11-20-2013

The Kronecker-Weber Theorem: An Exposition

Amber Verser
Lawrence University, avoboegirl17@gmail.com

Lawrence University

Honors Project

Deparment of Mathematics and Computer Science

The Kronecker-Weber Theorem

An Exposition

Author:
Amber Verser

Advisor:
Scott Corry

October 22, 2013

Abstract

This paper is an investigation of the mathematics necessary to understand the Kronecker-Weber Theorem. Following an article by Greenberg, published in *The American Mathematical Monthly* in 1974, the presented proof does not use class field theory, as the most traditional treatments of the theorem do, but rather returns to more basic mathematics, like the original proofs of the theorem [3]. This paper seeks to present the necessary mathematical background to understand the proof for a reader with a solid undergraduate background in abstract algebra. Its goal is to make what is usually an advanced topic in the study of algebraic number theory more accessible to advanced undergraduates and early graduate students, with a minimal amount of higher level number theory required. It also seeks to develop an appreciation for the power and elegance of this theorem and its role in mathematics, since it combines understanding in many branches – classical Galois theory, geometry, complex numbers, abelian groups, and number theory.

Contents

1 Historical Background **3**

2 Classical Galois Theory **5**
2.1 Minimal Polynomials 7
2.2 Field Extensions 8
2.3 Field Automorphisms 11
2.4 The Galois Group 14
2.5 The Galois Correspondence 15
2.6 Field Compositums 20
2.7 Cyclotomic Polynomials 20

3 Ramification Theory **21**
3.1 Dedekind Domains 21
3.2 Decomposition and Inertia Groups 27
3.3 Ramification in Cyclotomic Extensions 29
3.4 Valuations 30

4 Proof of the Kronecker-Weber Theorem **33**

5 Conclusion **37**

6 Acknowledgments **38**

1 Historical Background

Polynomials are the essence of much of modern algebra, since polynomials are by definition the functions that can be created using standard arithmetic operations (addition and multiplication) with a given number of variables. Furthermore, from any commutative ring R, we can form the set of polynomials in one variable, x, with coefficients in R. This set, denoted $R[x]$, is itself a ring with the usual polynomial addition and multiplication as operations. The most familiar polynomial rings would be the polynomials in a single variable with coefficients in the integers, denoted $\mathbb{Z}$; the real numbers, denoted $\mathbb{R}$; the complex numbers, $\mathbb{C}$; and the rational numbers, $\mathbb{Q}$.

Consider the polynomial ring $\mathbb{Q}[x]$. First note that there are many polynomials with coefficients in $\mathbb{Q}$ that do not have roots in $\mathbb{Q}$; $x^3 - 2$, for example. A polynomial $P \in \mathbb{Q}[x]$ can have at most d_P roots, where d_P denotes the degree of the polynomial P. Furthermore, every root of a polynomial with coefficients in $\mathbb{Q}$ has exactly d_P roots in $\mathbb{C}$, counted with multiplicity. In fact, from the Fundamental Theorem of Algebra, we know that every polynomial P in $\mathbb{C}[x]$ has exactly d_P roots. This property is called *algebraically closed*. However, the complex numbers contain many numbers that are not derived algebraically from $\mathbb{Q}$ – numbers that are not roots of polynomials with coefficients in $\mathbb{Q}$. Instead, let $\bar{\mathbb{Q}}$ denote the field of all algebraic numbers over $\mathbb{Q}$, that is, the complex numbers which are roots of polynomials with coefficients in $\mathbb{Q}$. Then $\bar{\mathbb{Q}}$ is algebraically closed, and is in fact the smallest such field containing $\mathbb{Q}$. The study of Galois theory seeks to understand the underlying structure of this field.

Mathematicians such as Cardano investigated polynomials by attempting to come up with formulas for their roots. The quadratic formula was an early known solution for a general class of polynomials, and Cardano sought to create similar formulas for larger degree polynomials. As early as 1545, Cardano and his student Ferarri published in *Ars Magna* a cubic and a quartic formula, which produced the roots for any general polynomial of degree less than 5 in $\mathbb{Q}[x]$. However, throughout the next 200 years, although they tried, mathematicians could not find a general formula for quintics or any higher degree polynomials, using only standard arithmetic operations and nth roots. [5] Lagrange took the methods of solving polynomials established by Cardano and Ferarri and analyzed them using permutations of the roots of the polynomials, which would become a central idea in Galois theory. Ruffini, instead of using single permutations, considered the permutation groups of the roots (now the Galois groups) and together with Abel proved there was no general formula for the roots of a quintic polynomial. [2] Galois built off both Abel's and Cardano's work, and with his development of abstract algebra, he expanded the existing ideas by developing the subject that would be later known as Galois theory. His theory fully explains exactly when higher degree polynomials are solvable (the roots can be written using basic arithmetic operations and nth roots applied to the rationals) and why they are not when they are not. He also was able to answer classical problems in geometry using his algebraic theory, including proving that the three traditional problems (Squaring the

Circle, Doubling the Cube, and Trisecting the Angle) were all impossible constructions with straight-edge and compass. Furthermore, he determined exactly which regular n-gons are constructible, beginning the long interconnection between algebra and geometry.

At the core of Galois theory is the Galois group, the group of field automorphisms of a given algebraic field that contains $\mathbb{Q}$. Since symmetries are bijective functions which preserve some mathematical structure, we can think of the Galois group as encoding the symmetries of a field extension – as a collection of bijective functions which preserve the algebraic structure of a field, which are by definition automorphisms. This also is a key way in which Galois theory is tied to geometry, since the idea of symmetry has its roots in geometric intuition. As mentioned above, for a given polynomial $P \in \mathbb{Q}[x]$, the Galois group acts on the roots of the polynomial and permutes them. Thus, Galois groups also encode the symmetries of the roots of polynomials.

With classical Galois theory and the development of the Galois group, a natural question arose, commonly called the inverse Galois problem: Which groups occur as Galois groups over $\mathbb{Q}$? This is still an open problem but has generated much research in several fields, including algebraic number theory and algebraic geometry. A natural place to begin investigating this question is to look at abelian groups, because these groups are classified by the Fundamental Theorem of Abelian Groups, so their structure is very well understood. This exploration leads to the main topic of this paper, the Kronecker-Weber Theorem, which states

Every abelian extension of $\mathbb{Q}$ is cyclotomic.

That is, every extension of $\mathbb{Q}$ with an abelian Galois group is contained inside the set of cyclotomic numbers (the field that contains the rationals together with the nth roots of unity for all n). Notice that this theorem is a much stronger assertion than simply claiming all abelian groups exist as Galois groups over $\mathbb{Q}$, although this fact is a direct result of this theorem. (Note this can be proven without using the Kronecker-Weber Theorem, by simply arguing that the cyclotomic extensions contain all abelian Galois groups.) Rather, this theorem restricts the field extensions that could possibly have abelian Galois groups to a well-understood class of fields.

The Kronecker-Weber Theorem is extremely powerful, since it further deepens the connection between algebra and geometry, connecting a whole class of groups to the set of numbers that are vertices of regular n-gons in the complex plane. Furthermore, the roots of unity connect to analysis, since they are special values of the exponential function e^{ix}. The numbers $e^{i\frac{2\pi}{n}}$, the roots of unity, are generalizations of Euler's formula $e^{i\pi} = -1$, which combines many of the most important constants in mathematics. Thus this theorem connects several large branches of mathematics in a surprising way, and is proven using yet another branch: number theory.

The first statement of the theorem was in 1853 in Leopold Kronecker's article *Über die algebraisch auflösbaren Gleichungen* (On Algebraically Solvable Equations) published in the *Berlin Akadamie der Wissenschaften.* However Kronecker did not prove the theorem

for field extensions of order a power of 2 [8]. In 1886 in *Theorie der Abel'schen Zahlkörper* (Theory of the Abelian Number Fields), Heinrich Weber supplied a proof that was also incomplete [17]. Finally, in 1896, David Hilbert published the first complete proof of the theorem in *Ein neuer Beweis des Kronecker'schen Fundementalsatzes über Abel'sche Zahlkörper* (A New Proof of the Kronecker Fundamental Theorem for Abelian Number Fields) [6].

Since the development of class field theory, the most frequently presented proofs of the Kronecker-Weber Theorem have relied on it. However, the original proofs did not use it, and we present here a proof that does not use class field theory, but rather a minimal amount of algebraic number theory, in order to make the theorem more accessible to younger students. We also present the necessary classical Galois theory and algebraic number theory to understand the given proof, thus allowing students with a solid undergraduate background in algebra to appreciate the theorem.

Remark: Recall that a field's *characteristic* is the smallest integer n such that

$$\underbrace{1+1+\cdots+1}_{n \text{ times}} = 0.$$

If no such n exists, we say the field has characteristic 0. Every finite field must have prime characteristic p and order p^f for some f. For the most part, we will be working over fields of characteristic 0. For simplicity, unless otherwise stated, we will assume our fields are characteristic 0 throughout this paper.

2 Classical Galois Theory

Let K be a field of characteristic 0. The polynomial ring $K[x]$ has many of the same properties that the integers have, so this ring has a familliar algebraic structure. Like in the integers, $K[x]$ has a division algorithm:

For $P, Q \in K[x]$, where P is non-zero, there exist unique $q, r \in K[x]$ so that $Q = qP + r$ where $d_r < d_P$.

As a consequence, $K[x]$ is a *principal ideal domain* (all ideals in $K[x]$ are generated by single elements). Also, we can define the *greatest common divisor* of P and Q as the monic polynomial of highest degree that divides both P and Q. Using the division algorithm, we can generalize the Euclidean Algorithm, as in the integers.

If a non-constant polynomial $P(x) \in K[x]$ can be factored into non-constant polynomials $A(x), B(x) \in K[x]$ so that $A(x)B(x) = P(x)$, then we call P *reducible*. If no such

polynomials exist and P is not constant, we call $P(x)$ *irreducible*. We can also extend Euclid's Lemma to these polynomials.

Lemma: Let $P(x)$ be an irreducible polynomial in $K[x]$. Then, if $P(x) \mid A(x)B(x)$ then $P(x) \mid A(x)$ or $P(x) \mid B(x)$.

Proof: If $P(x) \mid A(x)$, we are done. So suppose that $P(x)$ does not divide $A(x)$. Then, since P is irreducible, the greatest common divisor of P and A must be 1. Thus, from the Euclidean Algorithm, there exist polynomials $f(x), g(x) \in K[x]$ so that

$$f(x) \cdot P(x) + g(x) \cdot A(x) = 1.$$

This implies that

$$f(x) \cdot P(x) \cdot B(x) + g(x) \cdot A(x) \cdot B(x) = B(x).$$

However, since $P(x) \mid A(x)B(x)$, there is some polynomial $h(x)$ so that $P(x)h(x) = A(x)B(x)$, so we have

$$P(x)\big[f(x)B(x) + g(x)h(x)\big] = B(x).$$

Thus $P(x) \mid B(x)$. $\square$

The most common application of Euclid's Lemma is the Fundamental Theorem of Arithmetic, which states that all integers can be uniquely factored into the product of primes. We can also generalize this in $K[x]$.

Theorem (Unique Factorization): All non-zero $P(x) \in K[x]$ can be uniquely factored into a product of monic irreducible polynomials and a constant, in other words

$$P(x) = c \cdot p_1(x)p_2(x) \cdots p_t(x),$$

where $c \in K$ and each p_i is a monic irreducible polynomial in $K[x]$, not necessarily distinct.

Proof of Unique Factorization: Existence: Without loss of generality, suppose that P is monic (if not, factor out the coefficient to become the c above). We will proceed by induction on d_P. First suppose that $d_P = 1$. These polynomials are all by definition irreducible. Now, suppose all polynomials with degree less than n can be factored into irreducible polynomials. Let $d_P = n$. If $P(x)$ is irreducible, then it can be factored. Otherwise, $P(x) = A(x)B(x)$ where $0 < d_B \leq d_A < d_P = n$. However, both B and A can be factored into irreducible polynomials, since their degrees are less than n. Thus P can also be factored into irreducible polynomials.

Uniqueness: Suppose that $P(x) = A_1(x)A_2(x)\dots A_r(x) = B_1(x)B_2(x)\dots B_s(x)$ where all the A_i's and B_i's are monic irreducible polynomials. A_1 must divide the product of the B_i's. Since A_1 is irreducible, our lemma shows that A_1 must divide some B_i, without

loss of generality, say B_1. However since B_1 is also irreducible, $A_1 = B_1$. Similarly, $A_i = B_i$ for all $i \leq r = s$. $\square$

We call an integral domain with this property a *unique factorization domain*. Note that uniqueness does not hold for integral domains in general. We see that the algebraic properties we associate with $\mathbb{Z}$ still hold for polynomial rings with coefficients in fields of characteristic 0. These polynomial rings have a comfortable and familiar structure to work in, since our intuition about the inherent algebraic structure from the integers still applies.

2.1 Minimal Polynomials

Now, suppose we have some algebraic number $\alpha \in \bar{\mathbb{Q}}$. Consider the ideal $I_\alpha \subseteq \mathbb{Q}[x]$ containing all polynomials with α as a root. In other words,

$$I_\alpha = \{P(x) \in \mathbb{Q}[x] | P(\alpha) = 0\}.$$

Since $\mathbb{Q}[x]$ is a principal ideal domain, this ideal is generated by a single element, m_α, a monic polynomial with minimal degree in I_α.

Theorem 2.1.1: The polynomial m_α is irreducible and is the unique irreducible polynomial having α as a root.

Proof: First, let us argue m_α is irreducible: suppose that it were reducible, and we had $m_\alpha = A \cdot B$ for $A, B \in \mathbb{Q}[x]$. However,

$$0 = m_\alpha(\alpha) = A(\alpha)B(\alpha),$$

so $A(\alpha) = 0$ or $B(\alpha) = 0$; thus either A or B is in the ideal I_α. However, both A and B have smaller degree than m_α, which contradicts that m_α has minimal degree in I_α. Similarly, since m_α generates I_α, any polynomial P in I_α can be written as $Q(x) \cdot m_\alpha$, so m_α is the unique, monic irreducible polynomial in I_α. $\square$

We call m_α the *minimal polynomial* for α over $\mathbb{Q}$. For example, $m_{\sqrt[3]{2}} = x^3 - 2$, and $m_{\zeta_3} = x^2 + x + 1$ where ζ_3 is a primitive third root of unity.

Now, we consider the subring of $\bar{\mathbb{Q}}$ formed by adjoining α to $\mathbb{Q}$. This is a larger ring than $\mathbb{Q}$ in which m_α is no longer irreducible. This ring, denoted $\mathbb{Q}[\alpha]$, is the set of numbers of the form $q_0 + q_1\alpha + q_2\alpha^2 + \ldots + q_n\alpha^n$, where $q_i \in \mathbb{Q}$ for all i.

Theorem 2.1.2: The ring $\mathbb{Q}[\alpha]$ is equal to the subfield of $\bar{\mathbb{Q}}$, $\mathbb{Q}(\alpha)$, which is the smallest field containing both α and $\mathbb{Q}$.

