$ equals the degree of p(x).*

We will begin the proof with a lemma.

Lemma 1.4. *Let $p(x) \in F[x]$ be an irreducible polynomial of degree n over the field F and let K be the field $L = F[x]/p(x)$. Let $\theta = x mod\ p(x) \in K$. Then the elements $1, \theta, \theta^2, ...\theta^{n-1}$ are a basis for K as a vector space over F, so the degree of the extension $[K : F] = n$.*

Proof. The ring homomorphism $\phi : F[x] \to L$ has the kernel $(p(x))$. Therefore $\phi(x) = \theta$. Because $F[x]$ is a Euclidean domain, for any $a(x) \in K, a(x) = q(x)p(x) + r(x)$ where the degree of $r(x)$ is less than the degree of $p(x)$. Since $q(x)p(x)$ is in the kernel, every element of the field is a polynomial whose degree is less than n. Hence, the images of $1, x = \theta, x^2 = \theta^2, ...x^{n-1} = \theta^{n-1}$ span the quotient space as a vector space over F. Now we must show that the set is linearly independent. Suppose that it is not. Then there are $b_0, ...b_{n-1}$ such that

$$b_0 + b_1\theta + b_2\theta^2 ...b_{n-1}\theta^{n-1} = 0.$$

If this were so, then the image of a polynomial of degree $n-1$, $a(x) = b_0 + b_1x + b_2x^2 + ...b_{n-1}x^{n-1}$ in $F[x]/p(x)$ would be 0, implying that $a(x)$ was in the kernel and divisible by $p(x)$. But this is not possible because its degree is less then the degree of $p(x)$ and $p(x)$ is irreducible.

For $r(x) \in L$, there is a natural map $\sigma : L \to F[\theta], \sigma(\alpha) = r(\alpha)$. Under this map, α is the image of x, α^2 is the image of x^2, etc. Since, $1, \theta, \theta^2, ...\theta^{n-1}$ spans L then $1, \alpha, \alpha^2, ...\alpha^{n-1}$ span $F[\alpha]$ as a vector space over F and therefore the degree of the extension is n.[1, p. 517] □

Now we make an important assertion about the degree of any splitting field of any polynomial.

Theorem 1.5. *A splitting field of a polynomial of degree n over F is of degree at most $n!$*

Proof. The basis of this proof is the multiplicativity of degrees of field extensions. Starting with one root, α, then $F_1 = F[\alpha]$. By Theorem 2 above, we know that $[F_1 : F] \leq n$, and

equal to n if $p(x)$ is irreducible. Once we factor out $(x-\alpha)$ the remaining polynomial will have degree at most $n-1$. Adjoining a root of this polynomial, β, we have $F_2 = F_1[\beta]$ and $[F_2 : F_1] \leq n-1$. Continuing in this manner, it is clear that $[F_n : F] \leq n!$.[1, p. 558] □

1.3.1 Minimal Polynomials

A minimal polynomial of an element of an algebraic extension is the monic polynomial of least degree with coefficients in the base field that has that element as one of its roots. For example, the minimal polynomial of $\frac{-1+\sqrt{-3}}{2}$ is x^2+x+1. The other root of this polynomial is $\frac{-1-\sqrt{-3}}{2}$. We will show that if α is algebraic over K then, its minimal polynomial exists and is unique.

Theorem 1.6. *Let α be algebraic over K. Then there is a unique monic polynomial $p(x)$ irreducible in K such that α is a root of $p(x)$.*

Proof. Since α is algebraic, there is a polynomial of minimal degree $g(x)$ such that α is a root of $g(x)$. Multiplying by some constant, $g(x)$ will be monic because K is a field. Suppose that $g(x)$ were not irreducible. Then $a(x)b(x) = g(x)$. Since K is a field, if $a(\alpha)b(\alpha) = 0$, then either $a(\alpha) = 0$ or $b(\alpha) = 0$ contradicting the minimality of $g(x)$. So $g(x)$ is irreducible. Now consider another polynomial $F(x)$ for which $F(\alpha) = 0$. By the Euclidean algorithm, we know that for any $F(x), F(x) = q(x)g(x)+r(x)$ where the degree of $r(x)$ is less than the degree of $g(x)$. Substituting $x = \alpha$, we get that $F(\alpha) = q(\alpha)g(\alpha) + r(\alpha)$. Since $F(\alpha) = 0$, that would mean that $r(\alpha) = 0$. So $r(x) = 0$, that is the remainder is identically 0. That means that $g(x)$ divides all polynomials for which α is a zero and therefore it is the unique polynomial for which α is a zero of minimal degree. [1, p.520] □

1.4 Roots of Unity and Cyclotomic Polynomials

At this point, it will be useful to introduce the concept of roots of unity.

For any n, the polynomial $x^n - 1$ has n unique roots each of which is called an nth root of unity. Among these roots, some are known as primitive nth roots of unity.

Definition 1.7. *A primitive nth root of unity is a root of* $x^n - 1$ *but not a root of* $x^d - 1$ *for any* $d < n$.

An equally important concept is that of the nth cylotomic polynomial.

Definition 1.8. *The nth cyclotomic polynomial,* $\Phi_n(x)$*, is the irreducible polynomial of least degree whose splitting field is the splitting field of the polynomial* $x^n - 1$.

The primitive nth roots of unity and the extensions formed by adjoining them are an important focus for this paper. A cyclotomic extension is an extension of $\mathbb{Q}$ that is the splitting field of a cyclotomic polynomial. The notation ζ_n is used to designate a primitive nth root of unity. All the roots of the nth cyclotomic polynomial are primitive nth roots of unity. Every power of a primitive nth root of unity ζ_n is a root of unity. Therefore, the nth roots of unity form a cyclic group under multiplication and the primitive roots are generators of the group. For example, i is a primitive 4th root of unity and the 4th cyclotomic polynomial is $x^2 + 1$. The roots of this polynomial are i and $-i$, both of which generate the group of 4th roots of unity.

Every polynomial of the form $x^n - 1$ factors as $\prod_{i=1}^{n}(x - \zeta_n^i)$. We know this by the Division Algorithm and the Fundamental Theorem of Algebra which together tell us that each root of unity is a root of $f(x) = x^n - 1$ and there can be only n roots. Clearly, a cyclotomic extension will be $\mathbb{Q}[\zeta_n]$ where ζ_n is a primitive root of unity and its minimal polynomial will divide $f(x) = x^n - 1$ When n is odd, the only rational number that is a zero of $f(x)$ is 1. So we know that the cyclotomic polynomial will be a factor of $\frac{x^n-1}{x-1}$. We can show that when n is prime, that this polynomial is irreducible using Eisenstein's Criterion and substituting $x + 1$ for x. Then

$$\frac{(x+1)^p - 1}{x} = x^{p-1} + \binom{p}{p-1}x^{p-2} + ...\binom{p}{2}x + \binom{p}{1}.$$

This polynomial is irreducible because p divides all the coefficients except the leading coefficient and p^2 does not divide the constant term. Therefore, for all odd prime cyclotomic extensions, the cyclotomic polynomial is $\sum_{i=0}^{p-1} x^i$.[1, pgs. 308 and 541]

When n is not prime, we can express the polynomial $x^n - 1$ as the product of cyclotomic polynomials of degree p where p is a prime dividing n and the nth cyclotomic polynomial. Furthermore, the nth cyclotomic polynomial is of degree $\phi(n)$ where ϕ is the Euler totient function. Consider ζ_n where $p|n$. Then $\frac{n}{k} = p$ and $(\zeta_n^{ik})^p$, where $i = 1, 2, ...(p-1)$, are all clearly pth roots of unity and therefore, since p is prime, the pth cyclotomic polynomial has $p-1$ roots therefore $\prod_{i=1}^{p-1}(x - \zeta_n^{ik}) = \Phi_p(x)$ We can repeat this process for all primes dividing n. Then since each $(x - \zeta_n^i)$ is a factor of $x^n - 1$, then $x^n - 1 = (x-1)(\prod_{p|n} \Phi_p(x))g(x)$, where $g(x) = \prod_{(i,n)=1}(x - \zeta_n^i)$. We can see that each of these ζ_n^i is a primitive nth root of unity, because for no $m < n$ will $\zeta_n^{im} = 1$. Therefore, $g(x) = \Phi_n(x)$ and its degree is $\phi(n)$.

1.5 Galois Groups of Field Extensions

Now we turn to the fundamental ideas of Galois theory. For each field extension K of a base field F, there is a set of automorphisms which we will call $Aut(K)$. These automorphisms form a group under composition. The elements of $Aut(K)$ which fix F, known as $Aut(K/F)$ are a subgroup of $Aut(K)$. This is called the Galois group of (K/F). We can see that the Galois group is a subgroup because because $Aut(K/F)$ contains the identity and if σ and τ fix F clearly $\sigma\tau$ and σ^{-1} will also fix F. It is always true that $|Aut(K/F)| \leq [K : F]$ and an extension is called a Galois extension if $|Aut(K/F)| = [K : F]$. An extension is called abelian if the Galois group of that extension is abelian. We will assert without proof here one very important result of Galois theory. An extension K of F is Galois if it is a splitting field of a separable polynomial, that is a polynomial with no repeated roots.[1, p. 572]

Recall that in $\mathbb{Q}[x]$ every irreducible polynomial is separable.

Let us consider two polynomials we have discussed and their splitting fields, x^3-2 and x^2+1. They are both separable. First let us consider the splitting field of x^2+1. The factors of the polynomial are $(x+i)(x-i)$. The splitting field therefore is $\mathbb{Q}[i]$. So the elements of this splitting field are of the form $a+bi$. How can we categorize the automorphisms that do not alter the elements of the base field in any field extension? We must consider what the map will do to $a+bi$ when $b \neq 0$. This leads us to a fundamental concept in Galois theory.

Theorem 1.9. *Let K/F be a field extension and let $\alpha \in K$ be algebraic over F. Then for any $\sigma \in Aut(K/F), \sigma\alpha$ is a root of the minimal polynomial of α over F. Furthermore, any polynomial with α as a root, also has $\sigma\alpha$ as a root.*

Proof. Suppose α satisfies the equation

$$a_n\alpha^n + a_{n-1}\alpha^{n-1} + \cdots + a_1\alpha + a_0 = 0$$

where $a_n, ...a_0 \in F$. Recall that σ is a ring homomorphism and therefore an additive and a multiplicative homomorphism. Therefore, when we apply σ to the equation above we get

$$a_n\sigma(\alpha^n) + a_{n-1}\sigma(\alpha^{n-1}) + \cdots + a_1\sigma(\alpha) + a_0 = 0.$$

Therefore, for any polynomial for which α is a root, $\sigma\alpha$ is a root. Of course, this extends to the minimal polynomial of α. [1, p. 520] □

Corollary 1.10. *Given $\theta \in K$, where $K = [\mathbb{Q}, \theta], n = [K : \mathbb{Q}]$, the minimal polynomial of θ is $p(x) = \prod_{i=1}^{n}(x - \sigma_i(x)), \sigma_i \in G = Aut(K/\mathbb{Q})$ and the coefficients of $p(x) \in \mathbb{Q}$.*

Proof. Recall that the minimal polynomial of θ is irreducible and therefore separable and has no repeated roots. By Theorem 1.3, the degree of the extension, n, equals the degree of the minimal, $p(x)$ of θ and therefore the polynomial has n distinct roots. By the theorem above, for each $\sigma_i \in G, \sigma_i(\theta)$ is a root of $p(x)$ and therefore each $(x-\sigma_i(\theta))$ is a factor of $p(x)$.

