Topics in Inverse Galois Theory

Andrew Johan Wills

Thesis submitted to the Faculty of the
Virginia Polytechnic Institute and State University
in partial fulfillment of the requirements for the degree of

Master of Science
in
Mathematics

Ezra Brown, Chair
Nicholas Loehr
William Floyd

April 19, 2011
Blacksburg, Virginia

Keywords: Inverse Galois Theory, Rigid Groups, Kronecker-Weber Theorem

Topics in Inverse Galois Theory

Andrew Johan Wills

Abstract

Galois theory, the study of the structure and symmetry of a polynomial or associated field extension, is a standard tool for showing the insolvability of a quintic equation by radicals. On the other hand, the Inverse Galois Problem, given a finite group G, find a finite extension of the rational field $\mathbb{Q}$ whose Galois group is G, is still an open problem. We give an introduction to the Inverse Galois Problem and compare some radically different approaches to finding an extension of $\mathbb{Q}$ that gives a desired Galois group. In particular, a proof of the Kronecker-Weber theorem, that any finite extension of $\mathbb{Q}$ with an abelian Galois group is contained in a cyclotomic extension, will be discussed using an approach relying on the study of ramified prime ideals. In contrast, a different method will be explored that defines rigid groups to be groups where a selection of conjugacy classes satisfies a series of specific properties. Under the right conditions, such a group is also guaranteed to be the Galois group of an extension of $\mathbb{Q}$.

Acknowledgments

I would like to express my sincere appreciation to my advisor and thesis committee chair Dr. Ezra Brown. This thesis would not have been possible without his advice, his perspective, and our bi-weekly meetings.

I would also like to thank Dr. Nicholas Loehr and Dr. William Floyd for serving on my thesis committee. They have been both encouraging and supportive throughout. In particular, they provided invaluable assistance and insight to the editing process.

Finally, I would like to thank my colleagues, like Matt, Dave, Kelli, and my research companions Jim and Maria, for undergoing with me the same exciting struggle to write a thesis. And for those few breaks from academics, any acknowledgements would be incomplete without heartfelt gratitude to my family and girlfriend Sarah.

Contents

0.1 Introduction 1

1 Finding a Galois Group **3**

1.1 Background Information: What is a Galois Group? 3

1.1.1 Example: The extension $\mathbb{Q}(\zeta_n)/\mathbb{Q}$, where ζ_n is a primitive nth root of unity over $\mathbb{Q}$, is of degree $\varphi(n)$ where φ is Euler's phi-function. 5

1.1.2 Algebraic Field Elements 8

1.1.3 The Galois Group 10

1.2 Additional Theorems for Galois Groups 12

2 The Inverse Galois Problem **16**

2.1 Introduction and General Results 16

2.2 Results over $\mathbb{Q}$ 17

2.3 Rigid Groups 19

2.4 An Example with S_4 24

2.5 Proof for S_n 26

3 The Kronecker-Weber Theorem **28**

3.1 Background 28

3.1.1 Finite Fields 29

3.1.2 Algebraic Integers 31

3.1.3 Dedekind Domains, Extensions of Dedekind Domains 34

3.2 Ramification Theory of Ideals 36

3.2.1 Extended and Contracted Ideals 36

3.2.2 Decomposition of Prime Ideals in Extensions of Dedekind Domains: Introduction to Ramification 38

3.2.3 Decomposition Group, Ramification Group, and Inertia Group 41

3.3 Greenberg's Proof of The Kronecker-Weber Theorem 54
3.3.1 Application of Background Information to Kronecker-Weber Theorem Setup: 54
3.3.2 Proof Proper: 59

List of Figures

1.1.1 A Field Extension 3

3.2.1 Commutative Diagram 38
3.3.1 Proof Setup 55
3.3.2 Decomposition and Inertia Groups 56
3.3.3 Prime Factorization of (p) 57
3.3.4 Lemma 3 Setup 65

List of Tables

2.1 Conjugacy Classes of S_4 24

0.1 Introduction

The focus of this work is the so-called Inverse Galois Problem: given a finite group G, find a finite Galois extension of the rational field $\mathbb{Q}$ whose Galois group is G. Galois groups were first explored by their namesake Evariste Galois in the early 1800s to determine conditions for when a polynomial is solvable by radicals. Galois theory is, informally, the study of the group formed from the permutations of a field that are characterized by their effect on the roots of a polynomial associated with the field. More formally, given fields K and F with F contained in K, the group of automorphisms of K that fix every element of F is denoted $\mathrm{Aut}(K/F)$ and the dimension of K as a vector space over F is denoted $[K:F]$. We say K is Galois over F and K/F is a Galois extension if $|\mathrm{Aut}(K/F)| = [K:F]$, or equivalently, when K is a normal, separable extension of F. If K/F is Galois, $\mathrm{Aut}(K/F)$ is called the Galois group of K/F, written $\mathrm{Gal}(K/F)$. Furthermore, if $f(x)$ is a separable polynomial over F, then the Galois group of $f(x)$ over F is the Galois group of a splitting field of $f(x)$ over F.

Galois theory has a number of applications, from differential equations to coding theory, many of which demonstrate the ability to examine the action of one object on another to gain information about the structure of both. The Fundamental Theorem of Galois Theory exemplifies this theme by defining an inclusion-reversing bijection between subfields of K that contain the field F and subgroups of the Galois group. Using this correspondence, we convert questions about fields to questions about groups which are simpler structures. For example, we can use the statement that a polynomial is solvable by radicals if and only if its Galois group is solvable to show that the roots of a polynomial of degree five or greater cannot, in general, be formed by radicals. By showing that S_n ($n \geq 5$) is not solvable and showing that for every $n \geq 5$ there exists a polynomial of degree $n \geq 5$ over $\mathbb{Q}$ with Galois group isomorphic to S_n, we show that there always exists a polynomial whose roots cannot be expressed by radicals.

In the example above, we desired a specific group to be the Galois group of a field extension of $\mathbb{Q}$. We call this search for a field extension of $\mathbb{Q}$ that gives a desired group as the Galois group the Inverse Galois Problem. In general, it is relatively simple to find a field and an extension that give a desired Galois group but finding an extension of a *specific* field, like $\mathbb{Q}$, that gives a desired Galois group is significantly more complicated.

We not only introduce the Inverse Galois Problem in a comprehensible manner, but also compare a few different approaches to finding an extension of $\mathbb{Q}$ that gives a desired Galois group. We characterize one of these methods by elucidating a proof by M. J. Greenberg of the Kronecker-Weber Theorem, that any finite extension of $\mathbb{Q}$ with an abelian Galois group can be expressed as

a subextension of a cyclotomic extension of $\mathbb{Q}$, by using results from classical algebra instead of class field theory. In particular, we look at the ramified and unramified primes in a cyclotomic extension of the rationals. We also demonstrate another method by defining a rigid group as a group that has specific requirements on its conjugacy classes, in particular that it have a rigid class vector. Despite using very different techniques to solve similar problems, both approaches have similarities. For example, both rigidity and the results from classical algebra depend on transitivity of certain elements of the Galois group and ideals in the extension field.

In Part 1, we give a brief introduction to Galois theory with emphasis on examples of cyclotomic extensions. In Part 2, we state the Inverse Galois Problem and give a series of partial results. We also define rigid groups and use the definition to prove one of the above results. Finally, Part 3 is devoted to giving a proof of the Kronecker-Weber Theorem, one of the theorems given in Part 2.

Chapter 1

Finding a Galois Group

1.1 Background Information: What is a Galois Group?

The following definitions are standard and can be found in [1].

Definition 1. Given a field K containing a subfield F, we say K is an *extension field* (or *extension*) of F, denoted K/F and said "K over F".

Here, K/F does not refer to the creation of a quotient of K by F but rather describes K's relationship with F as a field extension of F.

Definition 2. The *degree* of a field extension K/F is the dimension of K as a vector space over F, $\dim_F K$, and is denoted $[K:F]$. If $[K:F] < \infty$, we say the field extension is *finite*. Otherwise, the field extension is said to be *infinite*.

Alternatively, instead of considering $[K:F]$ as the dimension of K as an F-vector space, $[K:F]$ can be defined to be the dimension of K as an F-module. Visually, we can represent K/F in Figure 1.1.1, where $n = [K:F]$.

Definition 3. If K is an extension of F and $f(x) \in F[x]$, $f(x)$ is said to *split completely* over a field

Figure 1.1.1: A Field Extension

$$\begin{array}{c} K \\ |_n \\ F \end{array}$$

if it factors into linear factors over that field. K is said to be a *splitting field* of $f(x)$ over F if it splits completely over K, but does not factor into linear factors in any proper subfield of K containing F.

This definition gives the splitting field of a polynomial a sense of minimality. For if L is properly contained in K and $f(x)$ splits over L, then K is not a splitting field.

Theorem 4. *Given a field F and a polynomial $f(x) \in F[x]$, there exists a field K containing F such that K is a splitting field of F. Furthermore, if K and L are both splitting fields for $f(x)$, then K and L are isomorphic [1, 536ff].*

Example 5. A splitting field of $x^n - 1$ over $\mathbb{Q}$ is given by $\mathbb{Q}(\zeta_n)$.

The polynomial $x^n - 1$ has n distinct solutions: $\{e^{2\pi ki/n}\}$, the nth roots of unity, n equally spaced points on the unit circle. Since the set of roots of $x^n - 1$ is contained in $\mathbb{C}$, $x^n - 1$ splits completely in $\mathbb{C}[x]$. $\mathbb{C}$ is not necessarily the splitting field for $x^n - 1$. However, the splitting field of $x^n - 1$ is at least contained in $\mathbb{C}$.

Note that the collection of nth roots of unity form a multiplicative group. As a finite multiplicative group contained in a field, the group is cyclic [10, 118]. Generators of the group are called *primitive* nth roots of unity and are denoted ζ_n. Primitive nth roots of unity are also defined as the nth roots where the smallest exponent a needed such that $x^a = 1$ is $a = n$. Given one primitive nth root of unity ζ_n, the other primitive roots of unity are given by ζ_n^a, where a and n are relatively prime. In fact, there are $\varphi(n)$ primitive nth roots of unity, where φ is Euler's phi function. We will look at Euler's phi function in greater detail in the next example. If a secific primitive nth root is required, we can assume it is $\zeta_n = e^{2\pi i/n}$.

ζ_n generates the roots of $x^n - 1$ and $\mathbb{Q}(\zeta_n)$ is the splitting field field for $x^n - 1$ over $\mathbb{Q}$. We call $\mathbb{Q}(\zeta_n)$, where ζ_n is a primitive nth root of unity, the *cyclotomic extension* generated by the nth roots of unity over $\mathbb{Q}$. Since ζ_n is primitive, it generates all the other nth roots so $\mathbb{Q}(\zeta_n) = \mathbb{Q}(\xi_1, ..., \xi_n)$ where $\xi_1, ..., \xi_n$ are the nth roots of unity. In general, writing $\mathbb{Q}(\zeta_n)$ refers to this cyclotomic extension given by a primitive nth root of unity ζ_n [1, 539].