Proof: Since m_α is irreducible, (m_α), the ideal generated by m_α, is a maximal ideal, so $Q[x]/(m_\alpha)$ is a field. However, $Q[x]/(m_\alpha) \cong \mathbb{Q}[\alpha]$ by the first isomorphism theorem, so $\mathbb{Q}[\alpha]$ is a field. However, $\mathbb{Q}[\alpha] \subseteq \mathbb{Q}(\alpha)$ and $\mathbb{Q}(\alpha)$ is the smallest field containing both $\mathbb{Q}$ and α; thus $\mathbb{Q}[\alpha] = \mathbb{Q}(\alpha)$. $\square$

For example, consider ζ_{17}, a primitive seventeenth root of unity. Thus, we know that $x^{17} - 1$ is a polynomial with ζ_{17} as a root, so $x^{17} - 1 \in I_{\zeta_{17}}$. However, we have

$$m_{\zeta_{17}} = x^{16} + x^{15} + \ldots + x + 1 = \Phi_{17}(x)$$

where $\Phi_n(x)$ is the nth cyclotomic polynomial. Furthermore, since $I_{\zeta_{17}}$ is generated by $\Phi_{17}(x)$, we know

$$x^{17} - 1 = \Phi_{17}(x) f(x),\ f(x) \in \mathbb{Q}[x].$$

In particular,

$$x^{17} - 1 = \Phi_{17}(x) \cdot (x - 1),$$

and we have the following isomorphism:

$$\mathbb{Q}(\zeta_{17}) \cong Q[x]/\big(\Phi_{17}(x)\big).$$

This can also be generalized. If we have $L \supseteq K$ where L and K are both fields of characteristic 0 and L is *algebraic* over K, that is L contains only numbers that satisfy polynomials in $K[x]$, then for $\alpha \in L$, we have the same equivalences as above.

2.2 Field Extensions

Suppose we have a field K of characteristic 0 and we have a field $L \supseteq K$. We call L a *field extension* of K. If L is algebraic, then we call L an algebraic field extension. We denote this extension as $L|K$. Furthermore, L can be described as a vector space over K, and we denote its dimension $[L : K]$, called the *degree* of L over K.

Now, suppose α is an algebraic number over K, and let d be the degree of m_α. Then the following holds:

Theorem 2.2.1: $K(\alpha)|K$ is an extension of degree d and, in particular, $\{1, \alpha, \alpha^2, \ldots, \alpha^{d-1}\}$ is a basis for $K(\alpha)$ over K.

Proof: We must show that the elements of our proposed basis span and are linearly independent. First, suppose that we have some $c_i \in K$, so that

$$c_0 + c_1\alpha + c_2\alpha^2 + \ldots c_{d-1}\alpha^{d-1} = 0.$$

Then the polynomial $c_0 + c_1 x + c_2 x^2 + \ldots c_{d-1}x^{d-1}$ is a polynomial which has α as a root. However, since m_α is the minimal polynomial of α and has a larger degree, this polynomial

must be 0. Thus $c_i = 0$ for all i, so the set $\{1, \alpha, \alpha^2, \ldots, \alpha^{d-1}\}$ is a linearly independent set. Now, to show that our set is spanning, recall that

$$K(\alpha) = K[\alpha] = \Big\{ \sum_{i=0}^{d} c_i \alpha^i \mid c_i \in K \Big\}.$$

Thus, for every $g \in K(\alpha)$, there is a polynomial $G \in K[x]$ so that $G(\alpha) = g$. However, by the division algorithm

$$G(x) = m_\alpha(x) \cdot q(x) + r(x)$$

for some $r \in K[x]$ that has degree less than d. Thus,

$$g = G(\alpha) = m_\alpha(\alpha) \cdot q(\alpha) + r(\alpha) = 0 \cdot q(\alpha) + r(\alpha) = r(\alpha)$$

which has degree less than d, so is a linear combination of the elements of our basis. Thus $[K(\alpha) : K] = d$. $\square$

Example: Let $\alpha = \sqrt[3]{2}$. Then $m_\alpha(x) = x^3 - 2$. Also, consider $\alpha\zeta_3$. Note that $m_\alpha(\alpha\zeta_3) = 0$, so $m_\alpha = m_{\alpha\zeta_3}$. Thus,

$$\mathbb{Q}(\alpha) \cong \mathbb{Q}[x]/(m_\alpha) \cong \mathbb{Q}(\alpha\zeta_3),$$

however $\mathbb{Q}(\alpha) \subseteq \mathbb{R}$ but $\mathbb{Q}(\alpha\zeta_3)$ is not. So although these two fields are isomorphic, they are very different fields.

Now, suppose that we have a chain of field extensions $M \supseteq L \supseteq K$ of finite degree.

Theorem (Tower Law): $M|K$ is also finite, and in particular $[M : K] = [M : L][L : K]$.

Proof: Let $n = [L : K]$ and let $\{a_1, a_2, \ldots, a_n\}$ be a basis for $L|K$. Similarly, let $m = [M : L]$ and let $\{b_1, b_2, \ldots, b_m\}$ be a basis for $M|L$. We will show that $\{a_i b_j\}$ is a basis for $M|K$.

First, we show it spans: let $\alpha \in M$ be arbitrary. Then, there are constants $c_i \in L$ so that

$$\alpha = \sum_{i=1}^{m} c_i b_i.$$

Similarly, for each i, there exist constants $k_{ij} \in K$ so that

$$c_i = \sum_{j=1}^{n} k_{ij} a_j.$$

Substituting this sum in the first expression gives

$$\alpha = \sum_{i=1}^{m} \sum_{j=1}^{n} k_{ij} a_j b_i.$$

Thus, this set spans M.

Now, we will show $\{a_i b_j\}$ is linearly independent. Suppose we had

$$0 = \sum_{i=1}^{m} \sum_{j=1}^{n} k_{ij}(a_i b_j),$$

for $k_{ij} \in K$. Then,

$$0 = \sum_{i=1}^{m} \Big(\sum_{j=1}^{n} k_{ij} b_j \Big) a_i.$$

Since the a_i's are linearly independent over L, for this equality to hold,

$$\sum_{j=1}^{n} k_{ij} b_j = 0$$

for all j. However, since the b_j's are linearly independent over K, this equality is only 0 if $k_{ij} = 0$ for all i and j. Thus, $\{a_i b_j\}$ is a linearly independent set, and therefore is a basis for $M|K$. $\square$

Example: Consider again our above example where $\alpha = \sqrt[3]{2}$. Then, we can form a chain of field extensions $\mathbb{Q} \subseteq \mathbb{Q}(\alpha) \subseteq \mathbb{Q}(\alpha)(\zeta_3)$. Note that $m_{\zeta_3} = x^2 + x + 1$ is irreducible in $\mathbb{Q}(\alpha)$. We know that $\mathbb{Q}(\alpha) \subseteq \mathbb{R}$ but the roots of m_{ζ_3}, ζ_3 and ζ_3^{-1} are not elements of $\mathbb{R}$, so are not in $\mathbb{Q}(\alpha)$. Thus, $m_{\zeta_3,\mathbb{Q}}$ is still the minimal polynomial of ζ_3 over $\mathbb{Q}(\alpha)$. Then, since $[\mathbb{Q}(\alpha) : \mathbb{Q}] = 3$ and $[\mathbb{Q}(\alpha)(\zeta_3) : \mathbb{Q}(\alpha)] = 2$, then $[\mathbb{Q}(\alpha)(\zeta_3) : \mathbb{Q}] = 3 \cdot 2 = 6$, and the set

$$\{1, \zeta_3, \alpha, \alpha\zeta_3, \alpha^2, \alpha^2\zeta_3\}$$

is a basis for $\mathbb{Q}(\alpha)(\zeta_3)|\mathbb{Q}$. Note there are also other subfields of this larger field, specifically $\mathbb{Q}(\alpha\zeta_3)$, as previously discussed, and $\mathbb{Q}(\alpha\zeta_3^2)$.

Furthermore, any field extension of finite degree is algebraic. Suppose $[L : K] = n$ and let $l \in L$ be arbitrary. Then the set $\{1, l, l^2, \ldots, l^n\}$ has $n+1$ elements, so there exist non-zero k_i's in K s.t. $k_0 + k_1 l + k_2 l^2 + \ldots + k_n l^n = 0$. Thus, l is a root of the polynomial $k_0 + k_1 x + k_2 x^2 + \ldots + k_n x^n \in K[x]$.

Suppose we have two extensions $L \supseteq K$ and $M \supseteq K$. Then, we define their *compositum* to be the smallest field which contains $L \cup M$, and we denote it LM. Note this field lies over both L and M. For example, if we have $\mathbb{Q}(\alpha)$ and $\mathbb{Q}(\zeta_3)$, then their field compositum, as expected, is $\mathbb{Q}(\alpha, \zeta_3)$.

Note also that if we have a field extension $K(\alpha, \beta)$, there is an element $\gamma \in K(\alpha, \beta)$ so that $K(\gamma) = K(\alpha, \beta)$. This theorem is called the Primitive Element Theorem. For proof

of this, see [1].

Above, we talked about adjoining roots of polynomials to form larger fields. However, a polynomial $P(x) \in K[x]$ has d_P roots in its algebraic closure, $\bar{K}$ (when K has characteristic 0), so we can adjoin all of the roots of a given polynomial. We define the *splitting field* of $P \in K[x]$ with roots $\alpha_1, \alpha_2 \ldots, \alpha_n$ to be $K(\alpha_1, \alpha_2, \ldots, \alpha_n)$. This is called the splitting field, because the polynomial splits into linear factors within this field: $P(x) = c(x - \alpha_1)(x - \alpha_2) \cdots (x - \alpha_n)$, for $c \in K$.

Theorem 2.2.2: Let $P \in K[x]$ be irreducible with degree n, and let K_P be the splitting field of P over K. Then, $n \leq [K_P : K] \leq n!$.

Proof: Let $K_P = K(\alpha_1, \alpha_2, \ldots, \alpha_n) = K_n$, $K(\alpha_1, \alpha_2, \ldots, \alpha_{n-1}) = K_{n-1}, \ldots, K(\alpha_1) = K_1$. First, note that $[K(\alpha_1) : K] = n$. Now, we consider $[K_i : K_{i-1}]$. Recall this is equal to the degree of the minimal polynomial of α_i over K_{i-1}. Furthermore, since $P = m_{\alpha_i, K}$, we know $m_{\alpha_i, K_{i-1}} \mid P$ and that

$$P = Q(x)(x - \alpha_1)(x - \alpha_2) \cdots (x - \alpha_{i-1}).$$

Moreover, $m_{\alpha_i, K_{i-1}}$ is relatively prime to each linear factor $x - \alpha_1, x - \alpha_2 \ldots x - \alpha_{i-1}$. Thus, $m_{\alpha_i, K_{i-1}} \mid Q$, and $d_Q = n - i + 1$. Thus, $[K_i : K_{i-1}] \leq n - i + 1$. By the Tower Law, we have

$$[K_P : K] = \prod_{i=1}^{n} [K_i : K_{i-1}] \leq \prod_{i=1}^{n} (n - i + 1) = n!. \square$$

2.3 Field Automorphisms

We now can speak of functions from field extensions to other field extensions. Recall that all non-trivial field homomorphisms are injective. Now, suppose we have $L_1 \supseteq K_1$ and $L_2 \supseteq K_2$, and suppose further we have an isomorphism $\tau : K_1 \to K_2$. We want to know when we can extend τ into an isomorphism $\phi : L_1 \to L_2$. First, we will consider homomorphisms, in other words injections, and then we will consider in what cases we have surjectivity.

Theorem 2.3.1: Let $L_1 = K_1(\alpha)$ for some α algebraic over K_1. Then $\phi : L_1 \to L_2$ exists if and only if L_2 contains β, a root of $\tau(m_{\alpha, K_1}) \in K_2[x]$. Furthermore, for each root $\beta \in L_2$, we have a homomorphism $\phi_\beta : L_1 \to L_2$. Moreover, ϕ_β is an isomorphism between $K_1(\alpha)$ and $K_2(\beta)$ and is the unique extension of τ so that $\phi_\beta(\alpha) = \beta$.

Proof: First suppose that $\phi : L_1 \to L_2$ is an extension of τ. Then $\beta = \phi(\alpha) \in L_2$. Then,

$$\tau(m_{\alpha, K_1})(\beta) = \phi(m_{\alpha, K_1})(\phi(\alpha))$$

since ϕ restricted to K_1 is τ. Since ϕ is a homomorphism,

$$\phi(m_{\alpha,K_1})(\phi(\alpha)) = \phi(m_{\alpha,K_1}(\alpha)) = \phi(0) = 0.$$

Thus, β is a root of $\tau(m_{\alpha,K_1})$.

Now, suppose that $\beta \in L_2$ is a root of $\tau(m_{\alpha,K_1})$. Recall that $K_1(\alpha) \cong K_1[x]/(m_{\alpha,K_1})$. Thus, it suffices to find a homomorphism from $K_1[x]/(m_{\alpha,K_1})$ to $K_2(\beta)$. From the fundametal homomorphism theorem, we can define a homomorphism Φ_β from $K_1[x] \to K_2(\beta)$ so that $\Phi_\beta(P(x)) = \tau(P)(\beta)$. Then, the kernel of Φ_β is

$$\begin{aligned} ker(\Phi_\beta) &= \{P \in K_1[x] \mid \tau(P)(\beta) = 0\} \\ &= \{P \in K_1[x] \mid \tau(P) \in (m_{\beta,K_2})\} \\ &= \{P \in K_1[x] \mid \tau P \in (\tau(m_{\alpha,K_1}))\} \\ &= \{P \in K_1[x] \mid P \in (m_{\alpha,K_1}) \\ &= (m_{\alpha,K_1}). \end{aligned}$$

Thus, we have a unique well-defined isomorphism $\Phi_\beta : K_1[x]/(m_{\alpha,K_1}) \to K_2(\beta)$ so that $x \mapsto \beta$. $\square$

This theorem has several corollaries:

Corollary 1: Suppose we have $K_1 = K_2 = K$ and τ is the identity function on K. Let $\phi : L_1 \to L_2$ be any extension of τ, so in other words, ϕ fixes K. Then, for $\alpha \in L_1$, $\phi(\alpha) \in L_2$ is a root of $m_{\alpha,K}$. In other words, any extension of a field automorphism permutes roots of minimal polynomials.

Proof (Corollary 1): This is clear by applying the theorem to ϕ restricted to $K(\alpha)$. $\square$

Example: Consider $\mathbb{Q}(\sqrt[3]{2}) \supseteq \mathbb{Q}$ and $\mathbb{Q}(\sqrt[3]{2}\zeta_3) \supseteq \mathbb{Q}$. Then, any homomorphism $\phi : \mathbb{Q}(\sqrt[3]{2}) \to \mathbb{Q}(\sqrt[3]{2}\zeta_3)$ must permute the roots of $x^3 - 2$. Thus, the only one that exists is defined by $\phi(\sqrt[3]{2}) = \sqrt[3]{2}\zeta_3$ and $\phi(1) = 1$.

Corollary 2: Let $L_1 = K(\alpha_1, \alpha_2, \ldots, \alpha_n)$ be a splitting field of a polynomial $P \in K[x]$. Suppose $\phi : L_1 \to L_2$ is an isomorphism that also fixes K. Then $L_2 = L_1 = K(\alpha_1, \alpha_2, \ldots, \alpha_n)$ and ϕ restricts to a permutation of the $\{\alpha_i\}$ and is completely determined by the permutation.