Since, by Theorem 1.6, the minimal polynomial of θ is unique and the order of the Galois group equals the degree of the extension, n, then $p(x) = \prod_{i=1}^{n}(x-\sigma_i(x)), \sigma_i \in G = Aut(K/\mathbb{Q})$ must equal the minimal polynomial of θ and therefore its coefficients must be in $\mathbb{Q}$. $\square$

When K is an extension of $\mathbb{Q}$, this theorem allows us to characterize the elements of $Aut(K/\mathbb{Q})$. Each element of the set must map roots of the minimal polynomial to other roots of the same minimal polynomial. Therefore, in the example of $\mathbb{Q}[i]$, if we consider the element i of the extension, it is clear from the theorem that $\sigma \in Aut(\mathbb{Q}[i]/\mathbb{Q})$ is defined by $\sigma : i \to -i$. We know that since this extension is Galois, the order of the Galois group is equal to the degree of the extension, which is 2. So, we have completely defined $Aut(K/F)$; it is the simple group of order 2.

Now, let us consider the other example that we have discussed above, the splitting field of $x^3 - 2$. Using the concept of roots of unity, it is clear that

$$x^3 - 2 = (x - \sqrt[3]{2})(x - \zeta_3\sqrt[3]{2})(x - \zeta_3^2\sqrt[3]{2})$$

and the splitting field will be $K = \mathbb{Q}[\zeta_3, \sqrt[3]{2}]$. For simplicity, we will use $\zeta = \zeta_3$. The fixed field F of the Galois group is $\mathbb{Q}$. This extension is Galois, because it is the splitting field of a separable polynomial. What is the structure of the Galois group? We know from Theorem 1.5 that the order is no more than 6. Now, we must consider the minimal polynomials of each element of the field extension. First, the minimal polynomial of ζ is x^2+x+1. The two roots of this polynomial are ζ and ζ^2. Therefore, one element of $Aut(K/\mathbb{Q})$ is $\sigma : \zeta \to \zeta^2$. The order of this element is 2. We can see this because

$$\sigma\zeta^2 = (\sigma\zeta)(\sigma\zeta) = \zeta^2\zeta^2 = \zeta \to \sigma^2 = I.$$

Another element of the field extension is $\sqrt[3]{2}$. The minimal polynomial of this element is $x^3 - 2$. We saw above that the roots of this polynomial are $\sqrt[3]{2}, \zeta\sqrt[3]{2}$, and $\zeta^2\sqrt[3]{2}$. So, we

know that $\sqrt[3]{2}$ must map to one of the roots of this polynomial and therefore we know that another element of $Aut(K/F)$ is $\tau : \sqrt[3]{2} \to \zeta\sqrt[3]{2}$. The order of this element is 3. We can see this because

$$\tau^2(\sqrt[3]{2}) = \tau(\zeta\sqrt[3]{2}) = \zeta^2\sqrt[3]{2}$$

and

$$\tau^3(\sqrt[3]{2}) = \tau(\zeta^2\sqrt[3]{2}) = \zeta^3\sqrt[3]{2} = \sqrt[3]{2} \to \tau^3 = I.$$

We know by Lagrange, that since 2 and 3 divide the order of the group, that $6\,||Aut(K/F)|$ and since by Theorem 1.5 $|Aut(K/F)| \leq 6$, $|Aut(K/F)| = 6$. We have defined four elements, $1, \sigma, \tau,$ and τ^2. The other elements of the group are the compositions of two elements, which are $\sigma\tau$, $\sigma\tau^2$ and $\tau\sigma$, $\tau^2\sigma$. Clearly, since the $|Aut(K/F)| = 6$ these four elements are not distinct. We can examine the effect of the $\sigma\tau$ and $\tau\sigma$ on our basis elements.

$$\sigma\tau(\sqrt[3]{2}) = \sigma(\zeta\sqrt[3]{2}) = \zeta^2\sqrt[3]{2}$$

$$\tau\sigma(\sqrt[3]{2}) = \tau(\sqrt[3]{2}) = \zeta\sqrt[3]{2}$$

Clearly, this group is not abelian, so we can propose that $\sigma\tau = \tau^2\sigma$. To check, we can again consider the effect of the map on $\sqrt[3]{2}$.

$$\tau^2\sigma(\sqrt[3]{2}) = \tau^2(\sqrt[3]{2}) = \tau(\zeta\sqrt[3]{2}) = \zeta^2\sqrt[3]{2}$$

So, now we understand the nature of the Galois group, and it is clearly S_3 the smallest non-abelian group.

1.5.1 The Fundamental Theorem of Galois Theory

This leads us to the basic organizing theorem of Galois theory, which gives a relationship between the subgroups of the Galois group, G, of K/F and the subfields of K containing F.

In order to follow the proof of the Kronecker-Weber theorem, the crucial result is that there is an inclusion-reversing correspondence between the subgroups of G, H_1 and H_2 and their corresponding fixed fields E_1 and E_2. That means that $E_1 \subseteq E_2$ if and only if $H_2 \leq H_1$. So, a smaller subgroup of G corresponds to a larger fixed field extension of F and when the subgroup is the identity, then the fixed field is the entire extension. In addition, we can make a stronger assertion for normal subgroups. If $F \subseteq E \subseteq K$ and $H \trianglelefteq G$, then $Aut(E/F) \cong G/H$ and the extension E/F is Galois. These two assertions are elements of the Fundamental Theorem of Galois Theory, the proof of which can be found in any basic algebra text. [1, p.574] The splitting field of $x^3 - 2$ gives us a good example of this theorem. Consider the two subgroups $A = \{1, \sigma\}$ and $B = \{1, \tau, \tau^2\}$ (explained on page 11) of the Galois group G. The fixed field of A is $\mathbb{Q}[\sqrt[3]{2}]$. The degree of this extension as a vector space over $\mathbb{Q}$ as we have seen above is 3 and $|A| = 2$ This extension is not Galois, that is it is not the splitting field of a polynomial. This subgroup is not normal in G,

$$\tau^2\sigma\tau(\sqrt[3]{2}) = \tau^2\sigma(\zeta\sqrt[3]{2}) = \tau^2(\zeta^2\sqrt[3]{2}) = \zeta\sqrt[3]{2}$$

while $\sigma(\sqrt[3]{2}) = \sqrt[3]{2}$. Correspondingly, the fixed field of B is $\mathbb{Q}[\zeta]$ which has degree 2 and $|B| = 3$. The subgroup B is normal in G, as we can see by

$$\sigma\tau\sigma(\sqrt[3]{2}) = \zeta^2\sqrt[3]{2} = \tau^2(\sqrt[3]{2})$$

$$\sigma\tau^2\sigma(\sqrt[3]{2}) = \zeta\sqrt[3]{2} = \tau(\sqrt[3]{2}).$$

This fixed field is the splitting field of $p(x) = x^2 + x + 1$ and is therefore Galois.

1.6 Norms and Discriminants

For each element of an algebraic extension of $\mathbb{Q}$ there are two important measures known as the norm and the discriminant. For each element of an algebraic extension, θ, of an

extension K of any field F, where $\sigma_i \in Aut(K/F)$, the norm is defined as follows.

Definition 1.11. *The norm of an element theta of an algebraic extension of degree n, is defined as* $N_{K/F}(\theta) = \prod_{\sigma_i \in G} \sigma_i(\theta), G = Aut(K/F)$.

Now consider the norm of a primitive element θ of K where $K = \mathbb{Q}[\theta]$. Then, by Corollary 1.10, the minimal polynomial has n unique roots and the minimal polynomial is

$$\prod_{i=1}^{n}(x - \sigma_i(\theta)).$$

It is easy to see from the equations above, that for a primitive element, the constant term of the minimal polynomial, C, is equal to the norm, up to sign. When the degree of the extension is even, $N(\theta) = C$ and when the degree of the extension is odd $N(\theta) = -C$. Also, note that the norm is dependent on the particular extension of the base field, since it is the product of all Galois conjugates.

We can also show two other important properties of the norm.

Theorem 1.12. $N_{K/F}(\alpha\beta) = N_{K/F}(\alpha)N_{K/F}(\beta)$.

Proof. This property is evident from the fact that $\sigma(\alpha\beta) = \sigma(\alpha)\sigma(\beta)$ for all $\sigma \in Aut(K/F)$. □

Theorem 1.13. $N_{K/F}(r\alpha) = r^n N_{K/F}(\alpha), r \in F, [K : F] = n$.

Proof.

$$N_{K/F} = \prod_{i}^{n} \sigma_i(r\alpha)$$

$$N_{K/F} = \prod_{i}^{n} r\sigma_i(\alpha)$$

$$N_{K/F} = r^n N_{K/F}(\alpha)$$

□

Another important number associated with each element in an algebraic number field and its corresponding minimal polynomial is its discriminant. The discriminant can be defined in many ways, but for our purposes the most useful definition is as follows.

Definition 1.14. $\Delta(\alpha) = \prod_{1 \le i < j < n} (\alpha_i - \alpha_j)^2$ *where* α_i *is a root of the minimal polynomial of* α.

The norm and the discriminant of a primitive element α of the extension K of F with a minimal polynomial $f(x)$ are related by the theorem below.