We have already shown that $\mathbb{Q}(\zeta_n)$ is a splitting field for the polynomial $x^n - 1$. To give an example of finding the degree of an extension, we look at the extension of $\mathbb{Q}$ generated by the nth roots of unity for some n.

1.1.1 Example: The extension $\mathbb{Q}(\zeta_n)/\mathbb{Q}$, where ζ_n is a primitive nth root of unity over $\mathbb{Q}$, is of degree $\varphi(n)$ where φ is Euler's phi-function.

Recall that $\mathbb{Q}(\zeta_n)$, where ζ_n is a primitive nth root of unity, is the cyclotomic extension generated by the nth roots of unity over $\mathbb{Q}$. ζ_n generates all the other nth roots so $\mathbb{Q}(\zeta_n) = \mathbb{Q}(\xi_1, ..., \xi_n)$ where $\xi_1, ..., \xi_n$ are the nth roots of unity.

Euler's phi-function $\varphi(n)$ evaluated at an integer n is defined to be the number of integers z with $1 \leq z \leq n$ that are relatively prime to n. The order of $(\mathbb{Z}/n\mathbb{Z})^\times$ is $\varphi(n)$ where $(\mathbb{Z}/n\mathbb{Z})^\times$ is the group of integers modulo n where each element has a multiplicative inverse. Let μ_n be the group of nth roots of unity over $\mathbb{Q}$, where the group operation is multiplication. Then $\mu_n \cong \mathbb{Z}/n\mathbb{Z}$, where the group operation in $\mathbb{Z}/n\mathbb{Z}$ is addition. In particular, the isomorphism is given by $z \mapsto \zeta_n^z$ for a given primitive nth root of unity ζ_n and $z \in \mathbb{Z}/n\mathbb{Z}$. The primitive nth roots of unity correspond to the elements of $\mathbb{Z}/n\mathbb{Z}$ that are relatively prime to n. There are $\varphi(n)$ such elements and so $\varphi(n)$ primitive nth roots of unity.

Sometimes the nth roots of unity and the dth roots of unity for some integer d will interesect. If d divides n and ζ is a dth root of unity, then $\zeta^n = (\zeta^d)^{n/d} = 1$ so the dth root of unity ζ is also an nth root of unity. And, $\mu_d \subseteq \mu_n$. If $n \neq d$, then the containment must be strict since there are n nth roots of unity and only d dth roots of unity.

On the other hand, if $\mu_d \subseteq \mu_n$ and ζ is a dth root of unity, ζ is also contained in the multiplicative group μ_n and the order of ζ must divide n, the order of μ_n. This alone only shows that $(d,m) \neq 1$, but if we specify that ζ be a primitive dth root of unity, in other words, that ζ be a generator of μ_d, then the order of ζ is d so we conclude the stronger result that d divides n. If d and n are relatively prime, then $\mu_d \cap \mu_n = \{1\}$.

The goal is to show the degree of $\mathbb{Q}(\zeta_n)/\mathbb{Q}$ is $\phi(n)$ and there are precisely $\phi(n)$ primitive nth roots of unity. We will construct a minimal polynomial of degree $\varphi(n)$ over $\mathbb{Q}$ from the primitive nth roots of unity.

Definition 6. Let the *nth cyclotomic polynomial* $\Phi_n(x)$ be the polynomial whose roots are the primitive nth roots of unity.

$$\Phi_n(x) = \prod_{\substack{\zeta \in \mu_n \\ \zeta \text{ primitive}}} (x - \zeta).$$

In the setting of $\mathbb{Z}/n\mathbb{Z}$, $\Phi_n(x)$ is equivalently given by

$$\Phi_n(x) = \prod_{\substack{1 \leq z < n \\ (z,n)=1}} (x - \zeta_n^z)$$

where ζ_n is a fixed primitive nth root of unity.

Note that $\Phi_n(x)$ is of degree $\varphi(n)$ as desired but to serve as a minimal polynomial, it must also be irreducible and in $\mathbb{Q}[x]$. $\Phi_n(x)$ can also be defined recursively.

Definition 7. The cyclotomic polynomials $\Phi_n(x)$ are defined inductively for $n = 1, 2, ...$ by

$$\Phi_1(x) = x - 1$$

and

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

[10, 121].

A few small values of Φ_n are given here:

$$\begin{aligned}
\Phi_5(x) &= x^4 + x^3 + x^2 + x + 1 \\
\Phi_6(x) &= x^2 - x + 1 \\
\Phi_7(x) &= x^6 + x^5 + x^4 + x^3 + x^2 + x + 1 \\
\Phi_8(x) &= x^4 + 1.
\end{aligned}$$

If p is a prime number, then

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

The two definitions for $\Phi_n(x)$ are equivalent. To see this, take the first definition, $\Phi_n(x) = \prod_{\zeta \in \mu_n \text{ primitive}} (x - \zeta)$, and consider the polynomial $x^n - 1$ whose roots are all the nth roots of unity, including the primitive ones:

$$x^n - 1 = \prod_{\zeta \in \mu_n} (x - \zeta).$$

If d is a divisor of n, we showed that $\mu_d \subseteq \mu_n$. Each element of μ_n has order d dividing n (here n can equal d). Then if we group factors $x - \zeta$ of $x^n - 1$ by the order of ζ, we have accounted for all the elements of μ_n. And if the order of a particular element $\zeta \in \mu_n$ is d, ζ is automatically a

primitive dth root of unity since it has order d. Then

$$x^n - 1 = \prod_{d|n} \prod_{\substack{\zeta \in \mu_d \\ \zeta \text{ primitive}}} (x - \zeta).$$

The inner product $\prod_{\substack{\zeta \in \mu_d \\ \zeta \text{ primitive}}} (x - \zeta)$ is precisely $\Phi_d(x)$ so

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

Dividing $\Phi_n(x)$ by $\prod_{d|n} \Phi_d(x)$, where $d < n$, removes all the roots of unity of order less than n. In other words, dividing by the product leaves only the nth primitive roots of unity:

$$x^n - 1 = \prod_{d|n} \Phi_d(x) = \Phi_n(x) \cdot \prod_{\substack{d|n \\ d<n}} \Phi_d(x) \implies \Phi_n(x) = \frac{x^n - 1}{\prod_{\substack{d|n \\ d<n}} \Phi_d(x)}.$$

It can be shown that the polynomial $\Phi_n(x)$ is monic with integer coefficients for all n and by induction on n, we can see $\Phi_n(x) \in \mathbb{Q}[x]$. Now that we have established that the two definitions are equivalent, we include two lemmas that will be instrumental in proving $\Phi_n(x)$ is irreducible.

Lemma 8. *Let f and g be polynomials over a field F and let f be irreducible in $F[x]$. If f and g have a common root in some field K containing F, then f divides g.*

Proof. Say f and g have a common root α in a field K containing F. If f does not divide g, then f and g are relatively prime in $F[x]$. Otherwise, f and g would share a common factor which contradicts the irreducibility of f. Since f and g are relatively prime, by the division algorithm, there exist $a, b \in F[x]$ such that

$$a(x)f(x) + b(x)g(x) = 1.$$

In particular, if $x = \alpha$, the common root of f and g, then f and g vanish at α and

$$1 = a(\alpha)f(\alpha) + b(\alpha)g(\alpha) = 0.$$

Since $1 \neq 0$, there is a contradiction, so f divides g. □

Lemma 9. *If f is a monic irreducible factor of $\Phi_n(x)$ in $\mathbb{Q}[x]$ and p is a prime number that does not divide n, then if $w \in \mathbb{C}$ is a root of f, w^p is also a root of f.*

Given one root of f, we can find others. We omit the proof of this lemma, but it can be found in [10, 220].

Theorem 10. *The cyclotomic polynomial $\Phi_n(x)$ is irreducible over $\mathbb{Q}$ for all $n \geq 1$.*

Proof. Let $f(x)$ be a monic irreducible factor of $\Phi_n(x)$ in $\mathbb{Q}[x]$. Let ζ be a root of f. Since ζ is a root of f, a factor of $\Phi_n(x)$, ζ is a primitive nth root of unity. Every other primitive nth root of unity has the form ζ^k for some integer k relatively prime to n and less than n. k factors into prime factors: $k = p_1 \cdot \ldots \cdot p_s$ where the p_i are prime. Since k and n are relatively prime, the p_i do not divide n.

By the lemma, $f(\zeta) = 0$ implies $f(\zeta^{p_1}) = 0$ which implies $f(\zeta^{p_1 p_2}) = 0$. Applying the lemma repeatedly gives $f(\zeta^k) = f(\zeta^{p_1 \cdots p_s}) = 0$. Since this can be done for all k relatively prime to n and less than n, every primitive nth root of unity is a root of f. Consequently, $\Phi_n(x)$ divides f. Since f was assumed to be a factor of $\Phi_n(x)$ and both f and $\Phi_n(x)$ are monic, f and $\Phi_n(x)$ must be equal [10, 260].

It is evident that any primitive nth root of unity is also a root of $\Phi_n(x)$ and since $\Phi_n(x)$ is irreducible, $\Phi_n(x)$ is the minimal polynomial for any primitive nth root of unity.

□

Corollary 11. *The degree of $\mathbb{Q}(\zeta_n)$ over $\mathbb{Q}$ is $\varphi(n)$:*

$$[\mathbb{Q}(\zeta_n) : \mathbb{Q}] = \varphi(n).$$

For example, the cyclotomic field $\mathbb{Q}(\zeta_8)$ has degree 4 over $\mathbb{Q}$. In particular, the minimal polynomial of the primitive 8th roots of unity is $\Phi_8(x) = x^4 + 1$. Incidentally, $\mathbb{Q}(\zeta_8) = \mathbb{Q}(i, \sqrt{2})$ where i is a primitive 4th root of unity and $\sqrt{2} = \zeta_8 + \zeta_8^7$.

Corollary 12. *If m and n are relatively prime, then $\Phi_m(x)$ is irreducible over $\mathbb{Q}(\zeta_n)$ [10, 260].*

1.1.2 Algebraic Field Elements

The solutions of a polynomial $f(x)$ with coefficients in F are not themselves necessarily contained in that field F. Consequently, we ask if there exists a field containing F that does in fact contain all the solutions of $f(x)$.

Definition 13. Given a field extension K/F. $\alpha \in K$ is *algebraic* over F if α is the root of a nonzero polynomial $f(x)$ in $F[x]$. If α is not algebraic over F, then α is called *transcendental* over F. The field extension K/F is described as an *algebraic extension* if α is algebraic over F for all $\alpha \in K$.

Note that if $\alpha \in F$, then α is algebraic over F because $f(x) = x - \alpha \in F[x]$ and $f(\alpha) = 0$. Also, if α is algebraic over F, then α is also algebraic over any field extension L of F because $f(x) \in F[x] \subseteq L[x]$ for all $f(x) \in F[x]$, in particular the ones with α as a root. We can show that the set of elements of K that are algebraic over F form a subfield of K that contains F [1, 527].

Definition 14. The *algebraic closure* $\bar{F}$ of a field F contained in a field K is the field of elements of K which are algebraic over F. F is *algebraically closed* in K if $\bar{F} = F$ [14, 61].