Proof (Corollary 2): From Corollary 1, we know that ϕ defines a permutation of the roots of $m_{\alpha,K}$, so $L_1 \subseteq L_2$. However, since ϕ is an isomorphism, $[L_1 : K] = [L_2 : K]$, so in

fact $L_1 = L_2$. $\square$

Example: Let $\alpha = \sqrt[3]{2}$. Suppose we let $L_1 = \mathbb{Q}(\alpha, \zeta_3\alpha, \zeta_3^2\alpha)$, the splitting field of $x^3 - 2$. Then, any field homomorphism of L_1 that fixes $\mathbb{Q}$ (which is any non-trivial homomorphism, since all non-trivial field homomorphisms fix $\mathbb{Q}$ by definition) must be an automorphism of L_1 that permutes the three roots of $x^3 - 2$.

Corollary 3: Now suppose $K_1, K_2|K$ are finite and $L|K$ is a splitting field containing K_1. Further suppose that $\tau : K_1 \to K_2$ fixes K and is an isomorphism. Then τ extends to an automorphism $\phi : L \to L$.

Proof (Corollary 3): We can see this using the primitive element theorem: $L = K_1(\beta)$ and for any root β' of $\tau(m_{\beta,K_1})$, we can find an isomorphism $\phi : K_1(\beta) \to K_2(\beta')$ extending τ. Thus, by corollary 2, $L = K_2(\beta')$, so ϕ is in fact a field automorphism of L that extends τ. $\square$

Example: Let $\alpha = \sqrt[3]{2}$, and let $K_1 = \mathbb{Q}(\alpha)$ and $K_2 = \mathbb{Q}(\alpha\zeta_3)$, and let τ be defined by $\tau(\alpha) = \alpha\zeta_3$. Then, we can extend τ to an automorphism ϕ of $\mathbb{Q}(\alpha, \zeta_3\alpha, \zeta_3^2\alpha)$ in the following way:

$$\begin{aligned} \phi(\alpha) &= \alpha\zeta_3 \\ \phi(\alpha\zeta_3) &= \alpha\zeta_3^2 \\ \phi(\alpha\zeta_3^2) &= \alpha. \end{aligned}$$

Note this is not the unique way of extending τ: We can define another field automorphism that extends τ, φ, such that $\varphi(\alpha\zeta_3) = \alpha$ and φ fixes $\alpha\zeta_3^2$. This corollary only guarantees that some extension exists; it does not guarantee uniqueness.

Suppose we have a field extension $L|K$ so that, for all $\alpha \in L$, all roots of $m_{\alpha,K}$ are in L. We call such a field extension *normal*. Equivalently, if a minimal polynomial $P \in K[x]$ has a root in L, then P splits into linear factors in L.

Theorem 2.3.2: $L|K$ is a splitting field if and only if L is finite and normal.

Proof: First, suppose that $L = K(\alpha_1, \alpha_2, \ldots, \alpha_n)$ is a splitting field of some polynomial $P \in K[x]$. Now, let $\beta \in L$, and let β_j be some root of $m_{\beta,K}$. From theorem 2.3.1, there exists an isomorphism $\tau : K(\beta) \to K(\beta_j)$. Furthermore, by corollary 3, τ extends to an isomorphism $\phi : L \to L$ so that $\phi(\beta) = \tau(\beta) = \beta_j$. Thus, $\beta_j \in L$. So L must contain all roots of $m_{\beta,K}$. Thus, L is normal.

Now, suppose that $L|K$ is finite and normal. We know there is some $\gamma \in L$ so that

$L = K(\gamma)$. Since L is normal, all the roots of $m_{\gamma,K}$ are in L. Thus,

$$L = K(\gamma) = K(\gamma_1, \gamma_2, \ldots, \gamma_n),$$

which implies L is the splitting field of $m_{\gamma,K}$. $\square$

2.4 The Galois Group

Suppose we have an extension $L|K$ that is finite and normal. From Theorem 2.3.1, we know there are automorphisms of L that fix K. We define the *Galois group* of L over K to be the group of all field automorphisms of L that fix K under function composition. In other words,

$$\mathrm{Gal}(L|K) = \{\sigma : L \to L \mid \sigma \text{ is an isomorphism and } \sigma(k) = k \text{ for all } k \in K\}.$$

Example: Consider $\mathbb{Q}(\zeta_{17})$, the splitting field of $\Phi_{17}(x)$, the 17th cyclotomic polynomial. First observe that every field automorphism is uniquely determined by the image of ζ_{17} under the automorphism. Furthermore, ζ_{17} must map to another primitive 17th root of unity, from our homomorphism theorem. Thus, for all $1 \leq j \leq 16$, we can define a function σ_j on this field so that $\sigma_j(\zeta_{17}) = \zeta_{17}^j$, and these are the only field automorphisms of $\mathbb{Q}(\zeta_{17})$. Thus,

$$\mathrm{Gal}(\mathbb{Q}(\zeta_{17}|\mathbb{Q})) = \{\sigma_j | 1 \leq j \leq 16\} \cong (\mathbb{Z}/17\mathbb{Z})^* \cong \mathbb{Z}/16\mathbb{Z},$$

the cyclic group of order 16. This generalizes for all $\mathbb{Q}(\zeta_p)$ for p prime:

$$\mathrm{Gal}(\mathbb{Q}(\zeta_p|\mathbb{Q})) \cong \mathbb{Z}/(p-1)\mathbb{Z}.$$

Even more generally, for any n,

$$\mathrm{Gal}(\mathbb{Q}(\zeta_n|\mathbb{Q})) \cong (\mathbb{Z}/n\mathbb{Z})^*,$$

the group of multiplicative units in $\mathbb{Z}/n\mathbb{Z}$. This isomorphism is intuitive: $\zeta_n^k \mapsto k \in \mathbb{Z}/n\mathbb{Z}$.

Note that, since L is a splitting field of m_α over K and every field automorphism of L permutes the roots of m_α, these permutations give a natural injection from the Galois group to the symmetric group of the roots of m_α:

$$\mathrm{Gal}(L|K) \hookrightarrow \mathrm{Sym}(\{\alpha_1, \alpha_2, \ldots, \alpha_n\}) \cong S_n.$$

Thus, we have $n \leq |\mathrm{Gal}(L|K)| \leq n!$, just like $[L : K]$.

Theorem 2.4.1 $|\mathrm{Gal}(L|K)| = [L : K]$.

Proof: Let $L = K(\gamma)$. Then $d = [L : K]$ is the degree of m_γ. Recall from above that $L = K(\gamma) = K(\gamma_i) = K(\gamma_1, \gamma_2, \ldots, \gamma_d)$, where the γ_i's are roots of m_γ. From our homomorphism theorem, we can define unique automorphisms that fix K from $K(\gamma_1)$ to $K(\gamma_i)$ by $\phi_i(\gamma_1) = \gamma_i$. Note that these ϕ_i are in fact field automorphisms of L, since $L = K(\gamma_1) = K(\gamma_i)$. This gives us d distinct automorphisms of L, so

$$|\operatorname{Gal}(L|K)| \geq d = [L : K].$$

Now, suppose $\rho \in \operatorname{Gal}(L|K)$. Then $\rho(\gamma)$ must be a root of m_γ. However, ρ is completely determined by $\rho(\gamma)$, so ρ must be one of the d previously constructed automorphisms. Thus, $\operatorname{Gal}(L|K) = [L : K]$. $\square$

Example: Consider again the splitting field of $x^3 - 2$. First, recall that this extension is of degree 6 and further note that it is equal to the field $\mathbb{Q}(\alpha, \zeta_3)$, with basis $\{1, \zeta_3, \alpha, \alpha\zeta_3, \alpha^2, \alpha^2\zeta_3\}$. Thus, we would expect $\operatorname{Gal}(\mathbb{Q}(\alpha, \zeta_3)|\mathbb{Q})$ to have 6 elements. Furthermore, since this is the splitting field of a degree 3 polynomial, we know that the Galois group must be isomorphic to a subgroup of S_3. Since it has 6 elements, it must be isomorphic to S_3 itself. We will show this. Let σ be the automorphism defined by

$$\sigma(\alpha) = \alpha\zeta_3,\ \sigma(\zeta_3) = \zeta_3.$$

Let τ be the automorphism defined by

$$\tau(\alpha) = \alpha,\ \tau(\zeta_3) = \zeta_3^2.$$

Remember that any automorphism must still represent a permutation of the three roots of $x^3 - 2$. The automorphism σ represents the permutation $(\alpha, \alpha\zeta_3, \alpha^2\zeta_3)$, when written in cycle notation, and τ represents the permutation $(\alpha)(\alpha\zeta_3, \alpha^2\zeta_3)$. Now,

$$\operatorname{Gal}(\mathbb{Q}(\alpha, \zeta_3)|\mathbb{Q}) = \{e, \sigma, \sigma^2, \tau, \sigma\tau, \sigma^2\tau\} \cong S_3,$$

where $\sigma \mapsto (123)$ and $\tau \mapsto (23)$, like we want.

2.5 The Galois Correspondence

The Galois group encodes information about the structure of a given field extension: it describes every possible field automorphism of the top field that fixes the base field. Furthermore, it connects two different algebraic structures, fields and groups, in an intimate way. When given a group, it is natural to talk about its subgroups and normal subgroups. The subgroups of the Galois group in fact exactly describe the intermediate fields and which of these are normal in a field extension. This bijection, due to Galois and subsequently called the Galois correspondence, is a beautiful theorem in algebra which gives the relation

and interplay between groups and fields. It also has some very nice applications to classic problems in abstract algebra, including proving the unsolvability of quintics, which was one of the primary problems that originally motivated Galois to develop this mathematics.

The correspondence develops very naturally. As we already have seen above, some automorphisms of $L|K$ fix larger fields than K. Let $H \leq G$. Then,

$$\mathrm{Fix}(H) = \{x \in K | h(x) = x \text{ for all } h \in H\}.$$

Note that this fixed set is in fact a field and $K \subseteq \mathrm{Fix}(H) \subseteq L$. Thus, we can describe intermediate fields by the subgroups that fix them.

Similarly, for $K \subseteq M \subseteq L$ an intermediate field, $L|M$ is a splitting field, so is finite and normal. Thus, we have

$$\mathrm{Gal}(L|M) = \{\varphi : L \to L | \varphi(m) = m \text{ for all } m \in M\}.$$

Note that $\mathrm{Gal}(L|M) \leq \mathrm{Gal}(L|K)$. Thus, we also have a map from intermediate fields to subgroups of the Galois group. The task is to show these are in fact inverse maps.

Theorem (Galois Correspondence): Let $L|K$ be a finite normal extension. Then, there is a natural bijection between the subgroups of $\mathrm{Gal}(L|K)$ and the intermediate fields $K \subseteq M \subseteq L$ as described by the following maps:

$$H \longmapsto \mathrm{Fix}(H)$$

$$\mathrm{Gal}(L|M) \longmapsto K \subseteq M \subseteq L$$

Furthermore, normal subgroups correspond to intermediate fields M where $M|K$ is normal, and

$$\mathrm{Gal}(L|K)/\mathrm{Gal}(L|M) = \mathrm{Gal}(M|K).$$

Proof of the Galois Correspondence: We will show that $H = \mathrm{Gal}(L|\,\mathrm{Fix}(H))$ for all $H \leq \mathrm{Gal}(L|K)$ and that $\mathrm{Fix}(\mathrm{Gal}(L|M)) = M$ for all $K \subseteq M \subseteq L$.

First suppose that $H \leq \mathrm{Gal}(L|K)$ is given. Note that every $h \in H$ fixes $\mathrm{Fix}(H)$, by definition, so $H \leq \mathrm{Gal}(L|\,\mathrm{Fix}(H))$. Thus $|H| \leq |\,\mathrm{Gal}(L|\,\mathrm{Fix}(H))| = [L : \mathrm{Fix}(H)]$. We will show that $[L : \mathrm{Fix}(H)] \leq |H|$ to prove equality.

By the primitive element theorem, we know that there is some $\gamma \in L$ so that $L = \mathrm{Fix}(H)(\gamma)$. Furthermore, H permutes the roots of $m_{\gamma,\mathrm{Fix}(H)}$. Consider the set of the images of γ under elements of H:

$$W := \{h(\gamma) | h \in H\}.$$

Note that $|W| \leq |H|$. Consider the polynomial

$$P(x) = \prod_{w \in W} (x - w) \in L[x].$$

Note that, for any $h \in H$,

$$h(P(x)) = h\Big(\prod_{w \in W} (x - w) \Big) = \prod_{w \in W} (x - h(w)) = \prod_{w \in W} (x - w).$$

Thus, $P(x) \in \mathrm{Fix}(H)[x]$. Moreover, $P(\gamma) = 0$ since $\gamma = e_H(\gamma) \in W$. Thus,

$$[L : \mathrm{Fix}(H)] \leq d_{m_{\gamma, \mathrm{Fix}(H)}} \leq d_{P(x)} = |W| \leq |H|,$$

which implies that $|H| = [L : \mathrm{Fix}(H)]$, so in fact $H = \mathrm{Gal}(L|\,\mathrm{Fix}(H))$.

Now, suppose that an intermediate field M is given. By the definition of $\mathrm{Gal}(L|M)$, note that $M \subseteq \mathrm{Fix}(\mathrm{Gal}(L|M))$. From above, we have shown that

$$\mathrm{Gal}(L|M) = \mathrm{Gal}(L|\,\mathrm{Fix}(\mathrm{Gal}(L|M))).$$

Thus, $[L : M] = [L : \mathrm{Fix}(\mathrm{Gal}(L|M))]$. From the Tower Law, however,

$$[L : M] = [L : \mathrm{Fix}(\mathrm{Gal}(L|M))][\mathrm{Fix}(\mathrm{Gal}(L|M)) : M],$$

so $[\mathrm{Fix}(\mathrm{Gal}(L|M)) : M] = 1$. Thus,

$$\mathrm{Fix}(\mathrm{Gal}(L|M)) = M.$$

We have proven that this map is in fact a bijective correspondence between the intermediate fields of our extension and the subgroups of our Galois group. Now, we must show that normal subgroups correspond to normal subfields.

First, suppose that $K \subseteq M \subseteq L$ with $M|K$ normal. Then, $M|K$ is a splitting field extension $K(\alpha_1, \alpha_2, \ldots, \alpha_n)$ where the α_i's are roots of a polynomal $P(x) \in K[x]$. Moreover, $\mathrm{Gal}(L|K)$ permutes the roots of P. Thus, for all $\phi \in \mathrm{Gal}(L|K)$, ϕ restricts to an automorphism of M. Thus, we can define a group homomorphism so that

$$\begin{array}{rcl} \rho : \mathrm{Gal}(L|K) & \longrightarrow & \mathrm{Gal}(M|K) \\ \phi & \longmapsto & \phi|_M. \end{array}$$

The kernel of this homomorphism is exactly the set of functions in $\mathrm{Gal}(L|K)$ that restrict to the identity on M, which is the set of functions that fix M, $\mathrm{Gal}(L|M)$. Since this is the

kernel of a homomorphism, this group is normal, and the first isomorphism theorem gives that

$$\mathrm{Gal}(L|K)/\mathrm{Gal}(L|M) \cong \mathrm{Im}(\rho).$$

However, from the tower law,

$$|\mathrm{Gal}(L|K)/\mathrm{Gal}(L|M)| = \frac{|\mathrm{Gal}(L|K)|}{|\mathrm{Gal}(L|M)|} = \frac{[L:K]}{[L:M]} = [M:K] = |\mathrm{Gal}(M|K)|.$$

Thus, $\mathrm{Gal}(L|K)/\mathrm{Gal}(L|M) \cong \mathrm{Gal}(M|K)$.