Theorem 1.15. *Given* α*, a primitive element of* K/F *with a minimal polynomial f(x) where* $\sigma_i \in Aut(K/F)$ *and* $\alpha_i = \sigma_i(\alpha)$*,*

$$\Delta(\alpha) = (-1)^{\binom{n}{2}} N_{K/F}(f'(\alpha)).$$

Proof. Recall that the discriminant is

$$\Delta(\alpha) = \prod_{1 \le i < j < n} (\alpha_i - \alpha_j)^2.$$

Since there are $\binom{n}{2}$ terms, each of which is squared in the discriminant and noting that

$$(\alpha_i - \alpha_j)^2 = -(\alpha_i - \alpha_j)(\alpha_j - \alpha_i),$$

we can rewrite the discriminant as

$$\Delta(\alpha) = (-1)^{\binom{n}{2}} \prod_{i \neq j} (\alpha_i - \alpha_j) = (-1)^{\binom{n}{2}} \prod_{i} \prod_{i \neq j} (\alpha_i - \alpha_j).$$

Now note that we can express the minimal polynomial of α as

$$f(x) = \prod_i (x - \alpha_i)$$

and therefore

$$f'(x) = \sum_k \prod_{j \neq k} (x - \alpha_j) \text{ and so } f'(\alpha_i) = \prod_{i \neq j} (\alpha_i - \alpha_j).$$

Substituting in the expression above, we have an expression for the discriminant

$$\Delta(\alpha) = (-1)^{\binom{n}{2}} \prod_i f'(\alpha_i).$$

Recall that since the elements of the Galois group fix the base field and the coefficients of the derivative of the minimal polynomial are in the base field, then

$$\sigma_i(f'(\alpha)) = f'(\sigma_i(\alpha)) = f'(\alpha_i).$$

Therefore, we have proved the assertion, given that that $N_{K/F)}(\beta) = \prod_i \sigma_i(\beta)$,

$$\Delta(\alpha) = (-1)^{\binom{n}{2}} N_{K/F}(f'(\alpha)).$$

□

The discriminants of primitive roots of unity are of particular interest in this paper. We can compute directly the discriminant for a prime root of unity by the equation below.

Theorem 1.16. *The discriminant of a primitive pth root of unity, $p \geq 3$, ζ_p is given by*

$$\Delta(\zeta_p) = (-1)p^{\frac{p-1}{2}} p^{p-2}.$$

Proof. We will start with the following lemma.

Lemma 1.17. *The norm of* $(\zeta_p - 1)$ *where* p *is prime and* $p \geq 3$ *and and* ζ_p *is a primitive* p*th root of unity is* p*.*

First find a polynomial, such that $(\zeta - 1)$ is a zero.

$$x - (\zeta_p - 1) = 0$$

$$x + 1 = \zeta_p$$

$$(x+1)^p = 1$$

$$x^p + px^{p-1} + \binom{p}{p-2}x^{p-2} ... + px + 1 = 1$$

$$x^p + px^{p-1} + \binom{p}{p-2}x^{p-2} ... + px = 0$$

$$x(x^{p-1} - px^{p-2} + \binom{p}{p-2}x^{p-3} ... + p) = 0$$

The polynomial $f(x) = x^{p-1} + px^{p-2} + \binom{p}{p-2}x^{p-3} ... + p$ is irreducible by Eisenstien's criterion and since $(\zeta_p - 1)$ is clearly a root $f(x)$, $f(x)$ must be the minimal polynomial of $(\zeta_p - 1)$. As we have seen above, the norm of an element is the constant term of its minimal polynomial when the degree is even and therefore, $N_{\mathbb{Q}[\zeta_p]}(\zeta_p - 1) = p$.

Now we can find the discriminant of the pth cyclotomic polynomial $\Phi(p)$ noting that

$$x^p - 1 = (x-1)\Phi(p).$$

Taking the derivative we have

$$px^{p-1} = x\Phi'(p) + \Phi(p) - \Phi'(p).$$

Evaluating at ζ_p,

$$p\zeta_p^{p-1} = (\zeta_p - 1)\Phi'(\zeta_p).$$

Taking the norm of both sides, we have

$$N_{\mathbb{Q}[\zeta_p]}(p\zeta_p^{p-1}) = N_{\mathbb{Q}[\zeta_p]}(\zeta_p - 1)\Phi'(\zeta_p)).$$

From theorems 1.11 and 1.12, Lemma 1.6 and the fact that the degree of the extension is $p-1$, we have

$$p^{n-1}N_{\mathbb{Q}[\zeta_p]}(\zeta_p^{p-1}) = pN_{\mathbb{Q}[\zeta_p]}(\Phi'(\zeta_p)).$$

Finally, for any primitive pth root of unity

$$N_{\mathbb{Q}[\zeta_p]}(\zeta_p) = \prod_{i=1}^{p-1} \zeta_p^i = \zeta_p^{\frac{p(p-1)}{2}} = 1.$$

So, by the above and Theorem 1.11,

$$N(f'(\zeta_p)) = p^{p-2},$$

and therefore by Theorem 1.13

$$\Delta(\zeta_p) = (-1)^{\frac{(p-1)(p-2)}{2}} p^{p-2} = (-1)^{\frac{(p-1)}{2}} p^{p-2}.$$

□

A generalization of this result is an important building block of Greenberg's proof of the Kronecker-Weber Theorem.

Chapter 2: Ring Theory and Algebraic Number Theory

2.1 Rings, Domains and Ideals

We establish here some basic concepts of ring theory. A ring is a set with multiplication and addition in which every nonzero element does not necessarily have a multiplicative inverse. Those elements of a ring which have multiplicative inverses are known as units of the ring. An ideal of a ring is a subset of the ring, that is closed under addition and closed under multiplication by the entire ring. In the integers, for example, the set of any multiples of any number other than ± 1 is an ideal. In this paper, we will consider only proper ideals, ideals that are not equal to the entire ring. One very important concept in ring theory is the prime ideal.

Definition 2.1. *A prime ideal is an ideal P of a ring R such that if $a, b \in R$ and $ab \in P$ then either $a \in P$ or $b \in P$.*

A domain is a ring R in which, whenever $a, b \in R$ and $ab = 0$, then $a = 0$ or $b = 0$. A principal ideal domain (PID) is a domain in which all proper ideals can be generated by one element. A unique factorization fomain (UFD) is a ring in which all elements have a unique prime factorization. The integers are an illustrative example of a UFD. Principal ideal domains are all unique factorization domains.

A Noetherian Ring is a ring where all ideals satisfy an ascending chain condition, which means that for every chain of ideals, $I_1 \subseteq I_2 \subseteq I_3 \cdots \subseteq I_k \ldots$, there is some k such that if $i \geq k$ then $I_i = I_{i+1} = I_{i+2} \ldots$ Another important property of Noetherian rings is proved below.

Theorem 2.2. *Every ideal of a Noetherian ring is finitely generated.*

Proof. Since all ideals satisfy an ascending chain condition, every non-empty set of ideals has a maximal element. Consider any non-empty set Σ of ideals. Suppose I_1 is a maximal element. Then our proposition is proved. Suppose not. Then by the ascending chain condition, there is an I_2 such that $I_1 \subseteq I_2$. If I_2 is not maximal, then we can find an I_3 that contains both. If we can continue this process forever, then we can create an infinitely ascending chain, which contradicts the ascending chain condition. Therefore, each chain must contain a maximal element. Now we must show that every ideal is finitely generated. Let I be an ideal of a Noetherian ring R. Let Σ be the set of all finitely generated ideals such that $S \in \Sigma \rightarrow S \subseteq I$. This set is non-empty because $(0) \in \Sigma$. By above, Σ has a maximal element I_1. If $I_1 \neq N$ then there is some x such that $x \in I_1$ and $x \notin I$. So, since I_1 is finitely generated, then the ideal generated by I_1 and x is also finitely generated, contradicting the maximality of I_1. Therefore, N is finitely generated. [1, p.458,656] $\square$

2.2 Integrally Closed Rings

For any domain, R, a field called the field of fractions, is the field formed by dividing by every non-zero element of the domain. For the integers, this field is the rationals. Consider a field K such that $R \subset K$. Then $x \in K$ is called integral over R if it is the root of a monic polynomial with coefficients in R. A domain $R \subset K$ is called *integrally closed* in K if for any $x \in K$, if x is integral over R, then $x \in R$. This leads us to important result.

Theorem 2.3. *The integers are integrally closed.*

Proof. Consider $\frac{r}{s}$ where r and s are integers and $\frac{r}{s}$ is in reduced form. If $\frac{r}{s}$ is the root of

a monic polynomial with integer coefficients, then

$$(\frac{r}{s})^n + a_{n-1}(\frac{r}{s})^{n-1} + ...a_0 = 0$$

$$a_{n-1}(\frac{r}{s})^{n-1} + ...a_0 = -(\frac{r}{s})^n$$

$$a_{n-1}r^{n-1}s + a_{n-1}r^{n-2}s^2 + ...a_0s^n = -r^n$$

$$s(a_{n-1}r^{n-1} + a_{n-1}r^{n-2}s + ...a_0s^{n-1}) = -r^n$$

Since r, s, a_i are all integers and r and s are relatively prime, and it is clear from the equation above that s must divide $r, s = 1$ and therefore, $\frac{r}{s}$ is an integer. □

An important object that we will be considering is the integral closure of a subring.

Definition 2.4. *If R and L are rings $R \subseteq L$, the integral closure of R in L is the set of elements of L that are integral over R.*

We will now consider some important properties of the elements of a ring that are integral over a subring. We will start with the following statement, which we will assert without proof.

Theorem 2.5. *Let R and S be commutative rings with identity and $R \subseteq S$. Then the following are equivalent:*

(1) $s \in S$ is integral over R.

(2) $R[s]$ is a finitely generated $R-$module.

(3) $s \in T$ for some subring T, $R \subseteq T \subseteq S$, that is a finitely generated $R-$module.

Several important results follow from this theorem.

Theorem 2.6. *Let R and S be as above, then:*

(a) The integral closure of R in S is a subring of S.

(b) Integrality is transitive, ie, if S is a subring of T and T integral over S and S is integral

over R then T is integral over R.

(c) The integral closure of R in S is integrally closed.

Proof. (1)If two elements of S, g and h are integral over R, then by 2 above, $R[g]$ and $R[h]$ are finitely generated $R-modules$. Therefore $R[g,h]$ must also be a finitely generated $R-module$ which contains $g+h$ and gh. So by 3 above, $g+h$ and gh are integral over R. So, for any two elements integral over R, their sum and product are also integral over R. Therefore, the integral closure of R forms a subring of S.
(2) Suppose that $R \subseteq S \subseteq T$ and T is integral over S and S is integral over R. Then,using (3) above, we must show that every $t \in T$ is an element of some finitely generated $R-module$. We know that for every $t \in T$, t is a root of a monic polynomial, $p(x)$, with coefficients in S. Since S is integral over R, $R[a_i]$ is a finitely generated $R-module$, by (2) above. So $R_1 = R[a_0, a_1, \ldots, a_{n-1}]$ is also a finitely generated $R-module$. Since t is a root of $p(x)$ with coefficients in R_1 and $p(x)$ is monic, then t is integral over R_1. So, $R_1[t]$ is finitely generated and since R_1 is a finitely generated $R-module, R[t]$ is a finitely-generated $R-module$ and T is integral over R. (3) By (1) we know that the integral closure of a ring is a possibly larger subring M contained in S. We know by (2) that the integral closure of M is integral over R. Therefore, the integral closure of M must equal M. If it did not, then M would not contain all elements integral over R.[1, p.692-693] □

The ring of integers is the integral closure of the integers in K. That is, it is the ring formed by all the elements of K that are roots of a monic polynomial with integer coefficients. The ring of integers of an algebraic extension K of $\mathbb{Q}$ denoted as $\mathcal{O}_K$ is fundamental to the proof of the Kronecker-Weber theorem. Since $\mathbb{Z}$ is a subring of any extension of $\mathbb{Q}$, by Theorem 2.6 above, we know that this is an integrally closed ring. This is one of three conditions of the structure known as a Dedekind domain.