Alternatively, a field $\bar{F}$ can be defined as the algebraic closure if $\bar{F}$ is algebraic over F and $\bar{F}$ contains all elements of K algebraic over F [1, 543].

Example 15. For $\mathbb{Q} \subset \mathbb{C}$, the set of all elements of $\mathbb{C}$ that are algebraic over $\mathbb{Q}$ is denoted $\bar{\mathbb{Q}} = \{\alpha \in \mathbb{C} : \alpha \text{ is algebraic over } \mathbb{Q}\}$. We can show $\bar{\mathbb{Q}}$ is an algebraic extension of $\mathbb{Q}$, that it is not a finite extension of $\mathbb{Q}$, and that $\bar{\mathbb{Q}} \neq \mathbb{C}$. On the other hand, if $\mathbb{C} \subseteq E$ and $z \in E$ is algebraic over $\mathbb{C}$, then $z \in \mathbb{C}$, so $\mathbb{C}$ is algebraically closed (this is another statement of the Fundamental Theorem of Algebra) [1, 545].

Example 16. Quadratic extensions of fields of characteristic $\neq 2$.

Let F be a field of characteristic $p \neq 2$ and let K be an extension of F of degree 2. Fix $\alpha \in K$ such that $\alpha \notin F$. K is a finite extension of F so K is an algebraic extension of F. In particular, $\alpha \in K$ satisfies some polynomial equation of degree at most 2 over F. Since α is not in F, the equation has no linear factors and must be a degree 2 polynomial

$$x^2 + bx + c$$

for some $b, c \in F$. We claim that $F(\alpha) = K$. Indeed, since $\alpha \notin F$, F is strictly contained in $F(\alpha)$ and $F(\alpha)$ must have degree greater than 1 over F. On the other hand, since $\alpha \in K$, $F(\alpha) \subseteq K$ so $F(\alpha)$ must have degree less than or equal to 2 over F. We conclude $[K : F(\alpha)] = 1$ and $F(\alpha) = K$.

By construction, α is a root of $x^2 + bx + c$. What is the other root? Since the characteristic of F is not 2, $2 \cdot 1_F \neq 0_F$ and the quadratic formula

$$\alpha = \frac{-b \pm \sqrt{b^2 - 4c}}{2}$$

is valid. Note that if $b^2 - 4c$ is the square of some element d in F, then

$$b^2 - 4c = d^2 \implies \alpha = \frac{-b \pm d}{2} \in F,$$

which is impossible since α was chosen not in F. In fact, though b^2-4c is in F, $\sqrt{b^2-4c}$ need not be in F. It is the root of the polynomial

$$x^2-(b^2-4c)$$

in K. We find the field extension of F generated by $\sqrt{b^2-4c}$. Note that $+\sqrt{b^2-4c}$ and $-\sqrt{b^2-4c}$ give the same field extension since $-1 \in F$: $F\left(+\sqrt{b^2-4c}\right) = F\left(-\sqrt{b^2-4c}\right)$ so we need not worry about specifying a specific positive or negative root.

We show that $F(\alpha) = F\left(\sqrt{b^2-4c}\right)$. $F(\alpha) \subseteq F\left(\sqrt{b^2-4c}\right)$ because $\alpha = \frac{-b}{2} \pm \frac{1}{2} \cdot \sqrt{b^2-4c}$, which is given by the quadratic formula. Alternatively, solving the same formula for $\sqrt{b^2-4c}$ gives $\sqrt{b^2-4c} = \mp(b+2\alpha)$ so $F\left(\sqrt{b^2-4c}\right) \subseteq F(\alpha)$ and consequently

$$F\left(\sqrt{b^2-4c}\right) = F(\alpha).$$

This shows $\sqrt{b^2-4c}$ is an element of $F(\alpha)$ and is a solution in K to the polynomial $x^2-(b^2-4c)$.

In summary, given K, an extension of F of degree 2, K is of the form $F(\sqrt{D})$ for some element D of F. Furthermore, D was not the square of any element of F. And conversely, any D that is not the square of some element of F gives a degree-2 extension of F, $F(\sqrt{D})$. Such extensions are called *quadratic* extensions [1, 522].

1.1.3 The Galois Group

Definition 17. An extension K/F is a *normal extension* if K is the splitting field for one or more polynomials over F.

In fact, K can be a splitting field for infinitely many polynomials over F [1, 650].

Definition 18. Let f be an irreducible polynomial in $F[x]$ with roots in a splitting field K. f is *separable* over F if all its roots are distinct. If f has a multiple root it is *inseparable*.

If K is a field extension of F, then K is said to be *separable* over F if the minimal polynomial of every element in K is separable. Otherwise, K is *inseparable* over F [1, 551].

So far, we have defined finite extensions, algebraic extensions, normal extensions, and separable extensions. Normal extensions are algebraic, but need not be finite or separable [1, 650].

Theorem 19. *Every finite extension of a finite field or of $\mathbb{Q}$ is a separable extension [1, 551].*

Now that we have characterized these various types of field extensions, we define one more extension: the Galois extension.

Definition 20. Let K be a finite extension of F. The set of automorphisms of K that fix F elementwise is denoted $\mathrm{Aut}(K/F)$. In general, $|\mathrm{Aut}(K/F)| \leq [K:F]$ [1, 562]. If $|\mathrm{Aut}(K/F)| = [K:F]$, then K is a *Galois extension* of F (K is *Galois* over F) and $\mathrm{Aut}(K/F)$ is called the *Galois group* of K/F and is denoted $\mathrm{Gal}(K/F)$.

Remark 21. This definition of a Galois extension emphasizes that we wish $\mathrm{Aut}(K/F)$ to have the maximum number of elements as possible.

Theorem 22. *Let K/F be a finite extension. K is the splitting field of a separable polynomial if and only if K is Galois over F.*

The forward direction is shown in [1, 562] and the reverse direction is in [1, 572]. This equivalent condition for a Galois extension emphasizes the relationship between the automorphisms over a field and the roots of a polynomial over the field. So, for K to be a Galois extension of F, K must be a normal and separable extension of F. K a normal extension means it is a splitting field for a polynomial over F.

As an example of finding the Galois group of a field extension, we look at the cyclotomic extension $\mathbb{Q}(\zeta_n)$ of nth roots of unity.

Example 23. The Galois group of the cyclotomic field $\mathbb{Q}(\zeta_n)$ is isomorphic to $(\mathbb{Z}/n\mathbb{Z})^\times$, the multiplicative group of integers modulo n.

If σ is an automorphism of $\mathbb{Q}(\zeta_n)$, then σ is completely determined by its action on the generator of the field, a primitive nth root of unity ζ_n. In this case, ζ_n is a root of the minimal polynomial $\Phi_n(x)$, so under σ, ζ_n must be mapped to another root of $\Phi_n(x)$, or equivalently, another primitive nth root of unity. The other primitive nth roots are all unique powers of ζ_n. So

$$\sigma(\zeta_n) = \zeta_n^z$$

for some integer z between 1 and n that is relatively prime to n. There are $\varphi(n)$ such integers z and hence $\varphi(n)$ distinct automorphisms of $\mathbb{Q}(\zeta_n)$. We conclude $[\mathbb{Q}(\zeta_n):\mathbb{Q}] = \varphi(n)$. The isomorphism between $(\mathbb{Z}/n\mathbb{Z})^\times$ and $\mathrm{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{Q})$ is given by

$$\begin{array}{rcl} (\mathbb{Z}/n\mathbb{Z})^\times & \to & \mathrm{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{Q}), \\ z \pmod n & \mapsto & \sigma_z \end{array}$$

where σ_z is an automorphism of $\mathrm{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{Q})$ defined by its action on ζ_n:

$$\sigma_z(\zeta_n) = \zeta_n^z.$$

This mapping is a homomorphism, one-to-one and onto [1, 596].

1.2 Additional Theorems for Galois Groups

After finding various Galois groups of field extensions, we see that there is some relationship between intermediate fields in a Galois extension and subgroups of the Galois group for that extension. The following theorem gives a glimps of this structure and is called the Fundamental Theorem of Galois Theory.

Theorem 24. *Let K be a Galois extension of F and $G = Gal(K/F)$. Then K is a Galois extension of every subfield that contains F. Furthermore, there is a bijection between the subfields of K containing F and subgroups of G, where any subfield L corresponds to the Galois group $Gal(K/L)$ and any subgroup H corresponds to the field of elements fixed element-wise by H:*

$$\begin{aligned} L &\rightarrow \{\textit{automorphisms in } G \textit{ fixing } L \textit{ element-wise}\}, \\ \{\textit{the fixed field of } H\} &\leftarrow H. \end{aligned}$$

Then $[K:L] = |H|$ while $[L:F] = |G:H|$, the index of H in G. Furthermore, the correspondence is inclusion reversing. If the fields L_1 and L_2 are associated with the groups H_1 and H_2, then $L_1 \subseteq L_2$ if and only if $H_2 \leq H_1$. Lastly, L is Galois over F if and only if H is a normal subgroup of G, and then

$$Gal(L/F) \cong Gal(K/F)/H = G/H.$$

It is important to note that if L is a field in the Galois extension K/F, then K is guaranteed to be a Galois extension of L, but L need not be a Galois extension of F. As stated in the theorem, this is only true when the subgroup H associated with L is normal in the Galois group of K/F [10, 402].

The next example is a demonstration of using the Fundamental Theorem of Galois Theory.

Example 25. The Galois group of $\mathbb{Q}(\zeta_5)$ over $\mathbb{Q}$ is $(\mathbb{Z}/5\mathbb{Z})^\times \cong \mathbb{Z}/4\mathbb{Z}$.

The minimal polynomial of ζ_5 over $\mathbb{Q}$ is $\Phi_5(x) = x^4 + x^3 + x^2 + x + 1$.

$$\mathrm{Gal}(\mathbb{Q}(\zeta_5)/\mathbb{Q}) = \{\sigma_1, \sigma_2, \sigma_3, \sigma_4\}$$

where $\sigma_z(\zeta_5) = \zeta_5^z$. $\sigma_1 = \text{id}$, since $\sigma_1(\zeta_5) = \zeta_5$. Since 2 is a generator in $(\mathbb{Z}/5\mathbb{Z})^\times$, then σ_2 is a generator of the Galois group. $(\mathbb{Z}/5\mathbb{Z})^\times$ has exactly one nontrivial, proper subgroup $\{1,4\}$ and the Galois group has exactly one nontrivial, proper subgroup $\{\sigma_1, \sigma_4\}$. Consider $\zeta_5 + \zeta_5^4 \in \mathbb{Q}(\zeta_5)$.

$$\sigma_1(\zeta_5 + \zeta_5^4) = \zeta_5 + \zeta_5^4 = (\zeta_5^{3\cdot 5})\zeta_5 + \zeta_5^4 = \zeta_5^{16} + \zeta_5^4 = \sigma_4(\zeta_5 + \zeta_5^4)$$

so $\zeta_5 + \zeta_5^4$ is an element of the fixed field of $\{\sigma_1, \sigma_4\}$. ζ_5 is a root of $\Phi_5(x)$, and thus $\zeta_5 + \zeta_5^4$ satisfies $x^2 + x - 1$ because

$$(\zeta_5 + \zeta_5^4)^2 + (\zeta_5 + \zeta_5^4) - 1 = \zeta_5^2 + 2\zeta_5^5 + \zeta_5^8 + \zeta_5 + \zeta_5^4 - 1 = \zeta_5^4 + \zeta_5^3 + \zeta_5^2 + \zeta_5 + 1 = 0.$$

$x^2 + x - 1 = \left(x - \frac{-1-\sqrt{5}}{2}\right)\left(x - \frac{-1+\sqrt{5}}{2}\right)$ in $\mathbb{C}[x]$ so $x^2 + x - 1$ has no linear factors in $\mathbb{Q}[x]$ and is irreducible over $\mathbb{Q}$. We conclude that

$$\mathbb{Q}(\zeta_5 + \zeta_5^4) = \mathbb{Q}(\sqrt{5})$$

is the fixed field of $\{\sigma_1, \sigma_2\}$ and is a quadratic extension of $\mathbb{Q}$ [1, 597].