Now, suppose that $H \trianglelefteq \mathrm{Gal}(L|K)$. We will show that $\mathrm{Fix}(H)|K$ is a normal extension. Let $\alpha \in \mathrm{Fix}(H)$ be arbitrary, and let $\alpha' \in L$ be one of the roots of m_α. We want to show that $\alpha' \in \mathrm{Fix}(H)$, or that $h(\alpha') = \alpha'$ for all $h \in H$. We define a homomorphism $\tau : K(\alpha) \to K(\alpha')$ so that τ fixes K and $\tau(\alpha) = \alpha'$. From our homomorphism theorem, we can extend τ to a field automorphism $\phi \in \mathrm{Gal}(L|K)$. Now, let $h \in H$. Then

$$h(\alpha') = h(\phi(\alpha)) = (h \circ \phi)(\alpha) = (\phi \circ \phi^{-1} \circ h \circ \phi)(\alpha).$$

Since $H \trianglelefteq \mathrm{Gal}(L|K)$, we know $\phi^{-1} \circ h \circ \phi = h' \in H$. Thus,

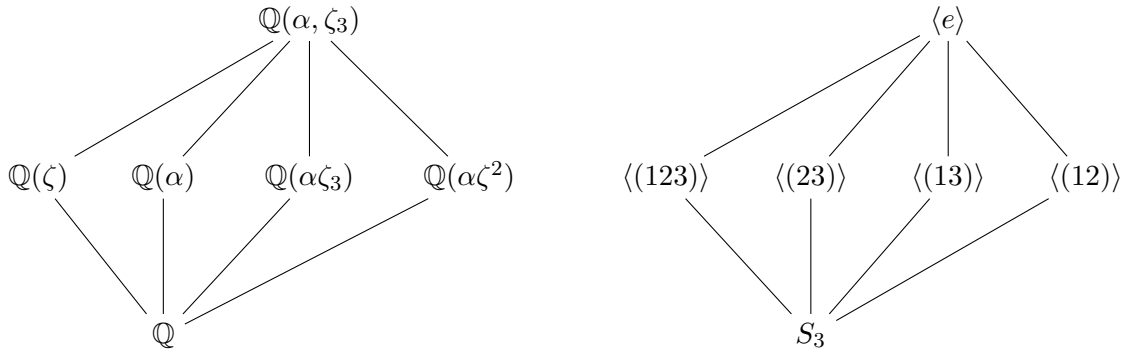
$$(\phi \circ \phi^{-1} \circ h \circ \phi)(\alpha) = (\phi \circ h')(\alpha) = \phi(h'(\alpha)) = \phi(\alpha) = \alpha'.$$

Thus, $h(\alpha') = \alpha'$, so $\alpha' \in \mathrm{Fix}(H)$, like we want. $\square$

Example 1: Recall, as we showed above, that $\mathrm{Gal}(\mathbb{Q}(\alpha, \zeta_3)|\mathbb{Q}) \cong S_3$. We know the subgroups of S_3 are as follows:

$$\langle e \rangle, \langle (12) \rangle, \langle (13) \rangle, \langle (23) \rangle, \langle (123) \rangle, S_3.$$

We want to find the fields that correspond to each of these subgroups. Note that $\mathrm{Fix}(\langle e \rangle) = \mathbb{Q}(\alpha, \zeta_3)$, so $\langle e \rangle$ corresponds to the whole field. Similarly, $\mathbb{Q}$ corresponds to S_3. Now, as above, σ is the permutation which is defined to fix ζ_3. Therefore, the subgroup generated by σ, equivalent to $\langle (123) \rangle$, corresponds to $\mathbb{Q}(\zeta_3)$. Similarly, τ fixes α, so $\langle (23) \rangle$ corresponds to $\mathbb{Q}(\alpha)$. Now, $\sigma \circ \tau$ fixes $\alpha\zeta_3^2$, so the subfield $\mathbb{Q}(\alpha\zeta_3^2)$ corresponds to the subgroup $\langle (12) \rangle$. Similarly, $\mathbb{Q}(\alpha\zeta_3)$ corresponds to $\langle (13) \rangle$. The figure below illustrates this correspondence:



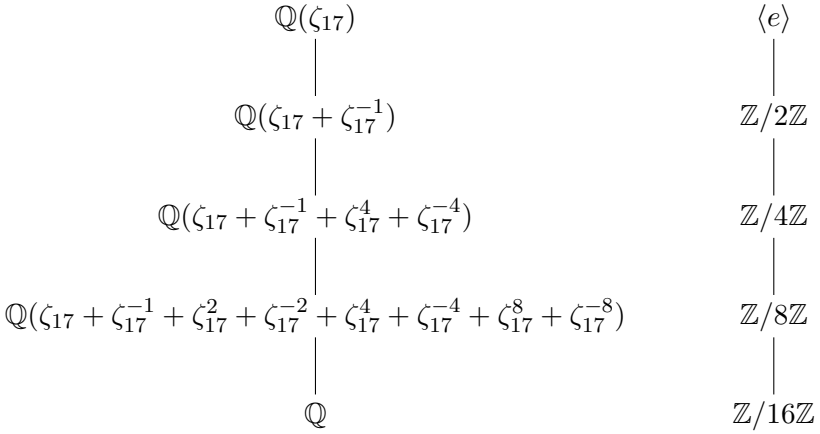
Example 2: Consider the field $\mathbb{Q}(\zeta_{17})$. We already argued that this field has Galois group over $\mathbb{Q}$ isomorphic to $\mathbb{Z}/16\mathbb{Z}$. Since this is commutative, every subgroup is normal, therefore every subfield of $\mathbb{Q}(\zeta_{17})$ is normal. The subgroups of $\mathbb{Z}/16\mathbb{Z}$ are

$$e \trianglelefteq \mathbb{Z}/2\mathbb{Z} \trianglelefteq \mathbb{Z}/4\mathbb{Z} \trianglelefteq \mathbb{Z}/8\mathbb{Z} \trianglelefteq \mathbb{Z}/16\mathbb{Z},$$

where each adjacent quotient is $\mathbb{Z}/2\mathbb{Z}$. Thus, $\mathbb{Q}(\zeta_{17})$ has a chain of normal subfields, where the degree between adjacent fields is 2. We have the following chain:

$$\mathbb{Q}(\zeta_{17}) \supseteq \mathbb{Q}(\zeta_{17}+\zeta_{17}^{-1}) \supseteq \mathbb{Q}(\zeta_{17}+\zeta_{17}^{-1}+\zeta_{17}^{4}+\zeta_{17}^{-4}) \supseteq \mathbb{Q}(\zeta_{17}+\zeta_{17}^{-1}+\zeta_{17}^{2}+\zeta_{17}^{-2}+\zeta_{17}^{4}+\zeta_{17}^{-4}+\zeta_{17}^{8}+\zeta_{17}^{-8}) \supseteq \mathbb{Q}$$

which corresponds to the above chain of subgroups. We can see this from the intuition of Galois groups in cyclotomic fields addressed above: Since the subgroup of $(\mathbb{Z}/17\mathbb{Z})^*$ isomorphic to $\mathbb{Z}/2\mathbb{Z}$ is $\{1,-1\}$, ζ_{17} and ζ_{17}^{-1} must be fixed by the subgroup $\mathbb{Z}/2\mathbb{Z}$. Thus $\mathbb{Q}(\zeta_{17}+\mathbb{Q}\zeta_{17}^{-1})$ is fixed by $\mathbb{Z}/2\mathbb{Z}$. The other subfields follow similarly. The image below illustrates the correspondence:



The Galois Correspondence can be used to prove that polynomials of degree 5 or higher cannot be solved by radicals. For a proof, see [1]. Furthermore, it can be used to prove which n-gons are constructible. The proof (see [12]) relies on the fact that the nth roots of unity are the algebraic interpretation of geometrical regular n-gons. This interplay between geometric constructions and the nth roots of unity is a vital connection in mathematics, and one of the many reasons the Kronecker-Weber Theorem is so strong, since it restricts an entire class of possible field extensions to an easily understood geometrical object: a regular n-gon.

2.6 Field Compositums

Suppose we have normal finite field extensions $L \supseteq K$ and $M \supseteq K$. Recall that their *field compositum* is the smallest field which contains both L and M. We denote it LM. Note that LM is also a normal extension of K. This gives us a way to concatenate two fields, and still maintain the properties we had before.

Theorem (2.6.1): $\mathrm{Gal}(LM|K)$ is a subgroup of $\mathrm{Gal}(L|K) \times \mathrm{Gal}(M|K)$. In particular, it is the subgroup J of pairs (σ, τ) where $\sigma = \tau$ on $L \cap M$.

Proof: We construct an isomorphism $\phi : \mathrm{Gal}(LM|K) \to J$ so that $\phi(\rho) = (\rho|_L, \rho|_M)$, for $\rho \in \mathrm{Gal}(LM|K)$. First we will show ϕ is injective: if $\sigma = \rho|_L$ and $\tau = \rho|_M$, then by definition for $x \in L \cup M$, $\sigma(x) = \tau(x) = \rho(x)$. Now, suppose ρ_1 and ρ_2 map to (σ, τ). Then, $\rho_1|_L = \rho_2|_L$, so for $l \in L$, $\rho_1(l) = \rho_2(l)$. Similarly, for $m \in M$, $\rho_1(m) = \rho_2(m)$. However, everything else in the field compositum is uniquely determined since L and M generate LM: For $x \in LM$, $\rho(x) = a \cdot \rho(l_1) + b \cdot \rho(m_1) + c \cdot \rho(l_2)\rho(m_2)$ where $l_1, l_2 \in L$ and $m_1, m_2 \in M$ and $a, b, c \in K$ are constants. Thus, for all $x \in LM$, $\rho_1(x) = \rho_2(x)$, so ϕ is injective.

Now we show that ϕ is surjective. Let $(\sigma, \tau) \in J$. Then, we construct $\rho \in \mathrm{Gal}(LM|K)$ that maps to (σ, τ):

$$\rho(x) = \rho(a \cdot l_* + b \cdot m_*) = a\rho(l_*) + b\rho(m_*) = a\sigma(l_*) + b\tau(m_*). \square$$

Example: Consider $\mathbb{Q}(\zeta_3)$ and $\mathbb{Q}(\zeta_{17})$. Then, the field compositum, $\mathbb{Q}(\zeta_3)\mathbb{Q}(\zeta_{17})$, has Galois group isomorphic to a subgroup of $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/17\mathbb{Z}$. However, since $\mathbb{Q}(\zeta_3) \cap \mathbb{Q}(\zeta_{17}) = \mathbb{Q}$, the Galois group of the field compositum is in fact the whole product.

2.7 Cyclotomic Polynomials

A *cyclotomic extension* is a field extension of $\mathbb{Q}$ of the form $\mathbb{Q}(\zeta_m)$ for some m. As a slight abuse of notation, all subfields of cyclotomic extensions will be called cyclotomic fields, to indicate that they are contained inside a larger cyclotomic extension.

Theorem 2.7.1: The compositum of cyclotomic fields is cyclotomic.

Proof: Let $K \subseteq \mathbb{Q}(\zeta_m)$ and $L \subseteq \mathbb{Q}(\zeta_n)$. Then, $KL \subseteq \mathbb{Q}(\zeta_m)\mathbb{Q}(\zeta_n) = \mathbb{Q}(\zeta_{lcm(m,n)})$. We can describe this relationship geometrically: the smallest k-gon which contains both a regular m-gon and a regular n-gon in its vertices is $k = lcm(m, n)$. $\square$

Recall that every cyclotomic extension ($\mathbb{Q}(\zeta_m)$ for some m) is abelian, since its Galois group is $(\mathbb{Z}/m\mathbb{Z})^*$, which is an abelian group of order $\phi(m)$. Remember the Kronecker-Weber Theorem states that the converse is also true: every abelian extension is cyclotomic (a subfield of a cyclotomic extension). Yet another part of the reason why this theorem is so powerful is that it restricts abelian extensions to very well-understood fields. Furthermore, cyclotomic fields have a lot of inherent geometry, as discussed above, so this theorem relates a class of groups with the geometry of the complex plane, specifically the regular n-gons formed by the roots of unity through the Galois correspondence, as mentioned above. However, this theorem requires a higher understanding of how much information the Galois group encodes about the field extension, which we get from algebraic number theory.

3 Ramification Theory

The proof of the Kronecker-Weber Theorem that we present relies on algebraic number theory, without using the more powerful tools of class field theory. The following is the number theoretical background for the proof. From classic Galois theory, we have the basic story of the Galois correspondence, applying to field extensions and subfields. However, there is another layer. Specifically, $\mathbb{Z} \subseteq \mathbb{Q}$, the ring of integers, has more structure than $\mathbb{Q}$, namely ideals, which are lost in fields. We call the *algebraic integers* the set of complex numbers that are zeros of monic polynomials in $\mathbb{Z}[x]$.

3.1 Dedekind Domains

Let $K \supseteq \mathbb{Q}$ be a field extension. Let $\mathcal{O}_K$ denote K intersected with the algebraic integers, the ring of integers in K. Note that $\mathcal{O}_K$ has the following properties:

- $\mathcal{O}_K$ is *noetherian*, that is every chain of ideals $\mathcal{I}_1 \subseteq \mathcal{I}_2 \subseteq \ldots \subseteq \mathcal{I}_k \subseteq \ldots$ has a maximal element. The main idea of the proof is that every ideal admits a finite integral basis over $\mathbb{Z}$, since K has a finite integral basis over $\mathbb{Q}$, and can be found in [11].
- $\mathcal{O}_K$ is *integrally closed*. We define the *integral closure* of a ring $A \subseteq B$ as

$$\bar{A} = \{b \in B | b \text{ integral over } A\}$$

in other words, the ring of numbers which are roots of monic polynomials in $A[x]$ contained in B. If $\bar{A} = A$, then A is *integrally closed*. Note that the integral closure of a ring is integrally closed [9]. Since $\mathcal{O}_K$ is the integral closure of $\mathbb{Z}$ in K, $\mathcal{O}_K$ is integrally closed.

- Every non-zero prime ideal $\mathfrak{p} \subseteq \mathcal{O}_K$ is maximal. Note that $\mathfrak{p} \cap \mathbb{Z} = (p)$, where (p) is a prime ideal in $\mathbb{Z}$. Now, $\mathcal{O}_K/\mathfrak{p}$ is an extension of $\mathbb{Z}/p\mathbb{Z}$ adjoining algebraic elements, so is a field. Thus $\mathfrak{p}$ is maximal.

We call any integral domain with the above properties a *Dedekind domain*.

Theorem (Unique Prime Factorization of Ideals): Every non-zero ideal $\mathfrak{a} \subseteq \mathcal{O}_K$ can be uniquely written, up to order, as

$$\mathfrak{a} = \mathfrak{p}_1\mathfrak{p}_2 \cdots \mathfrak{p}_r$$

where $\mathfrak{p}_1, \mathfrak{p}_2, \ldots, \mathfrak{p}_r$ are prime ideals in $\mathcal{O}_K$.