Definition 2.7. *A domain R is a Dedekind domain if it has the following properties:*

(1) R is Noetherian.

(2) R is integrally closed.

(3) All prime ideals of R are maximal.

What is most interesting is that this condition is equivalent to the statement that every ideal factors uniquely into prime ideals. [4, p. 28] This is analogous to the concept of a UFD, except the unique factorization is at the level of ideals instead of elements. It is a well known result of algebraic number theory that all rings of integers also satisfy conditions (2) and (3) and therefore that all rings of integers are Dedekind domains. [4, p.42]

It is important to understand factoring of prime ideals, so we will consider an example. The ring, $R = \mathbb{Z}[\sqrt{-5}]$ is a Dedekind domain. [This is the ring of integers for the field $\mathbb{Q}[\sqrt{-5}]$.] For the element 6 we can consider two factorizations, $6 = (2)(3)) = (1+\sqrt{-5})(1-\sqrt{-5})$. Note also that the ideal generated by neither 2 nor 3 of this ring is prime, because $6 \in (2)$ and $6 \in (3)$ but $(1+\sqrt{-5}), (1-\sqrt{-5}) \notin (2), (3)$. In fact, this ring is not a Principal Ideal Domain, so prime ideals are not necessarily generated by one element. We can understand factorization in this domain by considering the product $I^2, I = (1+\sqrt{-5}, 2)$. We can show that this product exactly equals the ideal generated by 2. Recall that the product of the two ideals I and J is defined as $\sum \alpha\beta$ when $\alpha \in I$ and $\beta \in J$. Therefore the generators of this ideal are

$$-4 + 2\sqrt{-5}, 4, 2 + 2\sqrt{-5}$$

so clearly, $I^2 \subseteq (2)$. In fact, $I^2 = (2)$. The number 2 is irreducible in this ring and is not the product of any two elements but it is still in the ideal as we see below

$$-4 + 2\sqrt{-5} + (-2 - 2\sqrt{-5}) + 4 + 4 = 2$$

Therefore, $I^2 = (2)$. Because this ring is a Dedekind domain, this is the unique prime factorization of (2) in $\mathbb{Z}[\sqrt{-5}]$.

2.3 Decomposition Groups, Inertia Groups and Ramification

One important piece of machinery that is needed for Greenberg's proof is the concept of a ramified prime. Consider an algebraic extension K over $\mathbb{Q}$ and an algebraic extension L over K of degree n. The integral closure of the integers in K and L, denoted as $\mathcal{O}_K$ and $\mathcal{O}_L$ respectively, are known as the rings of integers of K and L. As shown above, these are both Dedekind domains and therefore their ideals have a unique factorization of ideals and all prime ideals are maximal. Now consider a prime ideal $\mathfrak{p}_K$ of $\mathcal{O}_K$ and the ideal $\mathfrak{p}_K\mathcal{O}_L$. Denote $\mathcal{B}_p = \{\mathfrak{p}_i\}$ the set of all the prime ideals of $\mathcal{O}_L$ that lie over $\mathfrak{p}_K$. Then,

$$\mathfrak{p}_K\mathcal{O}_L = \prod_{i=1}^{g} \mathfrak{p}_i^{e_i}.$$

The number g is called the decomposition index of p. For a given $\mathfrak{p}_i$ if $\mathfrak{p}_i \cap \mathcal{O}_K = \mathfrak{p}_K$ then $f_i = [\mathcal{O}_L/\mathfrak{p}_i : \mathcal{O}_K/\mathfrak{p}_K]$. It is clear that only prime ideals lying over $\mathfrak{p}_K$ can be prime factors of $\mathfrak{p}_K\mathcal{O}_L$. The next two theorems will show us an important relationship among e_i, f_i and g.

Theorem 2.8. *Given $L/K/\mathbb{Q}$ an algebraic extension and $\mathfrak{p}_K$ is a prime ideal of $\mathcal{O}_K$ and each $\mathfrak{p}_i$ is a prime ideal of $\mathcal{O}_L$ lying over $\mathfrak{p}_K$ and*

$$\mathfrak{p}_K\mathcal{O}_L = \prod_{i=1}^{g} \mathfrak{p}_i^{e_i},$$

then for each $e_j = e_{L/K}(\mathfrak{p}_j)$ and $f_j = f_{L/K}(\mathfrak{p}_j)$

$$\sum_{i=1}^{g} e_i f_i = [L : K].$$

Proof. We begin the proof with a lemma.

Lemma 2.9. *Let R be a Dedekind domain and let I be an ideal of R such that*

$$I = \prod_{i=1}^{r} \mathfrak{p}_i^{a_i}$$

where each $\mathfrak{p}_i$ is a distinct prime ideal of R, then

$$|R/I| = \prod_{i=1}^{r} |R/\mathfrak{p}_i|^{a_i}.$$

Proof. By the Chinese remainder theorem,

$$R/I \cong R/\mathfrak{p}_1^{a_1} \times R/\mathfrak{p}_2^{a_2} ... \times R/\mathfrak{p}_r^{a_r}.$$

The ith prime factor of I occurs a_i times and therefore our lemma is proved. □

Now we can see also see that $[\mathcal{O}_L/\mathfrak{p}_i^{e_i} : \mathcal{O}_L/\mathfrak{p}_i] = e_i$ because if $n = |\mathcal{O}_L/\mathfrak{p}_i|$ then $|\mathcal{O}_L/\mathfrak{p}_i^{e_i}| = n^{e_i}$. Then we can see that

$$[\mathcal{O}_L/\mathfrak{p}_i^{e_i} : \mathcal{O}_K/\mathfrak{p}_K] = [\mathcal{O}_L/\mathfrak{p}_i^{e_i} : \mathcal{O}_L/\mathfrak{p}_i][\mathcal{O}_L/\mathfrak{p}_i : \mathcal{O}_K/\mathfrak{p}_K] = e_i f_i.$$

Therefore, again following the lemma for each $\mathfrak{p}_i$ then

$$[\mathcal{O}_L/\mathfrak{p}_K\mathcal{O}_L : \mathcal{O}_K/\mathfrak{p}_K] = \sum_{I=1}^{g} e_i f_i.$$

It can be shown, using concepts in algebraic number theory beyond the scope of this paper, that this quantity is equal to the degree of the extension, [4, p.187] so

$$[L : K] = \sum_{I=1}^{g} e_i f_i.$$

□

Theorem 2.10. *Given $L/K/\mathbb{Q}$ an algebraic extension, $\mathfrak{p}$ a prime of $\mathcal{O}_K$ and*

$$\mathfrak{p}_K\mathcal{O}_L = \prod_{i=1}^{g} \mathfrak{p}_i^{e_i},$$

then $e_1 = e_2 = ...e_g = e$ and $f_1 = f_2 = ...f$ and $n = efg$.

Proof. It has been shown that for a given $\mathfrak{p}_i$ and $\mathfrak{p}_j$ there is a $\sigma \in G = Aut(L/K)$ such that $\sigma(\mathfrak{p}_i) = \mathfrak{p}_j$. [4, p.189] Now, since σ fixes K, $\sigma(\mathfrak{p}_K\mathcal{O}_L) = \mathfrak{p}_K\mathcal{O}_L$ which implies that

$$\prod_{i=1}^{g} \mathfrak{p}_i^{e_i} = \prod_{i=1}^{g} (\sigma(\mathfrak{p}_i))^{e_i}.$$

So, $e_i = e_j$ by uniqueness of factorization of ideals. We can also see that $f_i = f_j$ because

$$f_j = |\mathcal{O}_L/\mathfrak{p}_j : \mathcal{O}_K/\mathfrak{p}_K| = |\mathcal{O}_L/\sigma(\mathfrak{p}_i) : \mathcal{O}_K/\mathfrak{p}_K| = |\mathcal{O}_L/\mathfrak{p}_i : \mathcal{O}_K/\mathfrak{p}_K| = f_i.$$

Therefore, from Theorem 2.8, we can see that $[L : K] = efg$. [4, p.189] □

The symbol e is known as the ramification degree of $\mathfrak{p}_K$ in $\mathcal{O}_L$. If $e > 1$ then $\mathfrak{p}_K$ is called a ramified prime. If $e = 1$ then the prime is unramified. If $e = n$ then $\mathfrak{p}_K$ is totally ramified. It is known, from a formula of Minkowski that provides a lower bound on the number of ramified primes, that all extensions of $\mathbb{Q}$ of degree $n > 1$, that is all extensions except the trivial extension, have at least one ramified prime.[4, p.116] $|\mathcal{B}_p|$ is denoted as g. [2, p.602]

We will now look at these quantities e, f, g and find their correspondence to subgroups of $G = Aut(L/K)$. There will be a subgroup H of G, such that $\sigma(\mathfrak{p}_i) = \mathfrak{p}_i$ for each $\mathfrak{p}_i \in \mathcal{B}_p$. This group is known as the decomposition group of $\mathfrak{p}_k$. Each $\sigma \in H$ will also induce an automorphism on each $\mathcal{O}_L/\mathfrak{p}_i$ which will be well defined because all of H fixes all elements

of $\mathfrak{p}_i$. We will call this induced automorphism σ_0. Then, there is a map ϕ_{0_i} from G to the group G_{0_i} the set of automorphisms on $\mathcal{O}_L/\mathfrak{p}_i$. If this map is not trivial, then it has some kernel which is a normal subgroup of H, which we will call T_0. [2, p.602]

Now consider the relationship of these subgroups to e, f, g. Clearly, since H fixes any $\mathfrak{p}_i$, then $g = \frac{n}{|H|}$ will be the number of Galois conjugates of $\mathfrak{p}_i$. It has been shown that the ramification degree $e = |T_0|$. [4, p. 226] So, if T_0 is not trivial, then $\mathfrak{p}_K$ is ramified. In addition, $\mathfrak{p}_K$ is not ramified in the fixed field of T_0, K_{T_0}[4, p. 226] and the prime ideal $\mathfrak{p}_i \cap K_{T_0}$ of K_{T_0} is totally ramified in L, that is $e = [L : K_{T_0}]$. [5, p 291-2]