We can also look at composites of Galois extensions.

Definition 26. If F_1 and F_2 are subfields of a field K, the *composite field* of F_1 and F_2 is the smallest subfield of K that contains both F_1 and F_2. The composite of F_1 and F_2 is denoted F_1F_2.

Theorem 27. *Let F be a field with K a Galois extension of F and F' any extension of F. Then KF' is a Galois extension of F' with Galois group*

$$Gal(KF'/F') \cong Gal(K/K \cap F'),$$

which is isomorphic to a subgroup of $Gal(K/F)$.

Going up to KF' over F' is called *sliding up* a Galois extension.

Corollary 28. *If F is a field with Galois extension K and field extension F', then*

$$[KF' : F'] = \frac{[K : F][F' : F]}{[K \cap F' : F]}.$$

Both the theorem and the corollary are not very strong in that the the composite extension is only guaranteed to be Galois over F' instead of F. On the other hand, if both field extensions are Galois, then we have a stronger result.

Theorem 29. *Let F be a field and let K_1 and K_2 be Galois extensions of F. Then the intersection $K_1 \cap K_2$ and the composite K_1K_2 are Galois over F. Furthermore, the Galois group of K_1K_2 over F is isomorphic to $H = \{(\sigma,\tau) : \sigma \mid_{K_1\cap K_2} = \tau \mid_{K_1\cap K_2}\}$, the subgroup of the direct product $Gal(K_1/F) \times Gal(K_2/F)$ where the elements $\sigma \in Gal(K_1/F)$ and $\tau \in Gal(K_2/F)$ are such that their restrictions to $K_1 \cap K_2$ match [1, 591ff].*

Note that the above Corollary still applies to K_1 and K_2. If we take the specific case where $F = K_1 \cap K_2$, then $\mathrm{Gal}(K_1K_2/F)$ is not a strict subgroup of $\mathrm{Gal}(K_1/F) \times \mathrm{Gal}(K_2/F)$.

Corollary 30. *Let F be a field and let K_1 and K_2 be Galois extensions of F with $K_1 \cap K_2 = F$. Then*

$$Gal(K_1K_2/F) \cong Gal(K_1/F) \times Gal(K_2/F)$$

[1, 591ff].

Theorem 31. *Let an integer n have the prime decomposition $n = p_1^{a_1} \cdot \ldots \cdot p_k^{a_k}$ where the p_i are distinct primes. The cyclotomic fields $\mathbb{Q}(\zeta_{p_i^{a_i}})$ intersect only in $\mathbb{Q}$ and their composite is the cyclotomic field $\mathbb{Q}(\zeta_n)$. Furthermore,*

$$Gal(\mathbb{Q}(\zeta_n)/\mathbb{Q}) \cong Gal(\mathbb{Q}(\zeta_{p_1^{a_1}})/\mathbb{Q}) \times \ldots \times Gal(\mathbb{Q}(\zeta_{p_k^{a_k}})/\mathbb{Q})$$

[1, 591ff].

Incidentally, recalling that $\mathrm{Gal}(\mathbb{Q}(\zeta_{p_i^{a_k}})/\mathbb{Q}) \cong (\mathbb{Z}/p_i^{a_i}\mathbb{Z})^\times$, the above theorem results in the Chinese Remainder Theorem:

$$(\mathbb{Z}/n\mathbb{Z})^\times \cong (\mathbb{Z}/p_1^{a_1}\mathbb{Z})^\times \times \ldots \times (\mathbb{Z}/p_k^{a_k}\mathbb{Z})^\times.$$

Another consequence of the theorem is that the Galois group of $\mathbb{Q}(\zeta_n)/\mathbb{Q}$ is an abelian group which we already knew as $\mathrm{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{Q}) \cong (\mathbb{Z}/n\mathbb{Z})^\times$.

Definition 32. A Galois extension with an abelian Galois group is called an *abelain* extension.

Our final topic in this section is extending the results for Galois groups from finite extensions to infinite extensions. Originally, a field extension K/F was defined to be Galois if the size of the automorphism group of K/F was equal to the degree of the extension K/F. Then the Galois group was defined to be the automorphism group of K/F. In subsequent results, we found a finite extension K/F to be Galois provided it is normal and separable. To extend the idea of Galois extensions to infinite extensions, we use the normal and separable characterization.

Definition 33. An arbitrary extension E/F that is algebraic, normal, and separable over F is said to be a *Galois extension*. If E/F is a Galois extension, the *Galois group* of E/F, denoted $\mathrm{Gal}(E/F)$, is the group of automorphisms on E that fix F, denoted $\mathrm{Aut}(E/F)$.

As might be expected, this new definition, that now applies to both finite and infinite extensions, does not maintain the level of structure that the fundamental theorem of Galois theory guarantees in finite extensions. In particular, the fundamental theorem of Galois theory gives a bijection between subgroups of the Galois group and intermediate fields of E and F. We give a brief example of some issues that might arise in the following example from [1].

Example 34. Consider the extension E of $\mathbb{Q}$ acquired by adding all the square roots of positive elements of $\mathbb{Q}$. E is equivalently given as the splitting field for all polynomials of the form $x^2 - p$ where p is a positive prime integer. From this description, it can be seen that E is a countably infinite extension of $\mathbb{Q}$.

Any automorphism σ in $\mathrm{Gal}(E/F)$ is defined by its action on the roots of each $x^2 - p$. Given a specific p, σ sends a root of p to itself or its negation. So any σ must have order 2. It turns out that $\mathrm{Gal}(E/F)$ contains uncountably many distinct elements and moreover, uncountably many subgroups of index 2. On the other hand, there are only countably infinitely many quadratic extensions of $\mathbb{Q}$. This effectively eliminates the possibility of a correspondence between subgroups of $\mathrm{Gal}(E/F)$ of index 2 in $\mathrm{Gal}(E/F)$ and extensions of $\mathbb{Q}$ of degree 2.

One method of tackling this problem, is to define a topology on the subgroups of $\mathrm{Gal}(E/F)$ called the Krull topology. In this topology, finite extensions of F correspond to *closed* subgroups in $\mathrm{Gal}(E/F)$ [1, 651]. We do not include this approach here.

Chapter 2

The Inverse Galois Problem

2.1 Introduction and General Results

The Inverse Galois Problem is the search for a Galois field extension of $\mathbb{Q}$ whose Galois group over $\mathbb{Q}$ gives a desired group. The question of whether such an extension exists for any given finite group is attributed to Emmy Noether [2], David Hilbert [11], or both depending on the reference. While the question has been answered affirmatively for many different kind of groups, the question is still an open problem. Weaker forms of the question lead to complete answers.

Theorem 35. *Given a finite group G, there exists a finite algebraic extension K of* $\mathbb{Q}$ *such that* $Aut(K/\mathbb{Q}) \cong G$.

As K is not guaranteed to be normal extension of $\mathbb{Q}$, this falls short of answering the Inverse Galois Problem in the form stated above. Ervin Fried and János Kollár gave a proof of this result with an erroneous lemma in 1978 [2, 121] and Fried fixed the lemma two years later providing a complete proof [3, 386].

Alternatively, if the other requirement, that the extension be of $\mathbb{Q}$, is relaxed, then every finite group is again realizable.

Proposition 36. *Every finite group is the Galois group of some Galois extension of* $\mathbb{C}(t)$ *and the Galois group of some Galois extension of* $\mathbb{R}(t)$.

The proof for this proposition can be found in [7, 7].

The difficulty in answering the Inverse Galois Problem is not finding field extensions that give a specific Galois group, but rather lowering the ground field to the rationals $\mathbb{Q}$. A closer result to the desired extensions of $\mathbb{Q}$ involves another field that contains $\mathbb{Q}$. On page9, we defined $\bar{\mathbb{Q}}$ to be

the set of elements of $\mathbb{C}$ that are algebraic over $\mathbb{Q}$. In particular, $\bar{\mathbb{Q}}$ is a strict subfield of $\mathbb{C}$ and is algebraically closed. Malle and Matzat show that given a finite group and an algebraically closed field $\bar{k}$ of characteristic zero, then the group is realizable by an extension of the function field $\bar{k}(t)$ [7, 12].

Corollary 37. *Every finite group is the Galois group of some extension of $\bar{\mathbb{Q}}(t)$, where $\bar{\mathbb{Q}}$ is the algebraic closure of $\mathbb{Q}$.*

Proof. The corollary follows immediately as $\bar{\mathbb{Q}}$ is an algebraically closed field of characteristic zero. □

When the Inverse Galois Problem is posed over the rationals $\mathbb{Q}$, the problem is still unanswered. The most comprehensive results were given by Igor Šafarevič and are summarized in the following theorem.

Theorem 38. *All solvable groups can be realized as Galois groups over $\mathbb{Q}$.*

This result is attributed to Šafarevič in 1954 [8, 1]. In many cases, explicit polynomials have been found or can be constructed that give a desired Galois group. Malle and Matzat have tables of polynomials for transitive groups of degree less than twelve in [7, 404]. On the other hand, the list is by no means comprehensive. For example, the nonsolvable primitive groups $L_2(16)$, $L_3(4)$, M_{23}, $L_2(25)$ and $L_2(27)$ have no known polynomials over either $\mathbb{Q}$ or $\mathbb{Q}(t)$ [7, 410].

2.2 Results over $\mathbb{Q}$

In building the background information for finding a Galois group, we supplied examples and theorems that help to form partial results for the Inverse Galois Problem.

Corollary 39. *Let G be a finite abelian group. There is a cyclotomic field with K as a subfield such that $Gal(K/\mathbb{Q}) \cong G$.*

Proof. For this proof, we assume the fact that given an integer m, there are infinitely many primes p such that $p \equiv 1 \pmod{m}$. More generally, Dirichlet's Theorem on Primes in Arithmetic Progressions states that for any a relatively prime to m, there are infinitely many prime p such that $p \equiv a \pmod{m}$.