Note that *elements* of $\mathcal{O}_K$ do not necessarily factor uniquely into irreducibles: Letting $K = \mathbb{Q}(\sqrt{-5})$ gives that $6 = (1 + \sqrt{-5})(1 - \sqrt{-5}) = 2 \cdot 3$.

Lemma 1: For every non-zero ideal $\mathfrak{a} \subseteq \mathcal{O}_K$, there exist non-zero prime ideals $\mathfrak{p}_1, \mathfrak{p}_2, \ldots, \mathfrak{p}_r$ such that

$$\mathfrak{a} \supseteq \mathfrak{p}_1\mathfrak{p}_2 \cdots \mathfrak{p}_r.$$

Proof: Suppose, for the sake of contradiction, that there are some ideals which do not have the above property, and call this set of ideals $\mathcal{M}$. Since $\mathcal{O}_K$ is noetherian, $\mathcal{M}$ has at least one maximal element, call this ideal $\mathcal{I}$. This cannot be prime, so we can find $b_1, b_2 \subseteq \mathcal{O}_K$ where $b_1b_2 \in \mathcal{I}$ but $b_1 \notin \mathcal{I}$ and $b_2 \notin \mathcal{I}$. Let $\mathcal{I}_1 = (b_1) + \mathcal{I}$ and $\mathcal{I}_2 = (b_2) + \mathcal{I}$. Then $\mathcal{I} \subseteq \mathcal{I}_1$ and $\mathcal{I} \subseteq \mathcal{I}_2$ and $\mathcal{I}_1\mathcal{I}_2 \subseteq \mathcal{I}$. Since $\mathcal{I}$ is a maximal ideal that does not contain a product of prime ideals, both $\mathcal{I}_1$ and $\mathcal{I}_2$ do. However, their product is in $\mathcal{I}$, which yields our desired contradiction. $\square$

Lemma 2: Let $\mathfrak{p}$ be a prime ideal of $\mathcal{O}_K$. We define

$$\mathfrak{p}^{-1} := \{x \in K | x\mathfrak{p} \subseteq \mathcal{O}_K\}.$$

Then $\mathfrak{a}\mathfrak{p}^{-1} \neq \mathfrak{a}$ for non-zero ideals $\mathfrak{a}$.

Proof: Let $a \in \mathfrak{p}$ non-zero. From Lemma 1, we know there is

$$\mathfrak{p}_1\mathfrak{p}_2 \cdots \mathfrak{p}_r \subseteq (a) \subseteq \mathfrak{p}.$$

Choose this so that r is minimal. Since $\mathfrak{p}$ is prime, some $\mathfrak{p}_i$, say $\mathfrak{p}_1$ is contained in $\mathfrak{p}$, but since $\mathfrak{p}_1$ is maximal, that implies that $\mathfrak{p}_1 = \mathfrak{p}$. However, since we chose r to be minimal, we can find some $b \in \mathfrak{p}_2\mathfrak{p}_3 \cdots \mathfrak{p}_r$ so that $b \notin (a)$. Thus, $a^{-1}b \notin \mathcal{O}_K$.

However, we also have that $b\mathfrak{p} \subseteq (a)$, so $a^{-1}b\mathfrak{p} \subseteq \mathcal{O}_K$. Thus $a^{-1}b \in \mathfrak{p}^{-1}$. Thus, $\mathfrak{p}^{-1} \not\subseteq \mathcal{O}_K$.

Now, suppose for contradiction that we have a non-zero ideal $\mathfrak{a}$ so that $\mathfrak{a}\mathfrak{p}^{-1} = \mathfrak{a}$. Let $\alpha_1, \alpha_2, \ldots, \alpha_n$ be generators of $\mathfrak{a}$ as a module over $\mathbb{Z}$. Then for all $y \in \mathfrak{p}^{-1}$, we have

$$y\alpha_i = \sum_{j=1}^{n} a_{ij}\alpha_j,\ a_{ij} \in \mathcal{O}_K.$$

We can express these coefficients in a matrix. Let A be the matrix where the ijth entry is $(y\delta_{ij} - a_{ij})$, where δ_{ij} is the ijth entry of the identity matrix. Note that by our definition of A,

$$A \cdot (\alpha_1, \alpha_2, \ldots, \alpha_n)^T = 0.$$

We can consider A as a system of linear equations in K. Since this product is 0, $\alpha_1, \alpha_2, \ldots, \alpha_n$ gives a non-zero solution to this system of equations, which implies that the determinant of A is 0. Thus, y is a zero of the polynomial

$$f(x) = \det(x\delta_{ij} - a_{ij}) \in \mathcal{O}_K[x].$$

Thus, $y \in \mathcal{O}_K$, since $\mathcal{O}_K$ is integrally closed, which implies that $\mathfrak{p}^{-1} \subseteq \mathcal{O}_K$, which gives our desired contradiction. $\square$

Proof of Unique Prime Factorization of Ideals: Existence: Let $\mathcal{M}$ be the set of ideals not equal to (1) or (0) without a prime ideal decomposition. Suppose, for the sake of contradiction, that $\mathcal{M}$ is non-empty. Recall from before $\mathcal{O}_K$ is noetherian, so we can find a maximal ideal of $\mathcal{M}$. Let this ideal be $\mathfrak{a}$. We know $\mathfrak{a} \subseteq \mathfrak{p}$, a maximal ideal of $\mathcal{O}_K$. Furthermore, since $\mathcal{O}_K \subseteq \mathfrak{p}^{-1}$, we have the following containments:

$$\mathfrak{a} \subseteq \mathfrak{a}\mathfrak{p}^{-1} \subseteq \mathfrak{p}\mathfrak{p}^{-1} \subseteq \mathcal{O}_K.$$

From our first lemma, we have $\mathfrak{a} \neq \mathfrak{a}\mathfrak{p}^{-1}$ and $\mathfrak{p} \neq \mathfrak{p}\mathfrak{p}^{-1}$. Furthermore, since $\mathfrak{p}$ is maximal, $\mathfrak{p}\mathfrak{p}^{-1} = \mathcal{O}_K$. Recall that $\mathfrak{a}$ is a maximal element of $\mathcal{M}$, so $\mathfrak{a}\mathfrak{p}^{-1} \notin \mathcal{M}$. Furthermore, $\mathfrak{a} \neq \mathfrak{p}$, so $\mathfrak{a}\mathfrak{p}^{-1} \neq \mathcal{O}_K$. Thus, $\mathfrak{a}\mathfrak{p}^{-1}$ must have a prime ideal decomposition, $\mathfrak{a}\mathfrak{p}^{-1} = \mathfrak{p}_1\mathfrak{p}_2 \cdots \mathfrak{p}_r$. Thus,

$$\mathfrak{a} = \mathfrak{a}\mathfrak{p}^{-1}\mathfrak{p} = \mathfrak{p}_1\mathfrak{p}_2 \cdots \mathfrak{p}_r\mathfrak{p}.$$

This gives a prime ideal decomposition of $\mathfrak{a}$, contradicting our assumption that $\mathfrak{a} \subseteq \mathcal{M}$. Thus, every ideal has a prime ideal decomposition.

Uniqueness: Suppose

$$\mathfrak{a} = \mathfrak{p}_1\mathfrak{p}_2 \cdots \mathfrak{p}_r = \mathfrak{q}_1\mathfrak{q}_2 \cdots \mathfrak{q}_s$$

are two prime ideal decompositions of $\mathfrak{a}$. Then $\mathfrak{p}_1$ must divide some $\mathfrak{q}_i$, say $\mathfrak{q}_1$. Since $\mathfrak{p}_1$ is maximal, $\mathfrak{p}_1 = \mathfrak{q}_1$. Multiplying by $\mathfrak{p}_1^{-1}$ yields

$$\mathfrak{p}_2 \cdots \mathfrak{p}_r = \mathfrak{q}_2 \cdots \mathfrak{q}_s.$$

Similarly, $\mathfrak{p}_i = \mathfrak{q}_i$ for all $i = 1, \ldots, r = s$. $\square$
Remark: This proof is based on its treatment in [11].

This theorem is particularly powerful, because it allows us to treat ideals in Dedekind domains similarly to integers. Now, in our example of $6 \in \mathbb{Z}[\sqrt{-5}]$, we can write the ideal generated by 6 as a unique product of prime ideals, specifically

$$(6) = (2, 1 + \sqrt{-5})^2 (3, 1 - \sqrt{-5})(3, 1 + \sqrt{-5}).$$

For proof of this factorization, see [15]. Note also that the proof of the Unique Factorization Theorem does not rely on $\mathcal{O}_K$ and rather applies to all Dedekind domains.

We can also generalize the Chinese Remainder Theorem.

Theorem (Chinese Remainder): Let $\mathfrak{a}_1, \mathfrak{a}_2, \ldots, \mathfrak{a}_g$ be ideals in $\mathcal{O}_K$ with the property that $\mathfrak{a}_i + \mathfrak{a}_j = \mathcal{O}_K$ for all $i \neq j$. Let $\mathfrak{a} = \mathfrak{a}_1 \mathfrak{a}_2 \cdots \mathfrak{a}_g$. Then

$$\mathcal{O}_K/\mathfrak{a} \cong \mathcal{O}_K/\mathfrak{a}_1 \oplus \mathcal{O}_K/\mathfrak{a}_2 \oplus \ldots \oplus \mathcal{O}_K/\mathfrak{a}_g,$$

where $A \oplus B = \{(a, b) | a \in A, b \in B\}$. [7] Note that this theorem looks very different in statement from the way the Chinese Remainder Theorem is usually stated. However, the proof below will illustrate that the traditional Chinese Remainder Theorem is in fact a specific case of this theorem.

Proof: Let φ_i be the map from $\mathcal{O}_K$ to $\mathcal{O}_K/\mathfrak{a}_i$ that takes k to $k \mod \mathfrak{a}_i$. Define the map

$$\varphi : \mathcal{O}_K \to \mathcal{O}_K/\mathfrak{a}_1 \oplus \mathcal{O}_K/\mathfrak{a}_2 \oplus \ldots \oplus \mathcal{O}_K/\mathfrak{a}_g$$
$$k \longmapsto (\varphi_1(k), \varphi_2(k), \ldots, \varphi_g(k)).$$

We will show that φ is onto with kernel $\mathfrak{a}$. Let $k_1, k_2, \ldots, k_g \in \mathcal{O}_K$. To show that φ is onto, it suffices to show that the set of congruences

$$x \equiv \varphi_i(k_i),\ i = 1, \ldots, g$$

is solvable, because such an x will map to $(k_1, k_2, \ldots, k_g)$. Note that this is the generalization of the familiar statement of the Chinese Remainder Theorem in $\mathbb{Z}$.

Since $\mathfrak{a}_i + \mathfrak{a}_j = \mathcal{O}_K$ for all $i \neq j$, we have the following product:

$$(\mathfrak{a}_1 + \mathfrak{a}_2)(\mathfrak{a}_1 + \mathfrak{a}_3) \cdots (\mathfrak{a}_1 + \mathfrak{a}_g) = \mathcal{O}_K.$$

Note that in its expansion, every term is in $\mathfrak{a}_1$ except the last. Thus,

$$\mathfrak{a}_1 + \mathfrak{a}_2\mathfrak{a}_3 \cdots \mathfrak{a}_g = \mathcal{O}_K.$$

Thus, there exists $v_1 \in \mathfrak{a}_1$ and $u_1 \in \mathfrak{a}_2\mathfrak{a}_3 \cdots \mathfrak{a}_g$ so that $u_1 + v_1 = 1$. Then $u_1 \equiv 1 \mod \mathfrak{a}_1$ and $u_1 \equiv 0 \mod \mathfrak{a}_i$ for all i greater than 1. Similarly, for each j, we can find a u_j so that $u_j \equiv 1 \mod \mathfrak{a}_j$ and $u_j \equiv 0 \mod \mathfrak{a}_i$ for all $i \neq j$. Then, we have

$$x = k_1u_1 + k_2u_2 + k_3u_3 + \ldots + k_gu_g$$

as a solution to our set of equivalences. Thus, φ is onto.

Now, the kernel of φ is $\mathfrak{a}_1 \cap \mathfrak{a}_2 \cap \ldots \cap \mathfrak{a}_g$, since these are the numbers for which φ_i will be 0 for all i. We must show this set of intersections is in fact the product of the ideals. We proceed by induction on g. Since $\mathfrak{a}_1 + \mathfrak{a}_2 = \mathcal{O}_K$, there exists $a_1 \in \mathfrak{a}_1$ and $a_2 \in \mathfrak{a}_2$ so that $a_1 + a_2 = 1$. Thus, for $a \in \mathfrak{a}_1 \cap \mathfrak{a}_2$, we have

$$a = aa_1 + aa_2 \in \mathfrak{a}_1\mathfrak{a}_2.$$

Thus, $\mathfrak{a}_1 \cap \mathfrak{a}_2 \subseteq \mathfrak{a}_1\mathfrak{a}_2$. Clearly $\mathfrak{a}_1\mathfrak{a}_2 \subseteq \mathfrak{a}_1 \cap \mathfrak{a}_2$, so we have equality. Now suppose that $g > 2$ and we know the equality holds for $g - 1$ ideals. Then,

$$\mathfrak{a}_1 \cap \mathfrak{a}_2 \cap \ldots \mathfrak{a}_g = \mathfrak{a}_1 \cap \mathfrak{a}_2\mathfrak{a}_3 \cdots \mathfrak{a}_g.$$

However, from above, we have that $\mathfrak{a}_1 + \mathfrak{a}_2\mathfrak{a}_3 \cdots \mathfrak{a}_g = \mathcal{O}_K$. Thus, from our case for two ideals, we have that $\mathfrak{a}_1 \cap \mathfrak{a}_2\mathfrak{a}_3 \cdots \mathfrak{a}_g = \mathfrak{a}_1\mathfrak{a}_2 \cdots \mathfrak{a}_g$ as we want. $\square$
Remark: This proof is based on its treatment in [7].

Let us return to our picture, where we have a field extension $K \supseteq \mathbb{Q}$ and the algebraic integers contained inside $\mathcal{O}_K \supseteq \mathbb{Z}$. Let $\mathfrak{p} \subseteq \mathcal{O}_K$ be a prime ideal. Then $\mathfrak{p} \cap \mathbb{Z} = (p)$, a prime ideal in $\mathbb{Z}$. The figure below shows this structure of extensions:

$$\begin{array}{ccccc} K & \supseteq & \mathcal{O}_K & \supseteq & \mathfrak{p} \\ | & & | & & | \\ \mathbb{Q} & \supseteq & \mathbb{Z} & \supseteq & (p) \end{array}$$

By unique factorization, (p) factors into primes,

$$(p) = \mathfrak{p}_1^{e_1}\mathfrak{p}_2^{e_2} \cdots \mathfrak{p}_g^{e_g},$$

where $\mathfrak{p}_1 = \mathfrak{p}$.

Theorem 3.1.1 When K is normal, in the above equation, $e_1 = e_2 = \ldots = e_g$, so (p) factors as such:

$$(p) = (\mathfrak{p}_1\mathfrak{p}_2 \cdots \mathfrak{p}_g)^e.$$

Proof: Let G be the Galois group of $K|\mathbb{Q}$. First, note that G acts on the ring $\mathcal{O}_K$. Note that each element of G must permute the $\mathfrak{p}_i$'s, since each element fixes (p) and the $\mathfrak{p}_i$'s are exactly the ideals that lie over (p). First, we will show that for each i, we can find a $\sigma_i \in \mathrm{Gal}(K|\mathbb{Q})$ so that $\sigma_i(\mathfrak{p}) = \mathfrak{p}_i$.