Since the elements of G fix K, the elements of G_0 fix $\mathcal{O}_K/\mathfrak{p}_K$ and therefore $\sigma_0 \in G_0$ implies that $\sigma_0 \in Aut(\mathcal{O}_L/\mathfrak{p}_j/\mathcal{O}_K/\mathfrak{p}_K)$. It can be shown that H/T is isomorphic to G_0 the Galois group of the extension $\mathcal{O}_L/\mathfrak{p}_j/\mathcal{O}_K/\mathfrak{p}_K$. [4, p.225] Recall that any finite field K which is an algebraic extension of $\mathbb{F}_p$ is the splitting field of the polynomial $p(x) = x^{p^n} - x$. Then $[K : \mathbb{F}_p] = n$. This extension is Galois because this polynomial is separable and generated by the Frobenius map $\sigma(\alpha) = \alpha^p$. [1, p.566] Because we know that G_0 is cyclic, we know that H/T_0 is also cyclic and generated by the coset of σ such that [4, p.230]

$$\sigma x = x^q (mod \mathcal{B}).$$

2.3.1 Discriminants and Ramified Primes

Recall that if $K = \mathbb{Q}[\alpha]$ then the discriminant α is defined as

$$\Delta_{K/\mathbb{Q}}(\alpha) = \prod_{1 \leq i < j < n} (\alpha_i - \alpha_j)^2.$$

For any finite extension $K/\mathbb{Q}$, this quantity is fixed and it is known as the discriminant of the extension. [4, p. 77] That is, for any $K/\mathbb{Q}$ where $K = \mathbb{Q}[\alpha] = \mathbb{Q}[\beta]$, then $\Delta_{K/\mathbb{Q}}(\alpha) = \Delta_{K/\mathbb{Q}}(\beta)$.

There is a fundamental relationship between ramified primes in an extension and the

discriminant of that extension. Let us consider again the example of $\mathbb{Q}[\sqrt{-5}]$. The minimal polynomial of $\mathbb{Q}[\sqrt{-5}]$ is x^2+5 and we know from elementary algebra that the discriminant of this polynomial is -20. The primes that divide 20 are 2 and 5. We have already shown that 2 is ramified, $(2) = (1+\sqrt{-5}, 2)^2$. It is obvious that 5 ramifies because $(5) = (\sqrt{-5})^2$. No other primes in this extension are ramified. We know this by the important result below. [4, p.210]

Theorem 2.11. *A prime p is ramified in the extension $K/\mathbb{Q}$ if and only if $p|\Delta_{K/\mathbb{Q}}$.*

Recalling our result for the discriminant of a primitive pth root of unity, Theorem 1.5, we know therefore that the only prime ramified in $\mathbb{Q}[\zeta_p]$ is p. Furthermore, it has been shown for any cyclotomic extension of degree of $p^n, p > 2$, that p is the only ramified prime and that p is totally ramified, that is $e = n$. [6, p. 262] In addition, for any cyclotomic extension of degree m, only the primes dividing m divide the discriminant, and therefore, the only primes ramified in $\mathbb{Q}[\zeta_m]$ are the primes dividing m. [4, p. 216]

Now that we have the basic machinery in place, we can proceed to the proof of the Kronecker-Weber Theorem.

Chapter 3: The Kronecker-Weber Theorem

3.1 Introduction to the Inverse Galois Problem

3.1.1 Example - Cyclic Group of Order 5

Recall the statement of the Kronecker-Weber Theorem

Theorem 3.1. *Any abelian extension is a subfield of a cyclotomic extension*

Although this is a very broad statement with many implications, let us consider the simple example of finding a polynomial whose Galois group is a cyclic group of order 5. Recall that if p is prime, then $G = Aut(\mathbb{Q}[\zeta_p]/\mathbb{Q})$ is cyclic and therefore there is a subgroup for every divisor d of $n = |G|$. The minimal polynomial of ζ_{11} is $x^{10} + x^9 + \cdots + 1$. Recall that if θ is a primitive element of K, and $p(x)$ of degree n is the minimal polynomial of θ, then $[F[\theta] : F] = n$ Therefore $G = Aut(\mathbb{Q}[\zeta_{11}]/\mathbb{Q})$ has order 10 and it has a subgroup of order 2 with a corresponding fixed field L where $[L : \mathbb{Q}] = 5$. For the purposes of this exercise, we will set $\omega = \zeta_{11}$. Now we consider the Galois group of this polynomial and find the polynomial that generates the subfield that has a Galois group of order 5. This will allow us to examine in detail how Galois groups work and how the groups and their subfields are related through the lens of the Fundamental Theorem of Galois Theory.

First, let us consider the elements of the Galois group. Recall that each element of the Galois group is a map from the field to itself where the roots of the minimal polynomial of an element are permuted. It turns out that a generator for the group is $\lambda : \omega \to \omega^2$.

The group structure is as follows:

$$
\begin{aligned}
\lambda(\omega) &= \omega^2 \\
\lambda^2(\omega) &= \lambda(\omega^2) &&= \omega^4 \\
\lambda^3(\omega) &= \lambda(\omega^4) &&= \omega^8 \\
\lambda^4(\omega) &= \lambda(\omega^8) &&= \omega^{16} &&= \omega^5 \\
\lambda^5(\omega) &= \lambda(\omega^5) &&= \omega^{10} \\
\lambda^6(\omega) &= \lambda(\omega^10) &&= \omega^{20} &&= \omega^9 \\
\lambda^7(\omega) &= \lambda(\omega^9) &&= \omega^{18} &&= \omega^7 \\
\lambda^8(\omega) &= \lambda(\omega^7) &&= \omega^{14} &&= \omega^3 \\
\lambda^9(\omega) &= \lambda(\omega^3) &&= \omega^6 \\
\lambda^{10}(\omega) &= \lambda(\omega^6) &&= \omega^{12} &&= \omega
\end{aligned}
$$

We know that this group will have a normal subgroup of order 2 and therefore the degree of its corresponding fixed field will be 5. The normal subgroup of order 2 is the subgroup consisting of $I = \lambda^{10}$ and λ^5. We can see that λ^5 has order 2 because

$$\lambda^5(\omega^{10}) = \lambda^4(\omega^9) = \lambda^3(\omega^7) = \lambda^2(\omega^3) = \lambda(\omega^6) = \omega.$$

Now we are looking for the fixed field of this subgroup of order 2. So we are looking for the elements of the field that are fixed under the map λ^5. A general element of this field is

$$a + b\omega + c\omega^2 + d\omega^3 + e\omega^4 + f\omega^5 + g\omega^6 + h\omega^7 + i\omega^8 + j\omega^9 + k\omega^{10}.$$

Applying the automorphism to this element using the group table above, we get

$$a + b\omega^{10} + c\omega^9 + d\omega^8 + e\omega^7 + f\omega^6 + g\omega^5 + h\omega^4 + i\omega^3 + j\omega^2 + k\omega.$$

So, in order for this element to be fixed under λ^5 then $b = k, c = j$, etc. and the general element of our fixed field L is

$$a + b(\omega + \omega^{10}) + c(\omega^2 + \omega^9) + d(\omega^3 + \omega^8) + e(\omega^4 + \omega^7) + f(\omega^5 + \omega^6).$$

We know that the order of the Galois group of this field extension is 5 because of the Fundamental Theorem of Galois Theory. Therefore, we know that the degree of this extension is 5. Therefore, the structure of the Galois group must be a cyclic group of order 5. The final step is to find a polynomial, $p(x)$, whose splitting field is L. Because the subgroup of order 5 is cyclic, every root of $p(x)$ will be a generator for the field extension. Also, we know that $p(x)$ for which L is a splitting field is of degree 5. Therefore, if we can find 5 generators of the field, $\alpha_1, \ldots, \alpha_5$, then the polynomial $(x-\alpha_1)(x-\alpha_2)(x-\alpha_3)(x-\alpha_4)(x-\alpha_5)$ will be a polynomial whose splitting field is L.

Proposition 3.2. *Each of the following generates L: $a_1 = \omega + \omega^{10}, a_2 = \omega^2 + \omega^9, a_3 = \omega^3 + \omega^8, a_4 = \omega^4 + \omega^7$ and $a_5 = \omega^5 + \omega^6$.*

Proof. We can see that each element can generate the next one in the equations below.

$$\begin{array}{rclcrcl}
(\omega + \omega^{10})^2 & = & \omega^2 + \omega^{20} + 2 & = & 2 + a_2 & \rightarrow & a_2 = a_1^2 - 2 \\
(\omega^2 + \omega^9)^2 & = & \omega^4 + \omega^{18} + 2 & = & 2 + a_4 & \rightarrow & a_4 = a_2^2 - 2 \\
(\omega^4 + \omega^7)^2 & = & \omega^8 + \omega^{14} + 2 & = & 2 + a_3 & \rightarrow & a_3 = a_4^2 - 2 \\
(\omega^3 + \omega^8)^2 & = & \omega^6 + \omega^{16} + 2 & = & 2 + a_5 & \rightarrow & a_5 = a_3^2 - 2 \\
(\omega^5 + \omega^6)^2 & = & \omega^1 0 + \omega^{12} + 2 & = & 2 + a_1 & \rightarrow & a_1 = a_5^2 - 2
\end{array}$$

So, clearly if we start with any of the elements, we can generate the next and therefore a basis of field L as a vector space over $\mathbb{Q}$. □

Now that we have our 5 primitive elements, we can generate a polynomial whose splitting field is L by simplifying

$$(x - (\omega + \omega^{10}))(x - (\omega^2 + \omega^9))(x - (\omega^3 + \omega^8))(x - (\omega^4 + \omega^7))(x - (\omega^5 + \omega^6)),$$

the final result of which is [see Appendix for details]

$$x^5 + x^4 - 4x^3 - 3x^2 + 3x + 1.$$

3.2 Greenberg's proof of the Kronecker Weber-Theorem

We will now consider Marvin J. Greenberg's proof of this theorem. It uses many basic facts from the fields of Algebraic Number theory and Galois Theory. The primary driver of the proof is the structure of finite fields, along with basic facts about ramification that we reviewed in the previous chapter.