Let G be a finite abelian group. Then there exist integers $n_1, \ldots, n_k$ such that

$$G \cong \mathbb{Z}_{n_1} \times \ldots \times \mathbb{Z}_{n_k}.$$

By the fact assumed above, there are infinitely many primes equivalent to 1 modulo n_i so we can pick distinct $p_1, ..., p_k$ such that

$$\begin{aligned} p_1 &\equiv 1 \pmod{n_1} \\ &\vdots \\ p_k &\equiv 1 \pmod{n_k}. \end{aligned}$$

Let n be the product of the p_i: $n = p_1 \cdot ... \cdot p_k$. Since each $p_i \equiv 1 \pmod{n_i}$, n_i divides $p_i - 1$. $\frac{p_i-1}{n_i}$ also divides $p_i - 1$ and consequently, the group $\mathbb{Z}_{p_i-1}$ has a subgroup of order $\frac{p_i-1}{n_i}$ which we call H_i. The quotient group of $\mathbb{Z}_{p_i-1}$ with H_i is cyclic and has order n_i and furthermore, the quotient

$$\frac{\mathbb{Z}_{p_1-1} \times ... \times \mathbb{Z}_{p_k-1}}{H_1 \times ... \times H_k} \cong \mathbb{Z}_{n_1} \times ... \times \mathbb{Z}_{n_k}.$$

Recalling that $\mathrm{Gal}(\mathbb{Q}(\zeta_{p_i^{a_k}})/\mathbb{Q}) \cong (\mathbb{Z}/p_i^{a_i}\mathbb{Z})^\times$, the group

$$\mathrm{Gal}\left(\mathbb{Q}\left(\zeta_{p_1 \cdot ... \cdot p_k}\right)/\mathbb{Q}\right) \cong (\mathbb{Z}/(p_1 \cdot ... \cdot p_k)\mathbb{Z})^\times$$

and by the Chinese Remainder Theorem,

$$\mathrm{Gal}\left(\mathbb{Q}\left(\zeta_{p_1 \cdot ... \cdot p_k}\right)/\mathbb{Q}\right) \cong (\mathbb{Z}/p_1\mathbb{Z})^\times \times ... \times (\mathbb{Z}/p_k\mathbb{Z})^\times \cong \mathbb{Z}_{p_1-1} \times ... \times \mathbb{Z}_{p_k-1}.$$

We have found a group $\mathbb{Z}_{p_1-1} \times ... \times \mathbb{Z}_{p_k-1}$ that is the Galois group of the extension $\mathbb{Q}\left(\zeta_{p_1 \cdot ... \cdot p_k}\right)$ over $\mathbb{Q}$. Furthermore, $\mathbb{Z}_{p_1-1} \times ... \times \mathbb{Z}_{p_k-1}$ has a subgroup $H_1 \times ... \times H_k$ where by the Fundamental Theorem of Galois Theory,

$$\mathrm{Gal}\left(\frac{\mathrm{Fix}\left(H_1 \times ... \times H_k\right)}{\mathbb{Q}}\right) \cong \frac{\mathrm{Gal}\left(\mathbb{Q}\left(\zeta_{p_1 \cdot ... \cdot p_k}\right)/\mathbb{Q}\right)}{\mathrm{Gal}\left(\mathbb{Q}\left(\zeta_{p_1 \cdot ... \cdot p_k}\right)/\mathrm{Fix}\left(H_1 \times ... \times H_k\right)\right)}$$

$$\cong \frac{\mathbb{Z}_{p_1-1} \times ... \times \mathbb{Z}_{p_k-1}}{H_1 \times ... \times H_k} \cong \mathbb{Z}_{n_1} \times ... \times \mathbb{Z}_{n_k} \cong G.$$

So we have a field extension $\mathrm{Fix}\left(H_1 \times ... \times H_k\right)$ whose Galois extension over $\mathbb{Q}$ is G and $\mathrm{Fix}\left(H_1 \times ... \times H_k\right)$ is contained in an extension generated by roots of unity [1, 599]. □

The Kronecker-Weber Theorem is the converse of this result. *The difference between the two theorems is subtle.* The above corollary guarantees that given an abelian group, there exists an extension of $\mathbb{Q}$, which by necessity is abelian, such that the the extension is contained in a cyclo-

tomic extension, and the Galois group of the extension gives the abelian group desired. Since this only guarantees existence, it says nothing about other field extensions that also give that Galois group. There could exist some extension of $\mathbb{Q}$ not contained in a cyclotomic extension of $\mathbb{Q}$ that also realizes the desired group. On the other hand, the Kronecker-Weber theorem shows this to be impossible.

Theorem 40. *(Kronecker-Weber Theorem) If K is a finite abelian extension of $\mathbb{Q}$, then K is contained in a cyclotomic extension of $\mathbb{Q}$.*

The proof of the Kronecker-Weber theorem will be given in a following section. Sometimes the Kronecker-Weber theorem is taken to mean the conjunction of the theorem we have stated and the corollary above: that any finite abelian group is realizable as the Galois group of an extension of $\mathbb{Q}$ and that extension must be contained in a cyclotomic extension. As we have already proved the corollary, we do not do so in the proof of the Kronecker-Weber theorem given in this paper.

Theorem 41. *S_n is a Galois group over $\mathbb{Q}$ for all n.*

The proof given in [1, 645 ff] uses something called a transcendence base to define an extension to be purely transcendental. The fixed field of S_n over $\mathbb{Q}$ is transcendental over $\mathbb{Q}$ which by further results shows that S_n is a Galois group over $\mathbb{Q}$. However, we will present the proof of this result as a consequence of the rigidity of S_n which we define below.

2.3 Rigid Groups

To define what it means for a group to be rigid, we need to recall what it means for a group to act on a set.

Definition 42. Let G be a group and X a set. A map from $G \times X$ to X, denoted by $g \cdot x$ for $g \in G$ and $x \in X$, is an *action* if

(1) $g_1 \cdot (g_2 \cdot x) = (g_1 \cdot g_2) \cdot x$ for all $g_1, g_2 \in G$, $x \in X$,

(2) $e_G \cdot x = x$ for all $x \in X$.

Actions have equivalence classes defined by how the group G acts on a specific element of X.

Definition 43. The *orbit* of G containing $x \in X$ is $G \cdot x = \{g \cdot x \mid g \in G\}$.

If the action on X has only one orbit, we say the group is transitive. In this case, given any two elements x, y of X, there exists $g \in G$ such that $y = g \cdot x$. Formally we write the following.

Definition 44. An action of a group G on a set X is *transitive* if X is nonempty and for all $x \in X$,

$$G \cdot x = X$$

where $G \cdot x = \{g \cdot x : g \in G\}$ is the orbit of x under G.

We often look at when a grou acts on itself through conjugation.

Definition 45. The group G acts on itself (i.e. $X = G$) by *conjugation* where for $g \in G$ and $x \in G$,

$$g \cdot x = gxg^{-1}$$

and gxg^{-1} is computed using the group operation of G. x, y in G are said to be *conjugate* if there exists $g \in G$ such that $y = g \cdot x = gxg^{-1}$.

With conjugation, the orbit of an element $x \in G$ becomes $G \cdot x = \{gxg^{-1} \mid g \in G\}$ and in this case, $G \cdot x$ is called the *conjugacy class* of G containing x.

Example 46. Two elements of S_n are *conjugates* (in the same conjugacy class), if and only if they have the same cycle shape [1, 126].

Theorem 47. *Let H be a subgroup of S_n that acts transitively on $\{1, ..., n\}$ by the action $s \cdot x = s(x)$ for $s \in S_n$ and $x \in \{1, ..., n\}$. If H contains a two-cycle and an $(n-1)$-cycle, H must be all of S_n [1, 642].*

Proof. Let H be a subgroup of S_n that acts transitively on $\{1, ..., n\}$ and that contains a two-cycle and an $(n-1)$-cycle. By reordering, we can assume the $(n-1)$-cycle is $(1\ 2\ ...\ (n-1))$. Let the two-cycle be $(i\ j)$ for some $i \neq j \in \{1, ..., n\}$. Since H is a transitive subgroup, there exists $t \in H$ such that $t(j) = n$. t has that $t(i) = k$ for some $j \in \{1, ..., n\}$. Then

$$t \cdot (i\ j) \cdot t^{-1} = (t(i)\ t(j)) = (k\ n).$$

In fact, given any transposition of the form $(a\ n)$ where $a \neq n$ and $a \in \{1, ..., n\}$, we can use $(k\ n)$ to get $(a\ n)$. Since $a \neq n$, $a = k + m \pmod{n-1}$ for some $m \in \{1, ..., n\}$ and

$$s^m \cdot (k\ n) \cdot s^{-m} = (s^m(k)\ s^m(n)) = (k + m \pmod{n-1}\ n) = (a\ n).$$

Furthermore, we can now find any transposition $(a\ b)$ where $a, b \in \{1, ..., n\}$ and $a \neq b$. We have

already shown $(a\ n), (b\ n) \in H$ so

$$(b\ n)(a\ n)(b\ n)^{-1} = (a\ b).$$

Since all the transpositions of S_n are contained in H, and any element of S_n is a product of transpositions, H is all of S_n [12, 175]. □

Note that if H contains an n-cycle, then H is a transitive subgroup. A weaker version of the above theorem is that if H is a subgroup of S_n containing a transposition, an $(n-1)$-cycle, and an n-cycle is all of S_n.

If we have a finite group G, we examine the action of the automorphism group of G, $\mathrm{Aut}(G)$, on the set of conjugacy classes of G. If C is a conjugacy class of G and $\alpha \in \mathrm{Aut}(G)$, then

$$\alpha \bullet C = \{\alpha(x) : x \in C\}.$$

A similar action on the set of conjugacy classes of G is induced by the Galois group of $\mathbb{Q}(\zeta_n)$ where $n = |G|$. Recall that $\mathrm{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{Q})$ is isomorphic to $(\mathbb{Z}/n\mathbb{Z})^\times$, the multiplicative group of integers modulo n. In fact, any $l \in (\mathbb{Z}/n\mathbb{Z})^\times$ is uniquely associated with $\sigma_l \in \mathrm{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{Q})$ where $\sigma_l(\zeta_n) = \zeta_n^l$ [9, 437]. Given $l \in (\mathbb{Z}/n\mathbb{Z})^\times$,

$$l \bullet C = \{x^l : x \in C\}.$$

While $l \bullet C$ need not be C, $l \bullet C$ is a conjugacy class of G. In fact, if $C(x)$ denotes the conjugacy class of $x \in G$, then $l \bullet C(x_0) = C(x_0^l)$. Take $y \in l \bullet C(x_0) = \{x^l : x \in C(x_0)\}$. Then $y = x^l$ where $x = gx_0g^{-1}$ for some $g \in G$. So

$$y = x^l = (gx_0g^{-1})^l = gx_0g^{-1}gx_0g^{-1}...gx_0g^{-1} = gx_0x_0...x_0g^{-1} = gx_0^lg^{-1} \in C(x_0^l).$$

Similarly, if $y \in C(x_0^l)$, then $y = gx_0^lg^{-1}$ for some $g \in G$. And

$$y = gx_0^lg^{-1} = gx_0...x_0g^{-1} = gx_0g^{-1}gx_0g^{-1}...gx_0g^{-1} = (gx_0g^{-1})^l$$

and since $gx_0g^{-1} \in C(x_0)$, $y = (gx_0g^{-1})^l \in l \bullet C(x_0)$. To reiterate, even though $l \bullet C(x_0)$ is the conjugacy class $C(x_0^l)$ of x_0^l, it need not be the same conjugacy class as that of x_0.