Let $P = \{\sigma(\mathfrak{p}) \mid \sigma \in G\}$. Suppose there is some i for which $\mathfrak{p}_i \notin P$. Then, from the Chinese Remainder Theorem, we can find $\alpha \in \mathcal{O}_K$ so that $\alpha \cong 0 \mod \mathfrak{p}_i$ and $\alpha \cong 1 \mod \sigma\mathfrak{p}$ for all $\sigma \in G$. Let

$$A = \prod_{\sigma \in G} \sigma\alpha.$$

Note that $A \in \mathfrak{p}_i \cap \mathbb{Z} = p\mathbb{Z}$, since $\alpha \in \mathfrak{p}_i$ but G fixes only $\mathbb{Z}$. Thus, $A \in \mathfrak{p}_i$. Thus, there must be some $\tau \in G$ so that $\tau\alpha \in \mathfrak{p}$, so $\alpha \in \tau^{-1}\mathfrak{p}$, which contradicts that $\alpha \cong 1 \mod \tau^{-1}\mathfrak{p}$.

We call the $\mathfrak{p}_i$'s the ideals *conjugate* to $\mathfrak{p}$, and they are exactly the ideals $\sigma\mathfrak{p}$ for $\sigma \in G$. Thus,

$$(p) = \sigma_i(p) = \sigma_i(\mathfrak{p}_1^{e_1}\mathfrak{p}_2^{e_2} \cdots \mathfrak{p}_g^{e_g}) = \sigma_i(\mathfrak{p}_1)^{e_1}\sigma_i(\mathfrak{p}_2)^{e_2} \cdots \sigma_i(\mathfrak{p}_g)^{e_g}.$$

Therefore, since $\sigma_i(\mathfrak{p}_1) = \mathfrak{p}_i$, $e_i = e_1$ for all i. We call e the *ramification index* of $\mathfrak{p}$ over p. □

Now, let's consider the residue field $\mathcal{O}_K/\mathfrak{p}_i$. This field must have characteristic p, since it is an algebraic extension of $\mathbb{Z}/p\mathbb{Z}$. Let the order of this field be p^{f_i}.

Theorem 3.1.2: All the residue fields $\mathcal{O}_K/\mathfrak{p}_i$ have the same degree,

$$f = f_1 = f_2 = \ldots = f_i.$$

Proof: Taking σ_i as above, we have that $\mathcal{O}_K/\mathfrak{p}_1 \cong \mathcal{O}_K/\sigma_i(\mathfrak{p}_1) = \mathcal{O}_K/\mathfrak{p}_i$. Thus $f_i = f_1$ for all i. Note that $f_i = [\mathcal{O}_K/\mathfrak{p}_i : \mathbb{Z}/p\mathbb{Z}]$, so all these extensions are of the same degree. □

Theorem (Fundamental Equality): Let $n = |G|$, and recall that

$$(p) = (\mathfrak{p}_1 \cdot \mathfrak{p}_2 \cdots \mathfrak{p}_g)^e.$$

Then we have

$$n = efg.$$

Proof: First, note that each residue field from above has order p^f, since $|\mathbb{Z}/p\mathbb{Z}| = p$ and the degree of the extension is f. Furthermore, $\mathcal{O}_K/\mathfrak{p}_i^e$ has p^{ef} elements for all i: We define a map from $\mathfrak{p}_i^{e-1}/\mathfrak{p}_i^e$ to $\mathcal{O}_K/\mathfrak{p}_i$ so that $k \mapsto k\alpha + \mathfrak{p}_i^e$, for some $\alpha \in \mathfrak{p}_i^{e-1}$ and $\alpha \notin \mathfrak{p}_i^e$. Note this is an isomorphism, so $\mathfrak{p}_i^{e-1}/\mathfrak{p}_i^e$ has p^f elements.

Also $\mathfrak{p}_i^e + \mathfrak{p}_j^e = \mathcal{O}_K$ for $i \neq j$. We know this because $\mathfrak{p}_i^e$ and $\mathfrak{p}_j^e$ are relatively prime, so generalizing the Euclidean Algorithm in $\mathcal{O}_K$ gives $a, b \in \mathcal{O}_K$ for which $a \cdot \mathfrak{p}_i^e + b \cdot \mathfrak{p}_j^e = (1)$. Thus, from the Chinese Remainder Theorem, we have

$$\mathcal{O}_K/(p) \cong \mathcal{O}_K/\mathfrak{p}_1^e \oplus \mathcal{O}_K/\mathfrak{p}_2^e \oplus \ldots \oplus \mathcal{O}_K/\mathfrak{p}_g^e.$$

Furthermore, $\mathcal{O}_K/(p)$ has p^n elements, since $\mathcal{O}_K/(p)$ is an extension of degree n of $\mathbb{Z}/p\mathbb{Z}$. Thus,

$$p^n = \underbrace{p^{ef} \cdot p^{ef} \cdots p^{ef}}_{g \text{ times}}.$$

So we have the fundamental equality, like we want:

$$n = efg. \square$$

Remark: This proof is based on its treatment in [7].

This equality is also a statement about the Galois group of K over $\mathbb{Q}$, so it simultaneously describes the number theoretical structure of the algebraic integers inside K and the Galois group's structure, as we will see.

3.2 Decomposition and Inertia Groups

As we mentioned above, the Galois group of $K|\mathbb{Q}$ acts on $\mathcal{O}_K$. Let $Z_\mathfrak{p} = \{\sigma \in G \mid \sigma\mathfrak{p} = \mathfrak{p}\}$, the subgroup that fixes $\mathfrak{p}$. We call this the *decomposition group*. We define the *decomposition field* of $\mathfrak{p}$ over $\mathbb{Q}$ to be the field fixed by $Z_\mathfrak{p}$. This group describes the number of ideals which lie over a prime (p) in $\mathcal{O}_K$. In particular, the index of the decomposition group lying inside the Galois group $(G : Z_\mathfrak{p}) = g$, where g is the number of prime ideals lying over (p) as above. Thus, if $(G : Z_\mathfrak{p}) = 1$, that is $Z_\mathfrak{p} = G$, then the prime p is still a prime ideal in O_K. We say then that p is *inert*. Similarly, if $(G : Z_\mathfrak{p}) = n$ (where $n = [K : \mathbb{Q}]$), that is $Z_\mathfrak{p} = 1$, then we say p is *totally split*, since (p) splits into the most possible prime ideals in O_K for the degree of the extension. Remember that $(G : Z_\mathfrak{p}) = g$, which implies that $|Z| = ef$.

Note also that the decomposition groups of the conjugates of $\mathfrak{p}$ are the conjugate subgroups of $Z_\mathfrak{p}$, in other words $Z_{\sigma\mathfrak{p}} = \sigma Z_\mathfrak{p} \sigma^{-1}$ for $\sigma \in G$, since, for all $\tau \in G$ we have the following:

$$\begin{aligned} \tau \in Z_{\sigma\mathfrak{p}} &\Rightarrow \tau\sigma\mathfrak{p} = \sigma\mathfrak{p} \\ &\Rightarrow \sigma^{-1}\tau\sigma\mathfrak{p} = \mathfrak{p} \\ &\Rightarrow \sigma^{-1}\tau\sigma \in Z_\mathfrak{p} \\ &\Rightarrow \tau \in \sigma Z_\mathfrak{p} \sigma^{-1}. \end{aligned}$$

Let $\kappa_\mathfrak{p} = \mathcal{O}_K/\mathfrak{p}$ and let $\mathbb{F}_p$ denote the finite field with p elements, $\mathbb{Z}/p\mathbb{Z}$. Now, consider the extension of the residue fields $\kappa_\mathfrak{p}|\mathbb{F}_p$.

Theorem 3.2.1: This residue extension is normal and there exists a surjective homomorphism,

$$Z_\mathfrak{p} \to \mathrm{Gal}(\kappa_\mathfrak{p}|\mathbb{F}_p).$$

Proof: Let $\theta \in \mathcal{O}_K$ be arbitrary, and let $\bar{\theta} \in \kappa_\mathfrak{p}$ be $\theta \mod \mathfrak{p}$. Let the minimal polynomial of θ over $\mathbb{Z}$ be f, and the minimal polynomial of $\bar{\theta}$ be $\bar{g} \in \mathbb{F}_p[x]$. Since K is a normal field extension, f splits into linear factors over $\mathcal{O}_K$, so $\bar{f} = f \mod \mathfrak{p}$ splits into linear factors over $\kappa_\mathfrak{p}$. Moreover, $\bar{f}(\bar{\theta}) = 0$, so $\bar{g} \mid \bar{f}$, which implies that $\bar{g}$ also splits into linear factors over $\kappa_\mathfrak{p}$. Thus, $\kappa_\mathfrak{p}|\mathbb{F}_p$ is a normal field extension.

Now, we clearly get a homomorphism from $Z \to \mathrm{Gal}(\kappa_\mathfrak{p}|\mathbb{F}_p)$. To show it is surjective, let $\bar{\sigma} \in \mathrm{Gal}(\kappa_\mathfrak{p}|\mathbb{F}_p)$. Then, $\bar{\sigma}(\bar{\theta})$ is a root of $\bar{g}$. Since $\bar{g}$ divides $\bar{f}$, $\bar{\sigma}(\bar{\theta})$ is also a root of $\bar{f}$. Thus, there is some θ' which is a root of f so that $\theta' = \bar{\sigma}(\bar{\theta}) \mod \mathfrak{p}$. Therefore, θ' is a root of the minimal polynomial of θ, so we know there is some $\sigma \in \mathrm{Gal}(K|\mathbb{Q})$ so that $\theta' = \sigma(\theta)$. Since $\sigma(\theta) = \bar{\sigma}(\bar{\theta})$, σ is mapped to $\bar{\sigma}$ by our homomorphism. Thus, the homomorphism is surjective. $\square$
Remark: This proof is based off its treatment in [11].

We have a surjective homomorphism, so we can consider its kernel. The kernel $T_\mathfrak{p} \leq Z_\mathfrak{p}$ is called the *inertia group* of $\mathfrak{p}$ over $\mathbb{Z}$. The fixed field $\mathrm{Fix}(T_\mathfrak{p})$ is called the *inertia field*, and is a normal extension of $\mathbb{Q}$. From above, $(Z : T) = f$, since the residue field extension is of degree f. Thus, we know

$$n = |\mathrm{Gal}(K|\mathbb{Q})| = (G : Z)(Z : T)|T| = gf|T|.$$

Thus $|T| = e$ from the fundamental equality, and the fundamental equality describes exactly the partitioning of the Galois group by the decomposition and inertia groups. Also note that another way to describe the inertia group is as the subgroup of Z (the group that fixes $\mathfrak{p}$) that fixes the residue field $\mathcal{O}_K/\mathfrak{p}$.

The inertia group has a chain of normal subgroups,

$$T = V_0 \trianglerighteq V_1 \trianglerighteq \ldots \trianglerighteq V_j \trianglerighteq \ldots,$$

where V_i is the kernel of taking $\sigma \in Z$ to its induced automorphism σ_i of $\mathcal{O}_K/\mathfrak{p}^{i+1}$. These V_i are called the *higher ramification groups* of $\mathfrak{p}$. Note that, for $j = 0$, the homomorphism $\sigma \mapsto \sigma_0$ induces an isomorphism of Z/T onto $\mathrm{Gal}(\kappa_\mathfrak{p}|\mathbb{F}_p)$ where $\sigma \mapsto \sigma|_{\kappa_\mathfrak{p}}$. In particular, Z/T is cyclic, since it is generated by the cosets of $\sigma \in \mathrm{Gal}(K|\mathbb{Q})$ so that

$$\sigma(x) \equiv x^p \mod \mathfrak{p}$$

for all $x \in \mathcal{O}_K$.

Theorem 3.2.2: The extension $\mathrm{Fix}(T)|\,\mathrm{Fix}(Z)$ is normal, with $\mathrm{Gal}(\mathrm{Fix}(T)|\,\mathrm{Fix}(Z)) \cong \mathrm{Gal}(\kappa_{\mathfrak{p}}|\mathbb{F}_p)$ and $\mathrm{Gal}(K|\,\mathrm{Fix}(T)) = T$. Let $\mathfrak{p} \cap \mathrm{Fix}(T) = \mathfrak{p}_T$ and $\mathfrak{p} \cap \mathrm{Fix}(Z) = \mathfrak{p}_Z$. Then, the ramification index of $\mathfrak{p}_T$ over $\mathfrak{p}_Z$ is e and the ramification index of $\mathfrak{p}_Z$ over p is 1. In other words, the ramification of p lies completely within the extension $\mathrm{Fix}(T) \supseteq \mathrm{Fix}(Z)$, even though there is a chain of fields $K \supseteq \mathrm{Fix}(T) \supseteq \mathrm{Fix}(Z) \supseteq \mathbb{Q}$.

Proof: The first claim we have already shown above, and the second follows from the first by the Galois correspondence. Now, if we show that $\mathcal{O}_K/\mathfrak{p}_T = \mathcal{O}_K/\mathfrak{p}$, then the fundamental identity gives us the other two statements. Note that T, the inertia group of $\mathfrak{p}$ over K, is also the inertia group of $\mathfrak{p}$ over $\mathrm{Fix}(T)$. Thus, we can apply our above theorem that gives us a surjective homomorphism from $Z \longmapsto \mathrm{Gal}(\kappa_{\mathfrak{p}}|\mathbb{F}_p)$ to the extension $K|\,\mathrm{Fix}(T)$. However, since the inertia group of this extension is T and the Galois group of this extension is T, the decomposition group must be the identity group, e. Thus, the only group that the decomposition group could have a surjective mapping onto is e, so $\mathrm{Gal}(\mathcal{O}_K/\mathfrak{p}|\mathcal{O}_K/\mathfrak{p}_T) = e$. Thus, $\mathcal{O}_K/\mathfrak{p} = \mathcal{O}_K/\mathfrak{p}_T$. Thus, $\mathfrak{p}_T$ is totally ramified over $\mathfrak{p}_Z$ and $\mathfrak{p}_Z$ is unramified over p. $\square$
Remark: This proof is based off its treatment in [11].

3.3 Ramification in Cyclotomic Extensions

In $\mathbb{Q}(\zeta_{p^r})$, p is the only ramified prime and p is totally ramified in $\mathbb{Z}[\zeta_{p^r}]$. More generally, for all $m > 2$, the ramified primes are the prime divisors of m, except for 2 when $4 \nmid m$. Furthermore, p is totally ramified in $\mathbb{Q}(\zeta_{p^r})$ except 2 in $\mathbb{Q}(\zeta_2)$. [7] We present the proof for $\mathbb{Q}(\zeta_p)$ where p is an odd prime, also based on its treatment in [7].

Theorem 3.3.1: Let $p \in \mathbb{Z}$ be prime. Then in $\mathbb{Q}(\zeta_p)$, p is totally ramified.
Proof: We will show that

$$p = \mathfrak{p}^e,$$

where $\mathfrak{p} = (1 - \zeta_p)$ and that $\mathfrak{p}$ is prime.