For this proof, we will consider an extension L/K where $G = Aut(L/K)$ and an ideal $p_K\mathcal{O}_L$ of the ring of integers of L, $\mathcal{O}_L$ lying over p and $p_K\mathcal{O}_L = \prod_i \mathcal{B}_i^e$. Recall that we defined H, the decomposition group of $\mathfrak{p}_i$ for which $\sigma(\mathfrak{p}_i) = \mathfrak{p}_i$ and that each $\sigma \in H$ defines an automorphism σ_0 of $\mathcal{O}_L/\mathfrak{p}_i/\mathcal{O}_K/\mathfrak{p}_K$ and that each $\sigma_0 \in G_0$ the Galois group of $\mathbb{F}_L/\mathbb{F}_K$. Recall that G_0 is cyclic, generated by the Frobenius map, and therefore H/T is also cyclic. We can construct a chain of normal subgroups in the following manner. The elements of H induce an homomorphism $\mathcal{O}_L/\mathfrak{p}_i^2$ and that map ϕ_1 will also have some normal subgroup T_1. Both T_0 and T_1 are normal in H and $T_1 \subseteq T_0$. In this way, we define a chain of normal subgroups of H.

We will state without proof a few additional facts about the structure of the group H and its chain of normal subgroups T_i. Since H is finite, it is clear that for some n, T_n will be trivial. Consider the finite field $\mathcal{O}_L/\mathfrak{p}_i$, which is a field extension of $\mathcal{O}_K/\mathfrak{p}_K$. When $|\mathcal{O}_K/\mathfrak{p}_K| = q$, $|\mathcal{O}_L/\mathfrak{p}_i = q^f$. The elements of $\mathcal{O}_L/\mathfrak{p}_i$ other than 0 form a multiplicative group of order $q^f - 1$. The group T/T_1 is isomorphic to a subgroup of this multiplicative group, so its order divides $q^f - 1$. Each $T_i/T_{i+1}, i \geq 1$ is isomorphic to a subgroup of the additive group of $\mathcal{O}_L/\mathfrak{p}_i$ which means that the group is either trivial or isomorphic to a direct product of cyclic groups of order p. [5, p.290-5]

In addition, we will need to use valuation theory to complete this proof. A valuation,

denoted v, on a field is always relative to a particular prime. It is the power of that prime in the prime factorization of an element of a field. For this proof we will need the fact that if T_{i+1} is the last non-trivial normal subgroup, for $\sigma \in T_i - T_{i+1}, v(x - \sigma(x)) = i + 1$ and further that $v(f'(x)) = (i + 1)(\lambda - 1)$ when the valuation is associated with the prime λ.[5, p.296]

Recall that a cyclotomic extension is an extension of $\mathbb{Q}$ obtained by adjoining a root of unity. We will denote the cyclotomic extension created by adjoining the nth roots of unity as $\mathbb{Q}_n$. We will review here some important facts about cyclotomic extensions that are relevant to this proof.

Theorem 3.3. *The Galois group of $\mathbb{Q}_n$ is isomorphic to the multiplicative group of the units of $\mathbb{Z}/n\mathbb{Z}$.*

Proof. Any cyclotomic extension of degree n is generated by a primitive nth degree of unity,ξ_n. First we will show that $\Phi(n)$ has order $\phi(n)$, the Euler phi function. The cyclotomic polynomial, $\Phi(n)$, is the minimal polynomial of an nth root of unity. Recall that $f(x) = x^n - 1 = \prod_i^n (x - \zeta_n^i)$ is the polynomial split by the cyclotomic field. So, for any $d|n$, $\zeta_n^{\frac{n}{d}}$ will be a dth root of unity and $\Phi(d)$ divides $f(x)$. After these polynomials are factored out what will remain will be $\Phi(n)$ which will have a factor for each $a < n$ such that $(a, n) = 1$, which is $\phi(n)$. So, since the any $d|n$ will be a zero divisor in $\mathbb{Z}/n\mathbb{Z}$, there are $\phi(n)$ units in the multiplicative group of $\mathbb{Z}/n\mathbb{Z}$. Clearly, therefore, there is an isomorphism from the units of $\mathbb{Z}/n\mathbb{Z}$ to the maps $\sigma(\xi) \to \xi^a$. [1, p.596] □

Now we can refer to our knowledge of the structure of this group to elucidate the structure of the Galois groups of cyclotomic extension. If n is prime then $\mathbb{Z}/n\mathbb{Z}^*$ is cyclic of order $p - 1$ since every non-zero element is a unit. If n is $p^r, p > 2$, then the multiplicative groups of the units of $\mathbb{Q}_n$ forms a group with an order of $p^{r-1}(p - 1)$ because $\frac{p^r}{p} = p^{r-1}$ elements are not units and therefore the number of units is $p^r - p^{r-1} = p^{r-1}(p - 1)$. The Galois group of $\mathbb{Q}[i] = \mathbb{Q}_4$ the simple group of order 2.

For any higher power of 2, the Galois group of the cyclotomic extension $\mathbb{Q}_{2^r}$ has order 2^{r-1}. More specifically, it is isomorphic to the direct product of two groups, one cyclic of order 2^{r-2} and the other of order 2 given by the mapping $\zeta \to \zeta^{-1}$ where ζ is a 2^r root of unity. [6, p.257]

Now, we need another essential fact about the Galois groups of field extensions. Given a base field F and two extensions K and L over F, the compositum of KL of K and L is defined as the smallest field such that $K \subseteq KL$ and $L \subseteq KL$.

Theorem 3.4. *Given K and L, finite Galois extensions of F with Galois groups G and H respectively, the Galois group of KL/F is isomorphic to the subgroup $\{(\phi, \psi)|\phi|_{K\cap L} = \psi|_{K\cap L}\}$ of $G \times H$.*

Proof. Define $R = Aut(KL/F)$ and $S = \{(\phi, \psi)|\phi|_{K\cap L} = \psi|_{K\cap L}\}$. Define a map $\lambda : R \to S$. Clearly this map is injective. Now, we must show that it is an isomorphism by showing that $|R| = |S|$. Let $M = K \cap L$ and $m = [M : F]$, $k = [KL : K]$ and $l = [KL : L]$. Now consider the groups $A = Aut(KL/K)$ and $B = Aut(KL/L)$ and the group AB consisting of $\sigma = \tau\pi, \tau \in A, \pi \in B$. So, AB is the group of automorphisms on KL whose fixed field is $M = K \cap L$. and $|AB| = kl$. Therefore $[KL : M] = kl$. Also, since $[KL : L][L : M] = kl$ and $[KL : L] = l$, then $[L : M] = k$. Similarly, $[K : M] = l$. Now we have $Aut(L : M) = k$ and $Aut(K : M) = l$. Using $\alpha \in Aut(K : M)$, $\beta \in Aut(L : M)$ and $\omega \in Aut(M/F)$, we can construct the elements of S by $\omega(\alpha, \beta)$. So, $|S| = mlk$. Similarly, since $[KL : F] = [KL : M][M : F] = mlk$, then $|R| = |S|$ and the map is an isomorphism.[2, p.603] □

Another basic fact about cyclotomic fields is the following.

Theorem 3.5. *The compositum of cyclotomic fields is cyclotomic.*

Proof. Any cyclotomic field, $\mathbb{Q}_n$ is contained in $\mathbb{Q}_k$ if $n|k$. So if $s = lcm(n, m)$, then $\mathbb{Q}_n \subset \mathbb{Q}_s$ and $\mathbb{Q}_m \subset \mathbb{Q}_s$. Therefore, the compositum of two cyclotomic fields, $\mathbb{Q}_n$ and $\mathbb{Q}_m$ will be contained in $\mathbb{Q}_s$ where $s = lcm(n, m)$, which is cyclotomic. □

Lemma 3.6. *If the Kronecker-Weber theorem holds for cyclic extensions of prime power order, then it holds for all abelian extension*

Proof. By the fundamental theorem of abelian groups, the Galois group G is a direct product of abelian groups of prime power order G_i. If K_i is the fixed field of each of these G_i, then K is the compositum of the K_i. If each K_i is cyclotomic, then since the compositum of a cyclotomic fields is cyclotomic, K is cyclotomic. □

Before we proceed to the proof, we need to recall the facts we established in the previous chapter. These are that for any algebraic extension K of $\mathbb{Q}$ the ideal $p\mathcal{O}_K$ can be factored in $\mathcal{O}_K$ as a product of powers of prime ideals of $\mathcal{O}_K, \mathfrak{p}_i$ that lie over p. We also defined $\mathcal{B}_p = \{\mathfrak{p} \subset \mathcal{O}_K | \mathfrak{p} \text{ lies over } p\}$. Then $f = [\mathcal{O}_K/\mathfrak{p}_i/\mathbb{F}_p]$. Also, e is the power of each prime factor in the factorization, known as the ramification index and $g = |\mathcal{B}_p|$. Then $efg = [K : Q]$. Also, the group $G = Aut(K/\mathbb{Q})$ will have a subgroup H that fixes each $\mathfrak{p}_i$ with a normal subgroup T_0. We established early in this chapter that H/T_0 is cyclic and that $e = |T_0|$. For the balance of the proof, we will assume that we are considering a given prime ideal, $\mathfrak{p}$ of a ring of integers of an algebraic extension K and L an algebraic extension of K. Then we will use $\mathcal{B}$ to represent a prime ideal of $\mathcal{O}_L$ lying over the prime ideal of K. Also, we will denote these finite fields as follows: $\mathbb{F}_L = \mathcal{O}_L/\mathcal{B}$ and $\mathbb{F}_K = \mathcal{O}_K/\mathfrak{p}$.

The proof of the Kronecker-Weber theorem depends on proving that all abelian extensions of prime power order are cyclotomic. The logic of the proof is based on the key fact that we can assume for an extension of degree λ^n, $\lambda > 2$ that the either only one prime not dividing λ is ramified in the extension or that the only prime ramified in the extension is λ. Using this fact, it is shown in two cases, one for primes greater than 2 and separately for powers of 2, that each of these abelian extension are cyclotomic. Then, by the logic of the fundamental theorem of abelian groups, all abelian extensions are cyclotomic.

Lemma 3.7. *If H/T_1 is abelian, then T_0/T_1 is cyclic of order dividing $q - 1$.*

Proof. Localizing if necessary, we can assume that $\mathcal{B}$ is a principal prime ideal of $\mathcal{O}_L$ generated by π. Then for each $\sigma \in H$, then since $\sigma(\pi) \in \mathcal{B} \rightarrow \sigma\pi = a\pi$ where $a \in \mathcal{O}_L, a \notin \mathcal{B}$.