Keep in mind that we are trying to find a Galois extension that gives the group G as Galois group.

Definition 48. Given a group G, and $\mathbf{x} = (x_1, ..., x_s) \in G^s$, we say $\mathbf{x}$ is a *generating system* of G if the components $x_1, ..., x_s$ generate G ($G = \langle x_1, ..., x_s \rangle$), and the product of the components is 1 ($x_1 \cdot ... \cdot x_s = 1$). The set of all generating systems with s components for a group G is denoted $\Sigma_s(G) := \{x \in G^s \mid \langle x \rangle = G, x_1 \cdot ... \cdot x_s = 1\}$.

We want to explicitly require that each component x_i be an element of a distinct conjugacy class. Given an ordered sequence of distinct conjugacy classes $(C_1, ..., C_s)$ of G, let

$$A_G(C_1, ..., C_s) = \{(x_1, ..., x_s) \mid x_i \in C_i, x_1 \cdot ... \cdot x_s = 1\}.$$

$A_G(C_1, ..., C_s)$ can be shortened to $A(C_1, ..., C_s)$ when the group is apparent, or even to A if the selection of conjugacy classes is evident. At this point, A need not be contained in $\Sigma_s(G)$ since the x_i need not generate G. And $\Sigma_s(G)$ need not be contained in A since $\Sigma_s(G)$ makes no distinction on which s distinct conjugacy classes are used while A is restricted to a fixed selection of conjugacy classes.

Define $\mathscr{A}_s(G)$ to be the set containing all non-empty $A_G(C_1, ..., C_s)$ where the conjugacy classes $C_1, ..., C_s$ range over distinct conjugacy classes of G. Then $\Sigma_s(G)$ is contained in $\mathscr{A}_s(G)$. Finally, define $\mathscr{A}(G)$ to be the union over all s of $\mathscr{A}_s(G)$. $\mathscr{A}(G)$ then also contains the union over all s of $\Sigma_s(G)$.

Note here that $\mathrm{Aut}(G)$ still acts on $\mathscr{A}(G)$ if we define the action as follows: given $A = A_G(C_1, ..., C_s) \in \mathscr{A}(G)$ and $\alpha \in \mathrm{Aut}(G)$,

$$\alpha \bullet A = \{(\alpha(x_1), ..., \alpha(x_s)) \mid x_i \in C_i, x_1 \cdot ... \cdot x_s = 1\}$$

and in terms of the previously defined action on conjugacy classes, $\alpha \bullet A$ is given equivalently as

$$\alpha \bullet A = \{(y_1, ..., y_s) \mid y_i \in \alpha \bullet C_i, y_1 \cdot ... \cdot y_s = 1\}$$

where $y_i = \alpha(x_i)$. The major definition of this section as defined by Thompson in [9, 438] can now be given.

Definition 49. We say $A = A_G(C_1, ..., C_s)$ is *rigid* if A is nonempty, G acts transitively on A by conjugation, and $G = \langle x_1, ..., x_s \rangle$ for any given $(x_1, ..., x_s) \in A$. A finite group G is said to be *rigid* (with respect to the conjugacy classes $C_1, ..., C_s$) if there exist conjugacy classes $C_1, ..., C_s$ of G, where $s \leq 6$, such that $A_G(C_1, ..., C_s)$ is rigid [9, 438].

The last condition for A to be rigid requires that A be a generating system and $A \subseteq \Sigma_s(G)$. The

requirement by Thompson that no more than six conjugacy classes be used is due to restrictions from his method of proof. On the other hand, Matzat and Malle define rigidity from a different perspective that makes no restriction on the number of conjugacy classes. Völklein points out that the rigidity condition initially appears to be very restrictive, and especially difficult to verify in non-solvable groups. However, many examples were found by Thompson, Matzat, Malle, and others for almost simple groups, each with rigid triples of conjugacy classes. In fact, "all these results were in the case $r = 3$ (triples), as one would expect because the rigidity condition seems harder to satisfy the longer the tuple gets" [11, 237].

We will see in the example of S_n that two conjugacy classes is insufficient to generate the group, while using too many conjugacy classesmakes transitivity impossible. For Thompson, the application of rigidity is especially useful for finite non-abelian simple groups.

Before giving examples of rigid groups, we give the consequence of rigidity as established by Thompson.

Theorem 50. *Suppose G is rigid, i.e., G has conjugacy classes $C_1, ..., C_s$, $s \leq 6$, such that $A_G(C_1, ..., C_s)$ is rigid. Then there exists an integer D and a subfield K of $\mathbb{Q}(\zeta_D)$ and a Galois extension L of K such that $Gal(L/K) \cong G$ [9, 441].*

Under additional conditions, given in [7, 30] among others, G can be said to be a Galois extension over $\mathbb{Q}$. We showed above that the powers that correspond to primitive elements of $\mathrm{Gal}(\mathbb{Q}(\zeta_{|G|})/\mathbb{Q}) \cong (\mathbb{Z}/|G|\mathbb{Z})^\times$ induce an action on the conjugacy classes of G. Given a series of conjugacy classes $\mathbf{C} = (C_1, ..., C_s)$, we can extend that action to $\mathbf{C}$ and say

$$\mathbf{C}^\star := \{\mathbf{C}^n \mid n \in (\mathbb{Z}/|G|\mathbb{Z})^\times\} = \{(C_1^n, ..., C_s^n) \mid n \in (\mathbb{Z}/|G|\mathbb{Z})^\times\}.$$

The index of the kernel of this action, the set of powers that send $\mathbf{C}$ to $\mathbf{C}$, is given by the size of $\mathbf{C}^\star$ and is denoted $d(\mathbf{C})$

$$d(\mathbf{C}) = |\mathbf{C}^\star|.$$

Malle and Matzat call $d(\mathbf{C})$ the *irreducibility degree* of $\mathbf{C}$. The irreducibility degree of $\mathbf{C}$ is exactly the degree over $\mathbb{Q}$ of the field K whose extension gives G as Galois group. We are particularly interested when $d(\mathbf{C}) = 1$ since then G is realizable as a Galois group over $\mathbb{Q}$. If $d(\mathbf{C}) = 1$ and $\mathbf{C}$ is rigid, $\mathbf{C}$ is said to be *rationally rigid*.

Corollary 51. *The monster simple group, a simple group of size*

$$2^{46} \cdot 3^{20} \cdot 5^9 \cdot 7^6 \cdot 11^2 \cdot 13^3 \cdot 17 \cdot 19 \cdot 23 \cdot 29 \cdot 31 \cdot 41 \cdot 47 \cdot 59 \cdot 71$$

Table 2.1: Conjugacy Classes of S_4

K_0	$\{\text{id}\}$	$\{(1)\}$
K_1	$\{\text{all 2-cycles}\}$	$\{(a\ b)\}$
K_2	$\{\text{all products of two disjoint 2-cycles}\}$	$\{(a\ b)(c\ d)\}$
K_3	$\{\text{all 3-cycles}\}$	$\{(a\ b\ c)\} = \{(a\ c)(a\ b)\}$
K_4	$\{\text{all 4-cycles}\}$	$\{(a\ b\ c\ d)\} = \{(a\ d)(a\ c)(a\ b)\}$

is a Galois group of an extension over $\mathbb{Q}$.

This particularly surprising result is remarked on in [11, 237].

2.4 An Example with S_4

To get an idea for showing why S_n is rigid in general, we start by attempting to show that S_4 is rigid with respect to the conjugacy classes $(K_0, K_1, K_2, K_3, K_4)$. The conjugacy classes K_0, K_1, K_2, K_3, K_4 of S_4 are determined by their cycle shape and are shown in Table 2.1 where $a, b, c, d \in \{1, 2, 3, 4\}$ are distinct. To show S_4 is rigid, we must first show that $A = \{(x_0, ..., x_4)\}$, where $x_i \in K_i$ and $x_0 \cdot ... \cdot x_n = (1)$, is nonempty. To show this, we take a combinatorial approach where each conjugacy class will be examined in order to see which elements are eligible to be coordinates of something in A.

Any $(x_0, ..., x_4) \in A$ must have that $x_0 = (1)$ since it is the only element of K_0. Let x_1 be some transposition $(a\ b) \in K_1$. As an example, we will say $x_1 = (1\ 2)$.

For $x_2 \in K_2$, recall also that the products of two 2-cycles in K_2 must be products of two disjoint 2-cycles. A product of 2-cycles where the 2-cycles are not disjoint is actually contained in K_3. First consider the case where $x_2 \neq (a\ b)(c\ d)$. In other words, we are stipulating that the pair of 2-cycles chosen for x_2 not have the $x_1 = (a\ b)$ as one of the 2-cycles. In the example problem, we are not considering $x_2 = (1\ 2)(3\ 4)$ and $x_2 = (3\ 4)(1\ 2)$, but something like $(1\ 3)(2\ 4)$ and $(1\ 4)(2\ 3)$ is allowed.

Since the 2-cycles must be disjoint, they can be reordered and we conclude $x_2 = (a\ c)(b\ d)$ where c, d are now fixed. Keeping in mind that $x_0 \cdot ... \cdot x_4 = 1$, we take the product of the elements chosen so far:

$$x_0 \cdot x_1 \cdot x_2 = (a\ b)(a\ c)(b\ d).$$

Notice that the first two transpositions cannot be disjoint by our choices so far, while the second two must be disjoint. Given any last element x_4 that will be in the product, that x_4 is a 4-cycle, and it has a unique inverse that is also a 4-cycle. Then for $x_0 \cdot x_1 \cdot x_2 \cdot x_3$ to cancel with x_4, $x_0 \cdot x_1 \cdot x_2 \cdot x_3$ must be a 4-cycle. So given that $x_0 \cdot x_1 \cdot x_2 = (a\,b)(a\,c)(b\,d)$, if we add some 3-cycle $x_3 = (x\,y)(x\,z)$, it turns out that for any choice of $(x\,y)$, since $(x\,z)$ and $(x\,y)$ have x in common, exactly two out of the four choices for $(x\,z)$ give a 4-cycle.

In the case where we have required that $x_2 \neq (a\,b)(c\,d)$, there are 6 choices for $(x\,y)$, and given a choice of $(x\,y)$, there are 2 choices for $(x\,z)$ that give the desired result. Consequently, there are 12 elements of A that all have the same choice of x_1 and x_2 where x_2 has the restriction given above.

What if $x_2 = (a\,b)(c\,d)$? Then $x_0 \cdot x_1 \cdot x_2 = (c\,d)$ and adjoining x_3 still must give a 4-cycle. Our choice of $(x\,y)(x\,z)$ cannot have $(x\,y)$ or $(x\,z)$ match $(c\,d)$ because either cancellation or conjugation will result in a 2-cycle. Then $(x\,y)(x\,z)$ cannot be in the set $\{(c\,d)(a\,c),(c\,d)(c\,b),(c\,a)(c\,d),(c\,b)(c\,d)\}$.