Recall that the minimal polynomial of ζ_p is

$$\Phi_p(x) = 1 + x + x^2 + \cdots + x^{p-1} = \prod_{i=1}^{p-1}(x - \zeta_p^i).$$

Then we have

$$\Phi_p(1) = \underbrace{1 + 1 + 1 + \cdots + 1}_{p \text{ times}} = p = \prod_{i=1}^{p-1}(1 - \zeta_p^i).$$

Let $u_i = \frac{1-\zeta_p^i}{1-\zeta_p} = 1 + \zeta_p + \zeta_p^2 + \cdots + \zeta_p^{i-1}$. First we will show that u_i has a multiplicative inverse and therefore show that u_i is a unit in $\mathbb{Z}[\zeta_p]$. Since $p \nmid i$, we know that there is some j so that $ij = 1 \mod p$. Thus,

$$u_i^{-1} = \frac{1-\zeta_p}{1-\zeta_{p^i}} = \frac{1-\zeta_p^{ij}}{1-\zeta_{p^i}} = 1 + \zeta_p^i + \zeta_p^{2i} + \cdots + \zeta_p^{(j-1)i},$$

which shows that $u_i^{-1} \in \mathbb{Z}[\zeta_p]$. Thus,

$$p = \prod_{i=1}^{p-1}(1-\zeta_p^i) = \prod_{i=1}^{p-1}(1-\zeta_p)(u_i) = (1-\zeta_p)^{p-1}\prod_{i=1}^{p-1} u_i.$$

Thus, $(p) = (1-\zeta_p)^{p-1} = \mathfrak{p}^{p-1}$. However, from the fundamental equality, we know that $[\mathbb{Q}(\zeta_p) : \mathbb{Q}] = n = efg = \phi(p) = p-1$, so we have that $\mathfrak{p}$ must be prime and $f = g = 1$. Thus, p is totally ramified in $\mathbb{Q}(\zeta_p)$. $\square$

3.4 Valuations

First note that for the rest of this paper, we will also be using the following theorem, due to Minkowski:
Minkowski's Theorem: For every finite extension K of $\mathbb{Q}$ of degree higher than 1, there exist primes that ramify in K and there are only finitely many ramified primes. For a proof of this theorem, see [9].

Let A be a ring with a unique non-zero prime ideal $m(A)$. Suppose further that A is a principal ideal domain, so that $m(A) = \pi A$ for some $\pi \in m(A)$. Such a ring is called a *discrete valuation ring*. Then, we define a function $v : A \to \mathbb{N}$ where $v(x) = n$ if $x = \pi^n u$ for u invertible. This is very similar to the p-adic norm on the rationals where v measures the 'π-ness' of x. The function v is called a *valuation* of A.

We can turn any Dedekind domain into a discrete valuation ring through localization. First, in $\mathbb{Z}$, let $(p) \subseteq \mathbb{Z}$ be a prime ideal. We define

$$\mathbb{Z}_{(p)} := \Big\{ \frac{n}{m} \mid n, m \in \mathbb{Z}, gcd(m,p) = 1 \Big\}.$$

Note that this creates a ring as above, where (p) is the only non-zero prime ideal. This is called a *local ring* and the process of forming $\mathbb{Z}_{(p)}$ is called *localization* at p.

More generally, suppose we have $\mathfrak{p} \subseteq \mathcal{O}_K$, where $\mathcal{O}_K$ is as before. Then we define

$$\mathcal{O}_{K\mathfrak{p}} := \Big\{ \frac{r}{s} \mid r, s \in \mathcal{O}_K, s \notin \mathfrak{p} \Big\}.$$

This ring is a discrete valuation ring, with $\mathfrak{p}$ as the only non-zero prime ideal.

Now, suppose we have $K|\mathbb{Q}$ a normal field extension, and let $\mathbb{Z}_{(p)}$ and $\mathcal{O}_{K\mathfrak{p}}$ be as above, with valuation v. Let $x \in \mathcal{O}_{K\mathfrak{p}}$ be such that $\mathcal{O}_{K\mathfrak{p}} = \mathbb{Z}_{(p)}[x]$.

Theorem 3.4.1: Let $\sigma \in \mathrm{Gal}(K|\mathbb{Q})$ and let i be an integer greater than or equal to -1. Then the following are equivalent:

1. σ operates trivially on the quotient ring $\mathcal{O}_{K\mathfrak{p}}/\mathfrak{p}^{i+1}$.
2. $v(\sigma(a) - a) \geq i + 1$ for all $a \in \mathcal{O}_{K\mathfrak{p}}$.
3. $v(\sigma(x) - x) \geq i + 1$.

Proof: First we will show (1) and (2) are equivalent. First, suppose that σ operates trivially on the quotient ring. For $a \in \mathcal{O}_{K\mathfrak{p}}$, $\sigma(a) = k\mathfrak{p}^{i+1} + a$ for some $k \in \mathcal{O}_{K\mathfrak{p}}$. Thus,

$$v(\sigma(a) - a) = v(k\mathfrak{p}^{i+1}) \geq i + 1,$$

with equality so long as $\mathfrak{p}^{i+1}$ does not divide a.

If $v(\sigma(a) - a) \geq i + 1$, then $\sigma(a) - a = \mathfrak{p}^{i+1}c$ for some $c \in \mathcal{O}_{K\mathfrak{p}}$, by the definition of our valuation. Thus,

$$\sigma(a) = c\mathfrak{p}^{i+1} + a$$

which reduces to $\sigma(a) \equiv a \mod \mathfrak{p}^{i+1}$. Thus, σ operates trivially on our quotient ring.

Now, we will show that (1) and (3) are equivalent and thus complete the proof. Let $\bar{x}$ be the image of x in $\mathcal{O}_{K\mathfrak{p}}/\mathfrak{p}^{i+1}$. Then, $\mathbb{Z}/p\mathbb{Z}[\bar{x}] = \mathcal{O}_{K\mathfrak{p}}/\mathfrak{p}^{i+1}$, so σ operates trivially on this quotient exactly when $\sigma(\bar{x}) = \bar{x}$. By the definition of our valuation, this happens exactly when $v(\sigma(x) - x) \geq i + 1$, which gives our equivalence. $\square$

Let G_i be the subgroup of $\mathrm{Gal}(K|\mathbb{Q})$ that satisfies the three conditions in the above theorem. Note that G_i is in fact V_i, the ith ramification group.

Theorem 3.4.2: The V_i form a decreasing sequence of normal subgroups of $V_{-1} = \mathrm{Gal}(K|\mathbb{Q})$ and V_i is trivial for i sufficiently large. Note also that by definition $G_0 = T = V_0$, the inertia group of $\mathfrak{p}$.

Proof: We have shown above that the V_i are a decreasing sequence of normal subgroups. Now, suppose that $i \geq \max\{v(\sigma(x) - x)\}$ for σ not the identity. This maximum exists, because $\mathrm{Gal}(K|\mathbb{Q})$ is finite, so our set of values is a finite subset of $\mathbb{N}$. Then, from (3) above, V_i must be trivial. $\square$

Recall that $\mathcal{O}_{K\mathfrak{p}}$ is the localized ring where $\mathfrak{p}$ lies above a ramified prime p in $K|\mathbb{Q}$. Furthermore, because $\mathcal{O}_{K\mathfrak{p}}$ is localized, $\mathfrak{p}$ is the only prime ideal in $\mathcal{O}_{K\mathfrak{p}}$. From before, $\mathcal{O}_{K\mathfrak{p}}$

is also a principal ideal domain, so let π be a generator of $\mathfrak{p}$. Note that $\mathbb{Z}_{(p)}[\pi] = \mathcal{O}_{K\mathfrak{p}}$, so π is an x in the above theorem. In particular, $v(\sigma(\pi) - \pi)$ determines fully which higher ramification groups σ is in.

Theorem 3.4.3: For $\sigma \in T = G_0$ to be in V_i for i non-negative,

$$\frac{\sigma(\pi)}{\pi} \equiv 1 \mod \mathfrak{p}^i.$$

Proof: Suppose $\sigma \in V_i$. Then, we know that $v(\sigma(\pi) - \pi) \geq i + 1$. Furthermore, $v(\pi) = 1$, so

$$i + 1 \leq v(\sigma(\pi) - \pi) = 1 + v\Big(\frac{\sigma(\pi)}{\pi} - 1\Big).$$

Then,

$$v\Big(\frac{\sigma(\pi)}{\pi} - 1\Big) \geq i,$$

which implies that

$$\frac{\sigma(\pi)}{\pi} \equiv 1 \mod \mathfrak{p}^i. \square$$

Now we define $\mathcal{U}^{(i)} := 1 + \mathfrak{p}^i$. Note that $\mathcal{U}^{(0)} \supseteq \mathcal{U}^{(1)} \supseteq \mathcal{U}^{(2)} \supseteq \ldots \supseteq \mathcal{U}^{(i)} \supseteq \ldots$, and that $\mathcal{U}^{(0)}$ is $\mathcal{O}_{K\mathfrak{p}} \setminus \mathfrak{p}$, the multiplicative group of invertible elements in $\mathcal{O}_{K\mathfrak{p}}$. Furthermore, each $\mathcal{U}^{(i)}$ is in fact a subgroup of $\mathcal{U}^{(0)}$, and since $\mathcal{U}^{(0)}$ is abelian, this is a chain of normal subgroups. Since $\mathcal{O}_{K\mathfrak{p}} = \mathbb{Z}_p[\pi]$, we know that $\mathcal{U}^{(0)}/\mathcal{U}^{(1)} \cong (\mathcal{O}_K/\mathfrak{p})^*$, the multiplicative group of the residue field.

Theorem 3.4.4: For each $i \geq 1$, the group $\mathcal{U}^{(i)}/\mathcal{U}^{(i+1)}$ is isomorphic to $\mathfrak{p}^i/\mathfrak{p}^{i+1}$, which is isomorphic to the additive group of $\mathcal{O}_K/\mathfrak{p}$.
Proof: Let each $x \in \mathfrak{p}^i$ correspond to $1 + x \in \mathcal{U}^{(i)}$, and similarly for $i + 1$. Then, this correspondence is clearly an isomorphism of the quotient groups. Now, since $\mathfrak{p}^i/\mathfrak{p}^{i+1}$ is a one-dimensional vector space over $\mathcal{O}_K/\mathfrak{p}$, this gives that $\mathfrak{p}^i/\mathfrak{p}^{i+1} \cong (\mathcal{O}_K/\mathfrak{p}, +)$.

Now, we know that $\sigma \in V_i$ if and only if $\frac{\sigma(\pi)}{\pi} \equiv 1 \mod \mathfrak{p}^i$, which implies that $\frac{\sigma(\pi)}{\pi} \in \mathcal{U}^{(i)}$. Thus, $V_i \leq U^{(i)}$ for all i. This gives us that V_i/V_{i+1} is isomorphic to a subgroup of $(\mathcal{O}_K/\mathfrak{p}, +)$. Note that since this field has characteristic p, this means that V_i/V_{i+1} is either a direct product of cyclic groups of order p or is trivial. Furthermore, T/V_1 is isomorphic to a subgroup of $(\mathcal{O}_K/\mathfrak{p})^*$. Thus the higher ramification groups form a chain of normal subgroups where each adjacent quotient is abelian of order some p-power. $\square$
Remark: All the proofs in this section are based off their treatments in [13].

We can extend this last fact to show that in fact T/V_1 is cyclic of order dividing $p - 1$ if Z/V_1 is abelian. For proof, see [3].

4 Proof of the Kronecker-Weber Theorem

Theorem (Kronecker-Weber): Every abelian extension of $\mathbb{Q}$ is cyclotomic.

The outline of this proof is due to Greenberg [3], based off of original proofs by Kronecker, Weber, and Hilbert as mentioned above. We will first simplify the theorem by showing that if the theorem holds for cyclic extensions of prime-power order with a single ramified prime, then it holds in the general case with the following lemmas.

Lemma 1: If the theorem holds for extensions of prime-power order, it holds for all abelian extensions.

Proof: Let $K|\mathbb{Q}$ be a normal abelian extension. Then, from the fundamental theorem of abelian groups, we can decompose $\mathrm{Gal}(K|\mathbb{Q})$ into the direct product of cyclic groups G_i of prime-power order:

$$\mathrm{Gal}(K|\mathbb{Q}) = G_1 \times G_2 \times \dots G_n.$$

Then, let $K_i = \mathrm{Fix}(G_i)$. Since $\mathrm{Gal}(K|\mathbb{Q})$ is abelian, $G_i \trianglelefteq \mathrm{Gal}(K|\mathbb{Q})$ so K_i is a normal field extension of $\mathbb{Q}$. Furthermore, $\mathrm{Gal}(K_i|\mathbb{Q}) \cong G_i$, so is an extension of prime-power order. By the way we constructed the K_i's, K is the field compositum of them. Thus, if each K_i is cyclotomic, it follows that K is cyclotomic (see theorem 2.7.1). $\square$

Thus, if the theorem holds for fields of prime-power order, it holds in general. Now we will use ramification to simplify further.

Lemma 2: Let $K|\mathbb{Q}$ be an abelian extension of order q^m for prime q. Then, it suffices to show the theorem when q is the only ramified prime in K.

Proof: We will prove this by constructing a field K' in which q is the only ramified prime, but which has the property that if K' is cyclotomic, K also is.

First suppose we have some prime $p \neq q$ that is ramified in K. Let $\mathfrak{p}$ be a prime ideal of $\mathcal{O}_K$ that lies over p. Then, since $\mathrm{Gal}(K|\mathbb{Q})$ is of order q^m, p does not divide the order of any subgroup of the Galois group. This means that all higher ramification groups V_j of $\mathfrak{p}$ are trivial (section 3.4). The order of T is a power of q, say q^u, so

$$p - 1 \equiv 0 \mod q^u,$$

from Lemma 1. Recall that $\mathrm{Gal}(\mathbb{Q}(\zeta_p)|\mathbb{Q})$ is cyclic of degree $p-1$. Since it is cyclic, it has a unique subgroup that has index q^u (the cyclic subgroup of order $\frac{p-1}{q^u}$), which corresponds to a unique subfield L which is cyclic of order q^u over $\mathbb{Q}$. From section 3.3, we know p is totally ramified in $\mathbb{Q}(\zeta_p)$ and no other primes are. Thus, in L, p is totally ramified and no other primes are.

Now look at the field compositum KL. We know this field has degree some q-power between m and $m+u$. Let $\mathfrak{p}'$ be a prime ideal of $\mathcal{O}_{KL}$ that lies over $\mathfrak{p}$ and T' the inertia group of $\mathfrak{p}'$ over p. Note that T' acts on K, and restriction to K maps T' into T, so we know that

$$T' \leq T \times \mathrm{Gal}(L|\mathbb{Q}) \leq \mathrm{Gal}(K|\mathbb{Q}) \times \mathrm{Gal}(L|\mathbb{Q}).$$

Note that $|T'| \geq q^u$, since the ramification of $\mathfrak{p}'$ over p must be at least as big as the ramification of $\mathfrak{p}$ over p. The higher ramification groups are still trivial, for the same reason as before, so T' is cyclic.