Therefore, the assignment $\sigma \to a_\sigma$ defines a map from each element of H to each element of the multiplicative group of $\mathcal{O}_L$. Recall from above that T_0/T_1 is isomorphic to a subgroup of that group and that it is cyclic, so it is generated by one element. Let $\tau \in T_0$ be such that the coset of τ generates T_0/T_1. Note the following fact and simplify the notation as below.

$$\sigma\pi = a\pi \to \pi = a^{-1}[\sigma\pi] \to \sigma^{-1}\pi = \sigma^{-1}[a^{-1}\sigma\pi] = \sigma^{-1}[a^{-1}][\sigma^{-1}\sigma\pi] = \sigma^{-1}[a^{-1}]\pi$$

$$\sigma\pi = a\pi, \tau\pi = b\pi, \sigma\tau\sigma^{-1} = c\pi$$

Note that our assumption tells us that H/T_1 is abelian and therefore $\overline{b} = \overline{c}$. Consider specifically any σ that induces the Frobenius map on $\mathbb{F}_L/\mathbb{F}_K$ and we compute the following.

$$\sigma\tau\sigma^{-1}\pi = \sigma\tau[\sigma^{-1}[a^{-1}]\pi] = \sigma(\tau[\sigma^{-1}(a^{-1})]b\pi) = (\sigma\tau\sigma^{-1})(a^{-1})\sigma(b)a\pi.$$

Therefore, $c = (\sigma\tau\sigma^{-1})(a^{-1})\sigma(b)a$. Reducing by mod $\mathcal{B}$ and recalling that since T is the kernel of the map $\phi_0 : \sigma \to \sigma_0$, then $\overline{c} = [\sigma\sigma^{-1}]a^{-1}\sigma_0(\overline{b})a \to \overline{c} = \sigma_0(\overline{b})$. Since σ_0 is defined by the Frobenius map $\sigma_0(\overline{b}) = \overline{b}^q$, then $\overline{c} = b^q$. Since $\overline{c} = \overline{b}$, then $\overline{b} = \overline{b}^q$ and $\overline{b}^{q-1} = 1$, so the order of all elements b have order dividing $q-1$ and the lemma is proved. [2, p.603] $\square$

Lemma 3.8. *K is an abelian extension of $\mathbb{Q}$ of degree λ^n where $G = Aut(K/\mathbb{Q})$, If $p \neq \lambda$ is ramified in K, if p is the only prime ramified in K then K is cyclotomic.*

Proof. Suppose $p \neq \lambda$ is ramified in K and $\mathcal{B}$ is a prime ideal lying over p. Then, p does not divide the order of any quotient groups of G, since they all must have order λ^k for some k. Let $\mathbb{F}_K = \mathbb{O}_K/\mathcal{B}$ and $\mathbb{F}_K$ will have characteristic p and order p^n. By facts stipulated above, T_0/T_1 will be isomorphic to a subgroup of the additive group of $\mathbb{F}_K$, but since $|T_0|$ divides λ^n then T_1/T_2 must be trivial. The same argument can be made for all quotient groups T_i/T_{i+1}. Since T_n for some n must eventually be trivial, this implies that T_1 is trivial. Therefore, $|T_0| \mid (p-1)$ and $\lambda^m \mid (p-1)$ for some m.

Now, consider the cyclotomic extension $\mathbb{Q}[\zeta_p]$. Then the extension is cyclic of degree $p-1$, and it has a unique subfield L where $[L:\mathbb{Q}] = \lambda^m$. Furthermore, p is totally ramified in L, $e = n$ and no other prime is ramified in L, by Theorem 2.11. Now consider KL, the compositum of K and L which has degree λ^{n+k}, $k \leq m$. Let $\mathcal{B}_{KL}$ be a prime ideal of KL lying over p and $T_{0_{KL}}$ its inertia group and $G_L = Aut(L/\mathbb{Q})$. Since $Aut(KL/\mathbb{Q}) = G \times G_L$, then $T_{0_{KL}} \trianglelefteq T_0 \times G_L$. Since T_0 and G_L both have order λ^m no element has order greater than λ^m. Since the fixed field of $T_{0_{KL}}$ contains the fixed field of T_0 then the order of $T_{0_{KL}}$ must not be less than the λ^m, the order of T_0. Therefore the order of $T_{0_{KL}}$ must exactly equal λ^m. Let $K_{T_{0_{KL}}}$ be the fixed field of $T_{0_{KL}}$. Then by facts listed above, p is unramified in $K_{T_{0_{KL}}}$. Recall that in L, p is totally ramified, so since in $K_{T_{0_{KL}}} \cap L$ p is unramified, that means that $e = n = 1$ and $K_{T_{0_{KL}}} \cap L = \mathbb{Q}$.

Recall that $K \subseteq K_{T_{0_{KL}}} \subseteq KL$. If we can show that $KL = K_{T_{0_{KL}}}L$, then KL will be cyclotomic if $K_{T_{0_{KL}}}L$ is. By construction and by the Fundamental Theorem of Galois theory $[KL : K_{T_{0_{KL}}}] = [L:\mathbb{Q}] = \lambda^m$. Note that

$$[KL:\mathbb{Q}] = [KL : K_{T_{0_{KL}}}][K_{T_{0_{KL}}} : \mathbb{Q}] \rightarrow \frac{[KL:\mathbb{Q}]}{[KL : K_{T_{0_{KL}}}]} = [K_{T_{0_{KL}}} : \mathbb{Q}]$$

and

$$K_{T_{0_{KL}}} \cap L = \mathbb{Q}, [K_{T_{0_{KL}}}L : \mathbb{Q}] = [K_{T_{0_{KL}}} : \mathbb{Q}][L:\mathbb{Q}].$$

We can substitute in (3.15) for $[K_{T_{0_{KL}}} : \mathbb{Q}]$ and recalling that $[KL : K_{T_{0_{KL}}}] = [L:\mathbb{Q}]$ we have

$$[K_{T_{0_{KL}}}L : \mathbb{Q}] = [KL:\mathbb{Q}].$$

Since the extensions are of the same degree, we can conclude that they are equal.

We know that no other prime can ramify in $K_{T_{0_{KL}}}$ since this prime would ramify in KL. Recall that the ramification index is equal to the degree of the inertia group which must

divide $|Aut(KL/\mathbb{Q})|$ and $Aut(KL/\mathbb{Q}) = G \times Aut(L\mathbb{Q})$. If $q \neq p$ then q does not ramify in L because L is the pth cyclotomic extension and only p ramifies in L. Therefore the inertia group in L must be trivial. Similarly, since the inertia group of p in G must divide the order of G, it must also be trivial. So, the inertia group of q in KL is trivial, so q does not ramify in K.

If p is the unique prime that ramifies in K where $q \neq \lambda$, then since p is not ramified in $K_{T_{0_{KL}}}$ and no other primes ramify in $K_{T_{0_{KL}}}$, it has no ramified primes and therefore $K_{T_{0_{KL}}} = \mathbb{Q}$ and $K = L$, the unique cyclotomic field of order $p-1$ and K is cyclotomic. [2, p.604]

So we have shown that if there is a unique ramified prime that does not divide the degree of the extension, then the extension is cyclotomic. Since every extension has a finite number of ramified primes, we can use the process outlined in the proof above to eliminate all but one of the ramified primes. Then, the theorem tells us that the remaining extension is cyclotomic. Now we are left with the cases where the ramified primes divide the degree of the extension. At this point we break up the proof into two cases, where the order of the extension is a power of an odd prime and for powers of 2. □

Lemma 3.9. *If K is an abelian extension of order λ^n, where λ is an odd prime,in which λ is the only ramified prime, then K/Q is cyclic.*

Proof. If $\mathcal{B}$ is a prime lying over λ and T_0 is its inertia group, then λ is not ramified in the fixed field of its inertia group. Therefore, no primes are ramified in the inertia group. Since, all extensions of $\mathbb{Q}$ have a ramified prime by Minkowski's Theorem, then the fixed field of the inertia group is $\mathbb{Q}$ and the inertia group is the entire Galois group. So, $e = n, f = 1$ and the degree of $K/\mathcal{B}$ over $\mathbb{Q}/\lambda$ is 1 and therefore $K/\mathcal{B} = \mathbb{Q}/\lambda$. Since a power of λ does not divide $\lambda - 1, T_1 = T_0$ and all the T_i/T_{i+1} are either trivial or cyclic of order λ.

Now we need to show that if $[K : \mathbb{Q}] = \lambda$ then T_2 is trivial.

Localizing if necessary, we can assume that $\mathcal{B}$ is principal generated by π. Suppose that T_{i+1} is the first trivial inertia group. Then, T_i is the whole group and $T_i - T_{i+1}$ is the whole

group less the identity. Recall the fact stipulated above that

$$v(f'(x)) = (i+1)(\lambda - 1).$$

Let $f(x)$ be the minimal polynomial of x over $\mathbb{Q}$. Consider the derivative of $f(x)$

$$f'(\pi) = \lambda\pi^{\lambda-1} + (\lambda-1)a_{\lambda-1}\pi^{\lambda-2} + \cdots + a_1.$$

Let v be the valuation associated with the prime $\mathcal{B}$. Since λ is totally ramified in K, its ramification index is the degree of the extension λ and since all the coefficients of $f(x)$ are integers then, $v(a_i) \equiv 0 mod\ (\lambda)$. Also $v(\lambda - i) = 0, 0 < i < \lambda$ since λ does not divide any of them. Since the valuation of a product is the sum of the valuations then $v(a^n) = nv(a)$. Since π generates $\mathcal{B}$ then $v(\pi) = 1$ and therefore if v_i is the valuation of the term of the derivative involving $\pi^{\lambda-i}$, then

$$\begin{aligned} v_i &= v((\lambda - (i-1))a_{\lambda-(i-1)}\pi^{\lambda-i}) \\ &= v(\lambda - (i-1)) + v(a_{\lambda-(i-1)}) + (\lambda - i)v(\pi)) \\ &\equiv (\lambda - i) mod(\lambda). \end{aligned}$$

This means that each term has a different value mod λ and since the valuation of a sum is the minimum of the valuations,

$$v(\lambda\pi^{\lambda-1}) = \lambda + \lambda - 1 = 2\lambda - 1 \geq v(f'(\pi)).$$

Therefore, combining 3.17 and 3.20 we see that, $2\lambda - 1 \geq (j+1)(\lambda - 1)$. Since, $\lambda > 2$, this

is only true when $j = 1$ by the following:

$$\begin{aligned} 2\lambda - 1 &\geq (j+1)(\lambda - 1) \\ 2\lambda - 1 &\geq (j+1)\lambda - j - 1 \\ j &\geq (j-1)\lambda. \end{aligned}$$

Therefore, $j = 1$ and T_2 is trivial.

Now we return to the case where $m > 1$. If we can show that an abelian extension of degree λ^m has a unique subgroup of order λ then the Galois group of the extension must be cyclic. So, for $G = Aut(K/Q)$, choose H such that $|H| = \lambda$. Therefore, its fixed field K^H had Galois group $G_H \cong G/H$. □

Lemma 3.10. *The Kronecker-Weber theorem holds for abelian extensions of order λ^n, where λ is an odd prime.*

Proof. By Lemma 3.9, we can assume that λ is the only prime ramified in the extension. Let ζ be a λ^{n+1} root of unity and then let K' be the unique subfield of order λ^n of $\mathbb{Q}[\xi]$. We know this subfield is unique because $\mathbb{Q}[\zeta]/\mathbb{Q}$ is cyclic of order $\lambda^n(\lambda - 1)$. Then λ is the only ramified prime in K'.