That leaves four remaining elements of the eight in K_3, each of which gives a 4-cycle in the product $x_0 \cdot x_1 \cdot x_2 \cdot x_3$. As mentioned, for any 4-cycle $(w\,x\,y\,z)$, there is a unique 4-cycle $(w\,x\,y\,z)^{-1} = (w\,z\,y\,x)$ that is the inverse. So given x_0, x_1, x_2, x_3, $x_0 \cdot \ldots \cdot x_3$ must be a 4-cycle for the final product to be (1), and there is only one 4-cycle that will give the product equal to (1). Consequently, there are 4 elements of A that all have the same choice of x_1 and $x_2 = (a\,b)(c\,d)$.

In conclusion, there is only one choice for K_0, 6 choices for K_1, 3 choices for K_2, 4 or 12 choices for K_3 given the choice in K_2, and 1 choice for K_4. Thus there are $1 \cdot 6 \cdot 2 \cdot 12 \cdot 1 + 1 \cdot 6 \cdot 1 \cdot 4 \cdot 1 = 168$ elements in A out of the 864 elements in $(K_0, K_1, K_2, K_3, K_4)$. In particular, A is nonempty.

Clearly A is far from being empty. However, we run into problems showing that S_4 acts transitively on A. A is transitive if $S_4 \cdot a = A$ for all $a \in A$. Given an element $a \in A$, there are only $|S_4| = 24$ different elements in S_4 that can act on a. This implies that the orbit of a has size at most 24. To be transitive, the orbit of a must be all 168 elements of A, so A is not transitive and not a rigid set!

To analyze what went wrong, note that our combinatorial approach to finding x_0, x_1, x_2, x_3, x_4 such that $x_0 \cdot x_1 \cdot x_2 \cdot x_3 \cdot x_4 = 1$ demonstrates that the more conjugacy classes we choose to consider, the more ways we have of combining elements from different conjugacy classes to obtain a product equal to e_G. On the other hand, an excess of elements in A makes it manifestly impossible for A to be transitive. We now show that a more prudent selection of conjugacy classes has beneficial results.

2.5 Proof for S_n

Since $S_2 \cong \mathbb{Z}_2$, a finite abelian group, S_2 is realized as a Galois extension. Consider S_n for $n \geq 3$ and the class vector $\mathbf{C} = (K_1, K_2, K_3)$ where

$$\begin{aligned} K_1 &\quad \{\text{all 2-cycles}\} \\ K_2 &\quad \{\text{all } (n-1)\text{-cycles}\} \\ K_3 &\quad \{\text{all } n\text{-cycles}\}. \end{aligned}$$

To show $A = A_G(\mathbf{C})$ is transitive we will show every element of A is a conjugate of a fixed element of A.

Let $(x_1, x_2, x_3) \in A$. x_3 is an n-cycle and is conjugate with all elements of S_n having the same cycle shape. Without loss of generality, we will assume that $x_3 = (1 \ldots n)$ through conjugation. On the other hand, $x_1 = (i\ j)$ for some $i, j \in \{1, \ldots, n\}$. Conjugating (x_1, x_2, x_3) with a power of x_3 will maintain x_3 in the third coordinate.

However, conjugating x_1 with x_3^{1-i} gives $\left(x_3^{1-i}\right)^{-1} = x_3^{i-1}$ and

$$x_3^{1-i} \cdot x_1 \cdot x_3^{i-1} = x_3^{1-i} \cdot (i\ j) \cdot x_3^{i-1} = (x_3^{1-i}(i)\ x_3^{1-i}(j)).$$

Note that $x_3^{n-i}(i) = n$ since $x_3 = (1 \ldots n)$, so $x_3^{1-i}(i) = x_3^{n-i+1}(i) = 1$. Similarly, $x_3^{1-i}(j) = x_3^{1-i}\left(x_3^{j-i}(i)\right) = x_3^{j-i}(1) = 1 + j - i$. Then

$$x_3^{1-i} \cdot x_1 \cdot x_3^{i-1} = (1\ 1 + j - i).$$

Alternatively, we could have chosen to conjugate x_1 with a different power x_3^{1-j}:

$$x_3^{1-j} \cdot x_1 \cdot x_3^{j-1} = (1\ 1 + i - j),$$

using the same reasoning as above.

If $1 + j - i > \frac{n}{2} + 1$, then $j - i > \frac{n}{2}$ so $i - j \leq -\frac{n}{2} = n/2 \bmod n$. In that case, $1 + i - j \leq \frac{n}{2} + 1$. In either case, we can choose k to be $1 + j - i$ or $1 + i - j$ such that $2 \leq k \leq \frac{n}{2} + 1$. Consequently, without changing x_3, (x_1, x_2, x_3) can be changed such that $x_1 = (1\ k)$ with $2 \leq k \leq n/2 + 1$ through appropriate conjugation.

Furthermore, $x_1 \cdot x_2 \cdot x_3 = 1$ so $x_1 = x_1^{-1} = x_2 \cdot x_3$ and $x_3 \cdot x_1 = x_2^{-1}$. Then $x_3 \cdot x_1$ is an $(n-1)$-cycle and

$$x_3 \cdot x_1 = (1 \ldots n)(1\ k) = (1\ (k+1)\ (k+2) \ldots n) \cdot (2 \ldots k).$$

Since $(1\ (k+1)\ (k+2)\ ...\ n)\cdot(2\ ...\ k)$ must be an $(n-1)$-cycle, k must be 2 or n. With the added restriction that $k \leq n/2+1$, we conclude k is 2. Then

$$x_3 \cdot x_1 = (1\ 3\ 4\ ...\ n),$$

an $(n-1)$-cycle, and (x_1, x_2, x_3) is conjugate to

$$g(x_1, x_2, x_3)g^{-1} = ((1\ 2), (1\ 3\ 4\ ...\ n)^{-1}, (1\ ...\ n))$$

where g is one of the powers of x_3 given above.

This fact simultaneously shows two things: A is nonempty because $((1\ 2), (1\ 3\ 4\ ...\ n)^{-1}, (1\ ...\ n)) \in A$, and S_n acts transitively on A because if a is fixed in A, then for all $x \in A$, a and x are conjugate to $((1\ 2), (1\ 3\ 4\ ...\ n)^{-1}, (1\ ...\ n))$ and are thus conjugate to each other. As stated above on page 20, it is sufficient that x_1, x_2, x_3 have a transposition, an $(n-1)$-cycle, and an n-cycle to show that $\langle x_1, x_2, x_3 \rangle = S_n$. Therefore, S_n is rigid with respect to the conjugacy classes K_1, K_2, K_3 and there exists a field extension L/K with K an extension of $\mathbb{Q}$ and $\mathrm{Gal}(L/K) \cong S_n$ [7, 33].

To see if S_n is rationally rigid, consider $d(\mathbf{C}) = |\mathbf{C}^\star|$, where $\mathbf{C}^\star = \{\mathbf{C}^m \mid m \in (\mathbb{Z}/n!\mathbb{Z})^\times\} = \{(C_1^m, ..., C_s^m) \mid m \in (\mathbb{Z}/n!\mathbb{Z})^\times$. Any k-cycle taken to a power relatively prime to k results in a k-cycle. Any $m \in (\mathbb{Z}/n!\mathbb{Z})^\times$ will be relatively prime to every integer less than or equal to n. In particular, if $x_1 \in K_1$, then $x_1^m = x_1 \in K_1$, if $x_2 \in K_2$, then $x_2^m \in K_2$ since it is an $(n-1)$-cycle, and if $x_2 \in K_3$, then $x_3^m \in K_3$ because it is an n-cycle. Then $\mathbf{C}^\star = \{\mathbf{C}\}$, and $d(\mathbf{C}) = 1$, so $\mathbf{C}$ is rationally rigid. We conclude there exists an extension $L/\mathbb{Q}$ such that $\mathrm{Gal}(L/\mathbb{Q}) \cong S_n$. $\square$

Corollary 52. *A_n is the Galois group of a finite extension of $\mathbb{Q}$ for all n.*

This corollary is not immediate from the proof for S_n and requires additional work with the class vector $\mathbf{C} = (2\text{-cycles}, (n-1)\text{-cycles}, n\text{-cycles})$ and can be found in [7, 34].

Chapter 3

The Kronecker-Weber Theorem

3.1 Background

Our primary goal in this section to provide the theorems necessary for Greenberg's proof of the Kronecker-Weber theorem found in [4] and updated in [5]. We look at the size of finite fields of a given characteristic, define integral elements over a ring, the algebraic integers, and Dedekind domains. A particularly important result of this section is that the algebraic integers over a ring form a ring themselves that is a Dedekind domain. Given an ideal in the algebraic integers of a Galois extension with a Galois group G, we find specific subgroups of G that are associated with the ideal: the decomposition group, the inertia group, and the ramification groups.

The secondary goal of the section, however, is to provide some explanation for why these particular theorems are important. Why, for example, is the ring of algebraic integers in a finite extension of the rational numbers such an important ring? The unique factorization property for the integers and other unique factorization domains has a number of benefits including that every irreducible element is prime, that every element is an integral element, and that greatest common divisors and least common multiples can be defined. Our hope is to identify beneficial characteristics of the integers and generalize these characteristics so they can be applied to other domains that might not meet all the requirements to be a unique factorization domain. Among others, quadratic field extensions will be used as examples, culminating in a proof that every quadratic extension is a cyclotomic extension.

The standard definitions and theorems, as well as their proofs, for finite fields, algebraic and integral elements, and Dedekind domains can be found in [1] and [14].

3.1.1 Finite Fields

Field extensions of $\mathbb{Q}$ are, by necessity, fields containing an infinite number of elements. However, from these fields of infinite order, we will find that taking quotients with ideals can give fields with a finite number of elements. Fields of a finite number of elements are called Galois fields and some properties are given below.

Definition 53. A *Galois field* is a field containing a finite number of elements.

If F is a Galois field with order n, then we will show $nF = 0$. If $\alpha \in F$, by Lagrange's theorem, where a is the additive order of α, a must divide the order of F, or $ga = n$ for some $g \in \mathbb{Z}$. Then $n \cdot \alpha = (ga) \cdot \alpha = g(a \cdot \alpha) = 0$ so $nF = 0$. In particular, if we let 1_F be the identity of F, then $n \cdot 1_F = 0$. The least such integer n such that $n \cdot 1_F = 0_F$ is particularly important.

Definition 54. The *characteristic* of a field F is the smallest positive integer p such that $p \cdot 1_F = 0_F$, where 1_F is the identity of F, provided such a p exists. Otherwise we define the characteristic to be 0.