Now, no element of $T \times \mathrm{Gal}(L|\mathbb{Q})$ has order higher than q^u, so T' cyclic implies $|T'| \leq q^u$. However, T' has order at least q^u, thus it must have order q^u. Consider $K' = \mathrm{Fix}(T')$. Let $\mathfrak{P} = \mathfrak{p}' \cap K'$. From section 3.2, $\mathfrak{P}$ is unramified over p. Also, $K' \cap L = \mathbb{Q}$, because $\mathfrak{P} \cap L$ must be both unramified and totally ramified over p.

Furthermore, $[KL : K'] = q^u = [L : \mathbb{Q}]$ from above, so

$$[K'L : \mathbb{Q}] = [KL : K'][K' : \mathbb{Q}] = [L : \mathbb{Q}][K' : \mathbb{Q}] = [KL : \mathbb{Q}]$$

so $K'L = KL$. Thus, since L is cyclotomic, if K' is cyclotomic, $K'L = KL$ is cyclotomic, which implies K is. Note that p no longer ramifies in K', and no new primes ramify in K', since any such prime would be ramified in KL.

Since only finitely many primes ramify (Minkowski), we can repeat this process for all $p \neq q$ that ramifies in K until we are left with a field K' where q is the only ramified prime, but $K'L = KL$. $\square$

This lemma has the following useful corollaries:
Corollary 1: Let $K|\mathbb{Q}$ be abelian with order q^m and suppose $p \neq q$ is the only ramified prime in K. Then p is totally ramified in K, $p \equiv 1 \mod q^m$, and K is the unique subfield of $\mathbb{Q}(\zeta_p)$ of degree q^m. Therefore $K|\mathbb{Q}$ is cyclic.

Proof: From our argument above, the field K' is unramified over $\mathbb{Q}$. Thus, from Minkowski, $K' = \mathbb{Q}$ which implies that $K = L$. $\square$

Corollary 2: If $K|\mathbb{Q}$ is abelian of odd degree, 2 is unramified in K.

Proof: Let $\mathfrak{p}$ lie over (2). We know the higher ramification groups, particularly V_1, are trivial from our argument above. However, T is also trivial, because it must be cyclic of order dividing $2-1=1$. Thus, the ramification index of (2) is 1, so 2 is unramified in K. $\square$

We have successfully reduced our theorem now to the case of abelian extensions of degree q^m where q is prime. As the previous corollary suggests, we must consider two separate cases: where $q = 2$ or when q is odd, because the information encoded in the inertia group is fundamentally different when $q = 2$. We will first consider the odd case.

Case 1: Let $K|\mathbb{Q}$ be abelian of degree q^m for q an odd prime, in which q is the only ramified prime (the reduction of our general case above). Then $K|\mathbb{Q}$ is cyclotomic.

Proof: First we will show that $K|\mathbb{Q}$ is cyclic. Let T be the inertia group of $\mathfrak{q}$, a prime lying over q. We know that q is unramified in $\mathrm{Fix}(T)$, so by Minkowski, since at least one prime must ramify in any extension, we have $\mathrm{Fix}(T) = \mathbb{Q}$, so $T = \mathrm{Gal}(K|\mathbb{Q})$, and thus q is totally ramified in K. Thus, from the fundamental equality, $(q) = \mathfrak{q}^n \in \mathcal{O}_K$ and the degree of the residue field extension is 1, so $\mathcal{O}_K/\mathfrak{q} = \mathbb{Z}/q\mathbb{Z}$. However T/V_1 must have order dividing $q-1$. However, no power of q divides $q-1$, so $V_1 = T$. Thus, every adjacent quotient V_j/V_{j+1} is either trivial or cyclic of order q.

To show that T is cyclic, we will show that there is a unique subgroup of index q in T. First suppose that $m = 1$, i.e. that $[K : \mathbb{Q}] = q$. We will show that V_2 is this subgroup, and is trivial in this case.

Localize, so that the prime ideal $\mathfrak{q}$ is principal, generated by π. Let $f(x)$ be the minimal polynomial of π over $\mathbb{Q}$, and let v be the valuation associated to π of K. Let V_{j+1} be the first trivial ramification group. Then $V_j = \mathrm{Gal}(K|\mathbb{Q})$. Then (from [3]),

$$f'(\pi) = \prod_{\sigma \neq e} (\pi - \sigma(\pi)).$$

This implies that

$$v(f'(\pi)) = (j+1)(q-1),$$

because $v(\pi - \sigma(\pi)) = j+1$ from before, and there are $q-1$ different σ's.

However, from calculus,

$$f'(\pi) = q\pi^{q-1} + a_{q-1}(q-1)\pi^{q-2} + \ldots + a_1$$

for a_i integers. Since q is totally ramified in K, $v(q) = q$, so

$$v(a_i) \equiv 0 \mod q.$$

Thus,

$$v_i := v(a_{q-i+1}(q-i+1)\pi^{q-i}) \equiv q - i \mod q.$$

By definition, $v(f'(\pi))$ is the minimum of the v_i's. Thus,

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

Therefore, $2q - 1 \geq (j+1)(q-1)$. However, since $q > 2$, the only j which satisfies this inequality is 1. Thus, V_2 is trivial.

For the case where $m > 1$, let i be the smallest index for which $V_i \neq \mathrm{Gal}(K|\mathbb{Q})$. Then, V_i is the unique subgroup of $\mathrm{Gal}(K|\mathbb{Q}) = V_1$ that has index q. See [16] for the proof.

Now, we still need to show that $K|\mathbb{Q}$ is cyclotomic. Recall that q is the only ramified prime in K, and that $[K:\mathbb{Q}] = q^m$. Consider the extension $\mathbb{Q}(\zeta_{q^{m+1}})$. Recall that this field is cyclic of order $q^m(q-1)$ from above and that q is the only ramified prime in this extension. Let K' be the unique subfield of this extension of order q^m. We will show that $K = K'$.

We know that q is the only ramified prime in KK' since q is the only ramified prime in both K and K'. Furthermore KK' is abelian. We showed above that in fact $KK'|\mathbb{Q}$ is cyclic. However, since KK' is a field compositum, its Galois group is a subgroup of $\mathrm{Gal}(K|\mathbb{Q}) \times \mathrm{Gal}(K'|\mathbb{Q})$. Thus, no element of $Gal(KK'|\mathbb{Q})$ can have order greater than q^m. But since this group is cyclic, $|Gal(KK'|\mathbb{Q})| \leq q^m$ which gives

$$[KK' : \mathbb{Q}] = [K : \mathbb{Q}] = [K' : \mathbb{Q}] = q^m.$$

Thus $K = K'$. $\square$

Note that this proof actually demonstrates that if K is an abelian extension of $\mathbb{Q}$ of degree q^m for q an odd prime in which q is the only ramified prime, then K is in fact the unique subfield of $\mathbb{Q}(\zeta_{m+1})$ of degree q^m.

Case 2: Let $K|\mathbb{Q}$ be an abelian extension of order 2^m. Then $K|\mathbb{Q}$ is cyclotomic.

Proof: First, we will consider the case where $m = 1$, that is, where K is a quadratic extension of $\mathbb{Q}$. Note that all quadratic extensions are abelian, since $\mathbb{Z}/2\mathbb{Z}$ is the only group of order 2. Since any quadratic extension $K = \mathbb{Q}(\sqrt{n})$ for some $n \in \mathbb{Q}$, we can reduce this to the case where $K = \mathbb{Q}(\sqrt{\pm p})$ for p prime. For $p = 2$, K is contained in $\mathbb{Q}(\zeta_8)$, since

$$(1+i)^2 = 2i.$$

Now, suppose that p is odd. Then, either p or $-p$ is a square in $\mathbb{Q}(\zeta_p)$. The main idea of this proof is to use quadratic reciprocity by finding the sum of $\left(\frac{a}{p}\right)\zeta_p^a$, where the values of a are the residue classes mod p and can be found in [7]. This implies that

$$\sqrt{\pm p} \in \mathbb{Q}(\zeta_p)(i).$$

Note also that $i = \zeta_4$. Thus,

$$\sqrt{\pm p} \in \mathbb{Q}(\zeta_p, \zeta_4) \subseteq \mathbb{Q}(\zeta_{4p}).$$

Thus every quadratic extension is cyclotomic.

We will procede by induction on m to show that every extension of degree 2^m is cyclotomic. From Lemma 2, we can assume that 2 is the only ramified prime in K. Note also that $K \subseteq \mathbb{C}$ and that $K/\mathbb{Q}$ is cyclic from Corollary 1 above. Since complex conjugation is an automorphism of order 2,

$$[K \cap \mathbb{R} : \mathbb{Q}] \geq 2^{m-1}.$$

Thus, the unique subfield of K that is quadratic must be real. Since 2 is the only ramified prime, this subfield must be $\mathbb{Q}[\sqrt{2}]$, since 2 must factor in K, and no other prime can.

Now consider $\mathbb{Q}(\zeta_{2^{m+2}})$. We know the subfield

$$L = \mathbb{Q}(\zeta_{2^{m+2}} + \zeta_{2^{m+2}}^{-1})$$

is cyclic of degree 2^{m+1} over $\mathbb{Q}$ and 2 is the only ramified prime from section 3.3. Thus, the unique quadratic subextension here is also $\mathbb{Q}(\sqrt{2})$. Thus

$$K \cap L \supseteq \mathbb{Q}(\sqrt{2}) \supset \mathbb{Q}.$$

This implies that $[KL : \mathbb{Q}] < 2^{2m}$. Furthermore,

$$\mathrm{Gal}(KL|\mathbb{Q}) < \mathrm{Gal}(K|\mathbb{Q}) \times \mathrm{Gal}(L|\mathbb{Q}).$$

Let σ and τ be generators of $\mathrm{Gal}(K|\mathbb{Q})$ and $\mathrm{Gal}(L|\mathbb{Q})$ so that σ and τ agree on $K \cap L$. Since they agree on $K \cap L$, $(\sigma, \tau) \in \mathrm{Gal}(KL|\mathbb{Q})$, so (σ, τ) generates a subgroup, G' of $\mathrm{Gal}(KL|\mathbb{Q})$ of order 2^m. Then $F = \mathrm{Fix}(G') \subseteq KL$ has degree 2^r for some $r < m$ and 2 is still the only ramified prime in F. Thus, from our inductive hypothesis, F is cyclotomic.

Now notice that $FL \subseteq KL$, since $F, L \subseteq KL$. Now let $\varphi \in \mathrm{Gal}(KL|\mathbb{Q})$ be an automorphism that fixes FL. Then we know that φ fixes both F and L, so in particular $\varphi \in G'$. However, $G' = \langle(\sigma, \tau)\rangle$, so this means that $\varphi = (\sigma, \tau)^i = (\sigma^i, \tau^i)$ for some i. However, φ also fixes L, so τ^i must be the identity in $\mathrm{Gal}(L|\mathbb{Q})$. However, σ and τ have the same order, so σ^i must also be the identity. Thus, the only automorphism of KL that fixes FL is the identity, so $KL \subseteq FL$. Thus $KL = FL$. Recall that both F and L are cyclotomic fields. Thus, K is cyclotomic. $\square$

This completes the proof of the Kronecker-Weber Theorem.

5 Conclusion

This proof of the Kronecker-Weber Theorem demonstrates the many different branches of mathematics the theorem relates to: it draws from group theory, number theory, elementary calculus, and geometric intuition. Thus, even the proof reflects the strength this theorem has to connect several different branches of mathematics together.

It should also be noted that once this theorem is established, it is relatively easy to show that in fact all finite abelian groups exist as Galois groups over $\mathbb{Q}$. The Kronecker-Weber Theorem shows that proving this only takes an exploration of cyclotomic fields and their Galois groups, which are a class of fields that are relatively concrete and easy to understand. In fact, since we know that $\mathrm{Gal}(\mathbb{Q}(\zeta_n)|\mathbb{Q}) = (\mathbb{Z}/n\mathbb{Z})^*$, all that we need to show that a given abelian group A is a Galois group over $\mathbb{Q}$ is:

1. There exists some n for which $A \leq (\mathbb{Z}/n\mathbb{Z})^*$ and

2. For $H \leq G$ for H and G abelian, there is some $K \leq G$ for which $G/K = H$.

Letting $H = A$, the Galois correspondence gives some normal subfield of $\mathbb{Q}(\zeta_n)$ whose Galois group is A, thus showing that all abelian groups are Galois groups over $\mathbb{Q}$. The proof of these facts may be found in [10]. Note that this strategy does not directly use the Kronecker-Weber Theorem but is informed by the result of the proof, since it only considers cyclotomic fields. Another argument, using algebraic geometry instead of number theory, may be found in [14], again demonstrating this theorem's connection to different branches of modern mathematics.

6 Acknowledgments

I thank my advisor, Professor Scott Corry, for his guidance and support throughout this project and for teaching the class that originally inspired this work. Also I thank Angela Vanden Elzen for her technological support and reference assistance.

References

[1] Julio R. Bastida. *Field Extensions and Galois Theory*, volume 22 of *Encyclopedia of Mathematics and its Applications*. Addison-Wesley, 1984.

[2] Richard Dedekind. *Theory of Algebraic Integers*. Cambridge University Press, 1996. Translated by John Stillwell.

[3] M. J. Greenberg. An Elementary Proof of the Kronecker-Weber Theorem. *The American Mathematical Monthly*, 81(6):601–607, Jun-Jul 1974.

[4] M.J. Greenberg. Correction to "An Elementary Proof of the Kronecker-Weber Theorem". *The American Mathematical Monthly*, 82(8):803, Oct 1975.

[5] Michiel Hazewinkel, editor. *Galois Theory*. Encyclopedia of Mathematics. Springer Verlag, 2001.

[6] David Hilbert. Ein neuer Beweis des Kronecker'schen Fundementalsatzes über Abel'sche Zahlkörper. *Nachrichten der Gesellschaft der Wissenschaften zu Göttingen*, pages 29 – 39, 1896.

[7] Kenneth Ireland and Michael Rosen. *A Classical Introduction to Modern Number Theory*. Springer-Verlag New York, Inc., 1986.

[8] Leopold Kronecker. Über die algebraisch auflösbaren Gleichungen. *Berlin Akadamie der Wissenschaft*, pages 365 – 374, 1853.

[9] Serge Lang. *Algebraic Number Theory*, pages 3–56, 71–97. Springer-Verlag New York, Inc., second edition, 1994.

[10] Serge Lang. *Algebra*. Springer-Verlag New York, Inc., third edition, 2002.

[11] Jürgen Neukirch. *Algebraic Number Theory*. Springer-Verlag Berlin Heidelberg, 1999. Translated by Norbert Schappacher.

[12] Charles C. Pinter. *A Book of Abstract Algebra*. Dover Publications, Inc., second edition, 1990.

[13] Jean-Pierre Serre. *Local Fields*, pages 5–15. Springer-Verlag New York, Inc., 1979. Translated by Marvin Jay Greenberg.

[14] Jean-Pierre Serre. *Topics in Galois Theory*. Research Notes in Mathematics. Jones and Bartlett Publishers, 1992. Notes written by Henri Damon.

[15] John Stillwell. *Elements of Number Theory*. Springer-Verlag New York, 2003.

[16] Anthony Várilly. The Kronecker-Weber Theorem, Fall 2001. Harvard University. http://exordio.qfb.umich.mx/archivos/20pdf/20de/20trabajo/20umsnh/aphilosofia/2007/grupos/KroneckerW.pdf.

[17] H. Weber. Theorie der Abel'schen Zahlkörper. *Acta Mathematica*, 8:193–263, 1886.