We claim that $K = KK' = K'$. Otherwise, KK' would have degree greater than λ^n. If λ is the only ramified prime in the extension of KK' which has degree greater than λ^n then by Lemma 3.9 then KK' is cyclic and must have an element of order greater than λ^n. But since the Galois group of KK' over $\mathbb{Q}$ is isomorphic to a direct product of the Galois groups of K and K', it cannot have an element of order greater than λ^n. This is a contradiction and our claim is proved. □

Lemma 3.11. *All quadratic extensions are cyclotomic.*

Proof. We need only consider all extension of the form $\sqrt{p}$ where p is prime. This is because for any cyclotomic extension of degree n, containing $\sqrt{p}$ and another cyclotomic extension

of degree m containing $\sqrt{q}$ then the cyclotomic extension of degree mn will contain $\sqrt{pq}$. For the case $p = 2$, $\mathbb{Q}[\sqrt{2}] \in \mathbb{Q}[\zeta_8]$ and note that $i \in \mathbb{Q}[\zeta_4]$.

We have already shown in chapter one that the absolute value of the discriminant of the pth cyclotomic extension, when p is prime, is $|p^{p-2}|$. Recall that the discriminant is:

$$\Delta_{K/\mathbb{Q}} = \prod_{i}^{n}(x - \sigma_i(\theta))$$

Therefore, the discriminant is a square of an element of the extension. Because p is odd, the discriminant is an odd power of p. So the square root of the discriminant is $p^k\sqrt{p}$ and $\sqrt{p}$ is an element of the cyclotomic extension. So, to ensure that both p and $-p$ are square, we need the $4p$th cyclotomic extension, which will necessarily contain i. Therefore, all quadratic extensions are cyclotomic. □

Lemma 3.12. *All cyclic extension of order 2^n are cyclotomic.*

Proof. We will prove this by induction on n. We have shown above that this statement is true for $n = 1$. Recalling that we have shown that all extensions where p, a ramified prime, does not divide 2, is the only ramified prime in 2, then the extension is cyclotomic, we can assume that 2 is the only ramified prime in K. If K is embedded in the complex numbers, since complex conjugation is of order 2, the fixed field of complex conjugation must have order at least 2^{n-1}. Because K is cyclic, this field must have a unique subfield of degree 2, so since we know 2 is a square, it must be the field $\mathbb{Q}[\sqrt{2}]$.

Recall that the Galois group of a cyclotomic extension $\mathbb{Q}[\zeta_m]$ is congruent to the group of units of $\mathbb{Z}/m\mathbb{Z}$. Therefore $\mathbb{Q}[\zeta_{2^{n+2}}]$ is the direct product of a cyclic group of order 2^n and the group of order 2 generated by the map $\sigma = \zeta \to \zeta^{-1}$. So, the fixed field of σ is $L = \mathbb{Q}[\zeta + \zeta^{-1}]$ and the extension has degree 2^n. This field also contains the subfield $\mathbb{Q}[\sqrt{2}]$ by the argument above. So the compositum of K and L, KL has degree no greater then 2^{2m} so $J = Aut(KL/\mathbb{Q}) < G \times H$, $G = Aut(K/\mathbb{Q}), H = Aut(L/\mathbb{Q})$. Choose

generators of G and H, τ and ϕ respectively that agree on $L \cap K$. Then $(\tau, \phi) \in J$ will generate a subgroup of order 2^m which will have a fixed field F. Since $[KL : F] = 2^n$, then $[KL : \mathbb{Q}] = [KL : F][F : \mathbb{Q}] < 2^{2m} \rightarrow [F : \mathbb{Q}] < 2^m$. So, by the inductive hypothesis, F is cyclotomic. $\square$

This series of assertions prove the Kronecker-Weber theorem.

3.3 Conclusion

This proof of the Kronecker-Weber theorem, is a useful window into many foundational ideas in ring theory in general and algebraic number theory in particular. While modern proofs of this theorem use the machinery of class field theory, of which the Kronecker-Weber theorem is simply a special case of its results, this proof is accessible with simpler concepts. It illuminates the structure of Dedekind domains, finite fields, and cyclic groups, giving a student the opportunity to explore and deepen understanding of these concepts.

Appendix 4: Simplification of Polyomial whose Galois group is cyclic of order 5

Recall that ω is a zero of the cyclotomic polynomial

$$\begin{aligned}\omega^{10}+\omega^9+\omega^8+\omega^7+\omega^6+\omega^5+\omega^4+\omega^3+\omega^2+\omega+1 &= 0\\ \omega^{10}+\omega^9+\omega^8+\omega^7+\omega^6+\omega^5+\omega^4+\omega^3+\omega^2+\omega &= -1\end{aligned}$$

First expand the expression and combine like terms. The constant terms are:

$$-\omega^{15}-\omega^{16}-\omega^{18}-\omega^{19}-\omega^{20}-\omega^{21}-\omega^{22}-2\omega^{23}-2\omega^{24}-2\omega^{25}-\omega^{26}-2\omega^{27}-2\omega^{28}-\omega^{29}$$
$$-2\omega^{30}-2\omega^{31}-2\omega^{32}-\omega^{33}-\omega^{34}-\omega^{35}-\omega^{36}-\omega^{37}-\omega^{39}-\omega^{40}$$

$$-\omega^4-\omega^5-\omega^7-\omega^8-\omega^9-\omega^{10}-1-2\omega-2\omega^2-2\omega^3-\omega^4-2\omega^5-2\omega^6-\omega^7$$
$$-2\omega^8-2\omega^9-2\omega^{10}-1-\omega-\omega^2-\omega^3-\omega^4-\omega^6-\omega^7$$

$$\begin{aligned}&= -2-3(\omega+\omega^2+\omega^3+\omega^4+\omega^5+\omega^6+\omega^7+\omega^8+\omega^9+\omega^{10})\\ &= -2-3(-1)\\ &= 1\end{aligned}$$

Now simplify the x terms. The coefficients are

$$\omega^{10}+\omega^{11}+2\omega^{12}+3\omega^{13}+2\omega^{14}+3\omega^{15}+3\omega^{16}+4\omega^{17}$$
$$+4\omega^{18}+5\omega^{19}+4\omega^{20}+4\omega^{21}+8\omega^{22}+4\omega^{23}+4\omega^{24}+5\omega^{25}$$
$$+4\omega^{26}+4\omega^{27}+3\omega^{28}+3\omega^{29}$$
$$+2\omega^{30}+3\omega^{31}+2\omega^{32}+\omega^{33}+\omega^{34}$$

$$\omega^{10}+1+2\omega+3\omega^2+2\omega^3+3\omega^4+3\omega^5+4\omega^6+4\omega^7$$
$$+5\omega^8+4\omega^9+4\omega^{10}+8+4\omega+4\omega^2+5\omega^3+4\omega^4+4\omega^5+3\omega^6+3\omega^7$$
$$+2\omega^8+3\omega^9+2\omega^{10}+\omega+\omega$$

$$
\begin{aligned}
&= 10 + 7(\omega + \omega^2 + \omega^3 + \omega^4 + \omega^5 + \omega^6 + \omega^7 + \omega^8 + \omega^9 + \omega^{10}) \\
&= 10 + 7(-1) \\
&= 3
\end{aligned}
$$

Now simplify the x^2 terms

$$
\begin{aligned}
&-\omega^6 - \omega^7 - 2\omega^8 - 3\omega^9 - 4\omega^{10} - 5\omega^{11} - 3\omega^{12} - 4\omega^{13} - 5\omega^{14} - 6\omega^{15} - 6\omega^{16} - 6\omega^{17} - 6\omega^{18} \\
&-5\omega^{19} - 4\omega^{20} - 3\omega^{21} - 5\omega^{22} - 4\omega^{23} - 3\omega^{24} - 2\omega^{25} - \omega^{26} - \omega^{27}
\end{aligned}
$$

$$
\begin{aligned}
&= -10 - 7(\omega + \omega^2 + \omega^3 + \omega^4 + \omega^5 + \omega^6 + \omega^7 + \omega^8 + \omega^9 + \omega^{10}) \\
&= 10 + 7(-1) \\
&= -3
\end{aligned}
$$

Now simplify the x^3 terms

$$
\begin{aligned}
&\omega^3 + \omega^4 + 2\omega^5 + 2\omega^6 + 3\omega^7 + 3\omega^8 + 4\omega^9 + 4\omega^{10} + 4\omega^{12} + 4\omega^{13} + 3\omega^{14} \\
&+3\omega^{15} + 2\omega^{16} + 2\omega^{17} + \omega^{18} + \omega^{19}
\end{aligned}
$$

$$
\begin{aligned}
&= 4(\omega + \omega^2 + \omega^3 + \omega^4 + \omega^5 + \omega^6 + \omega^7 + \omega^8 + \omega^9 + \omega^{10}) \\
&= -4
\end{aligned}
$$

Now simplify the x^4 terms

$$
-\omega - \omega^2 - \omega^3 + \omega^4 - \omega^5 - \omega^6 - \omega^7 - \omega^8 - \omega^9 + -\omega^{10}
$$

$$
\begin{aligned}
&= -(\omega + \omega^2 + \omega^3 + \omega^4 + \omega^5 + \omega^6 + \omega^7 + \omega^8 + \omega^9 + \omega^{10}) \\
&= 1
\end{aligned}
$$

So the minimal polynomial is $x^5 + x^4 - 4x^3 - 3x^2 + 3x + 1$

Bibliography

[1] D. S. Dummit and R. M. Foote, Abstract Algebra, 3rd ed. Hoboken. 2004.

[2] An Elementary Proof of the Kronecker-Weber Theorem, The American Mathematical Monthly, Vol. 81, No 6, 601 – 607, 1974.

[3] I. Kaplansky, Commutative Rings, rev. ed., Univ. Chicago Press, Chicago, 1974.

[4] R.A Mollin, Algebraic Number Theory, Boca Raton, 2011.

[5] P. Samuel and O. Zariski , Commutative Algebra, New York, 1958.

[6] E. Weiss, Algebraic Number Theory, New York, 1963.

Curriculum Vitae

Marla H Schnall recieved her Bachelor of Arts Degree in Russian Studies from Yale University in 1986. She worked as a Research Assistant at the Federal Reserve in Washington DC and for a small statistical consulting firm for several years before staying home to raise her children. For the last 15 years she has been a teacher in Fairfax County.