Proposition 55. *The characteristic of a field F is either 0 or a prime p.*

Proof. If $n = ab$ is composite and $n \cdot 1_F = 0_F$, then as in the relations above,

$$0_F = n \cdot 1_F = ab \cdot 1_F = (a \cdot 1_F)(b \cdot 1_F)$$

and since F is a field, either $a \cdot 1_F = 0_F$ or $b \cdot 1_F = 0_F$. So the characteristic of a field cannot be composite without contradicting its minimality. □

If the characteristic of a field F is p, then for all $\alpha \in F$, $p\alpha = p \cdot (1_F \alpha) = (p \cdot 1_F)\alpha = 0$. If $n \cdot 1_F = 0$, then $n \geq p$ by the minimality of p, so we can write $n = rp + q$ for some integers $r, q \in \mathbb{Z}$ where $0 \leq q < p$ by the division algorithm. Then $q \cdot 1_F = (n - rp) \cdot 1_F = n \cdot 1_F - r(p \cdot 1_F) = 0$. Again by the minimality of p, q must be 0. This shows that if $n \cdot 1_F = 0$, then the characteristic p divides n.

Recall that any field F can be written as a commutative ring with an identity $1_F \neq 0_F$ where every nonzero element has a multiplicative inverse in the ring. The integer multiples of 1_F form a subring E of F. In particular, E is the image of a mapping ϕ from $\mathbb{Z}$ to F defined by

$$n \mapsto n \cdot 1_F$$

for $n \in \mathbb{Z}$, and this mapping is a ring homomorphism because $(n+m)\cdot 1_F = n\cdot 1_F + m\cdot 1_F$, $(nm)\cdot 1_F = (n\cdot 1_F)(m\cdot 1_F)$ and $1\cdot 1_F = 1_F$. If the kernel of ϕ is zero, the characteristic of the field is 0 and the homomorphism from $\mathbb{Z}$ is an isomorphism. In that case, the ring E contains the integers $\mathbb{Z}$ and F contains a subfield isomorphic to the rationals $\mathbb{Q}$.

If F has no proper subfields, F itself is isomorphic to the rationals $\mathbb{Q}$. On the other hand, if the kernel is nonzero, p is the least positive integer contained in the kernel. If n is in the kernel, then p divides n. And if n is in $\mathbb{Z}$, then pn is in the kernel, so $\ker\phi = p\mathbb{Z}$. Taking the quotient of $\mathbb{Z}$ by the kernel $p\mathbb{Z}$ shows that $\mathbb{Z}/p\mathbb{Z}$ is isomorphic to the image of ϕ, E. In summary, a field with characteristic p has a subfield isomorphic to $\mathbb{Z}/p\mathbb{Z}$ and a field with characteristic 0 has a subfield isomorphic to $\mathbb{Q}$ [1, 510].

When the kernel of ϕ is nonzero, the image of ϕ is not only a ring but also a field since it is isomorphic to $\mathbb{Z}/p\mathbb{Z}$. We can explicitly calculate the inverses of any element of E. The ring E must be finite and it consists of the elements $0, 1_F, 2\cdot 1_F, ..., (p-1)\cdot 1_F$. Given $n\cdot 1_F \in E$, $n < p$, so n and p are relatively prime. Then there exist integers r, q such that $rn - qp = 1$. Let $r\cdot 1_F$ be the candidate for the inverse of $n\cdot 1_F$. Then $(r\cdot 1_F)(n\cdot 1_F) = rn\cdot 1_F = (1+qp)\cdot 1_F = 1_F + q(p\cdot 1_F) = 1_F$ which shows that $r\cdot 1_F$ is in fact the inverse of $n\cdot 1_F$. So we have another proof that E is a field [14, 63].

Example 56. The fields $\mathbb{Q}$ and $\mathbb{R}$ have characteristic 0.

Using the integers $\mathbb{Z}$, for any $p \neq 0$, a field of any characteristic p can be constructed since the finite field $\mathbb{Z}/p\mathbb{Z}$ has characteristic p.

One reason the characteristic of a field is important is that the characteristic has an observable effect on the order of a field.

Theorem 57. *If F is a finite field with characteristic $p \neq 0$, then the number of elements in F is a power of p.*

Proof. Let F be a finite field with characteristic $p \neq 0$. Then F contains a subfield isomorphic to $\mathbb{Z}/p\mathbb{Z}$, the image of the isomorphism that mapped an integer z to $z\cdot 1_F$. Since F is a finite field, the index n of F viewed as a field extension of $\mathbb{Z}/p\mathbb{Z}$ is finite so F is a finite, algebraic extension of $\mathbb{Z}/p\mathbb{Z}$. Then F has a basis $\{x_1, ..., x_n\}$ of size n over $\mathbb{Z}/p\mathbb{Z}$. The basis allows us to write any element of F as a unique linear combination of the form $a_1x_1 + ... + a_nx_n$ where the a_i come from $\mathbb{Z}/p\mathbb{Z}$. However, $\mathbb{Z}/p\mathbb{Z}$ is a finite field of size p, so each a_i can take on exactly p different values. Since each value of a_i gives a unique element of F, there are exactly p^n elements of F. □

A finite field of order p^n is denoted $\mathbb{F}_{p^n}$. In fact, any two finite fields of the same size are isomorphic [1, 550].

Since the size of F is p^n, p is the smallest nontrivial divisor of the size of F. $\mathbb{Z}/p\mathbb{Z}$ is a subfield of F with size p, so $\mathbb{Z}/p\mathbb{Z}$ is the smallest subfield contained in F. A field that does not contain any proper subfields is called a *prime field*. Since any subfield of an arbitrary field F contains 1_F, and thus the field $\mathbb{Z}/p\mathbb{Z}$ or $\mathbb{Q}$, the prime subfield of F must be the subfield generated by 1_F. Consequently, every field F can be written as an extension of its prime field [1, 511].

Corollary 58. *If F is a finite field consisting of m elements, and K is a finite field extension of F of degree n, then K has exactly m^n elements.*

To prove the corollary, we can use the same logic as in the proof of the theorem. Since K is a finite field extension of F of degree n, there exists a basis over F with n elements. Each coefficient of the basis elements is taken from F, a finite field with m elements, so there are m^n different combinations giving m^n distinct elements in K.

Theorem 59. *If F is a finite field with characteristic p and $|F| = p^n$, then the nonzero elements of F form a multiplicative group of size $p^n - 1$. Furthermore, the multiplicative group of a finite field is cyclic [14, 83].*

3.1.2 Algebraic Integers

The concept of integral extensions of rings is a generalization of the concept of algebraic extensions of fields. Suppose F is a subfield of a field K and let x be in K. For x to be algebraic over F, there must exist a nonzero polynomial with coefficients in F, with x as a root. We now additionally require that the nonzero polynomial be monic and we will work in rings.

Definition 60. Let R be a subring of a ring S. An element x in S is *integral* over R if x is the root of a monic, nonzero polynomial with coefficients in R. S is an *integral extension* of R if every element of S is integral over R.

The set of elements contained in the larger ring S that are integral over R is called the *integral closure* of R in S. When the integral closure of R is R, then R is said to be *integrally closed*. Furthermore, the integral closure of R in S is integrally closed in S so taking the integral closure repeatedly gives the same result as taking the integral closure once [1, 691].

We can also form a definition of algebraic that applies to rings instead of fields. An element x in S is *algebraic* over R if x is the root of a nonzero polynomial with coefficients in R. In this case, the algebraic closure of R in S forms a subring of S but not necessarily a field. If x is integral over

R, then x is algebraic over R since a monic polynomial that exists for x to be integral suffices to show x is algebraic.

The converse need not be true. For example, $3/2 \in \mathbb{Q}$ is algebraic over $\mathbb{Z}$ because $2x-3$ is a polynomial in $\mathbb{Z}[x]$ with $3/2$ as a root. However, $2x-3$ is not sufficient to show $3/2$ is integral because it is not monic. Dividing by the leading coefficient to make it monic does not help because $x-3/2$ is not a polynomial with all coefficients in $\mathbb{Z}$. However, if R is a field, the coefficients of the polynomial divided by the leading coefficient will still be in R. In general, if R and S are fields, then S is algebraic over R if and only if S is integral over R [1, 693].

The elements of an extension of $\mathbb{Q}$ which are integral over $\mathbb{Z}$ form an important ring of integral elements which we define as follows.

Definition 61. Let K be a field extension of $\mathbb{Q}$. An element $\alpha \in K$ is an *algebraic integer* if α is integral over the ring $\mathbb{Z}$. The *ring of algebraic integers* of K, also called the ring of integers in K, is the subring of elements of K integral over $\mathbb{Z}$.

$\sqrt{-1}$, $\sqrt{3}$, and $\sqrt[5]{7}$ are all algebraic integers since they are each respective roots of the monic polynomials with integer coefficients x^2+1, x^2-3 and x^5-7. We showed above that the polynomial $2x-3$ that we used to show $3/2$ is algebraic over $\mathbb{Z}$ was not sufficient to show that $3/2$ is integral over $\mathbb{Z}$, or an algebraic integer. However, it is not clear that one of the many other polynomials with $3/2$ as a root would not work instead. In other words, it is not easy to show something is not an algebraic integer based solely on the definition. We attempt to characterize the algebraic integers in the next theorem.

Theorem 62. *An element α in a field extension of $\mathbb{Q}$ is an algebraic integer if and only if α is algebraic over $\mathbb{Q}$ and its minimal polynomial has integer coefficients.*

Since every element has a single minimal polynomial, this theorem gives specific criteria to check for an algebraic integer. For example, the algebraic integers in $\mathbb{Q}$ are the integers $\mathbb{Z}$. Let $a/b \in \mathbb{Q}$ be an algebraic integer. Then $bx-a$ is a linear polynomial that evaluates to 0 at a/b. $bx-a$ is only monic if $b=1$, in which case $a/b = a \in \mathbb{Z}$ [1, 696].

$3/2$ is not an algebraic integer even though it is algebraic over $\mathbb{Z}$ because its minimal polynomial $x-3/2$ does not have integer coefficients.

Theorem 63. *Let F be a finite field extension of $\mathbb{Q}$. The ring of algebraic integers $\mathscr{D}$ in a field F is integrally closed. If K is a finite field extension of F and $\mathscr{A}$ is the ring of algebraic integers in K, then the integral closure of $\mathscr{D}$ in K is $\mathscr{A}$.*

Proof. We already have the result that the integral closure of R contained in S is integrally closed in S. Since $\mathscr{D}$ is by definition the integral closure of $\mathbb{Z}$ in F, $\mathscr{D}$ must be integrally closed in F. If $\mathscr{A}$ is the ring of algebraic integers in K, then $\mathscr{A}$ is the integral closure of $\mathbb{Z}$ in K. Consider the integral closure of $\mathscr{D}$ in K. If k is an element of the integral closure of $\mathscr{D}$ in K, then k satisfies some equation showing it is integral over $\mathbb{Z}$, we say it is *integrally dependent* over $\mathbb{Z}$, and then k is an element of $\mathscr{A}$. So the integral closure of $\mathscr{D}$ in K is contained in $\mathscr{A}$.

If k is integrally dependent over $\mathbb{Z}$, then k is the root of a monic polynomial with coefficients in $\mathbb{Z}$. Since $\mathbb{Z} \subseteq \mathscr{D}$, k is the root of a monic polynomial with coefficients in $\mathscr{D}$ and so k is integral over $\mathscr{D}$. In other words, k is in the integral closure of $\mathscr{D}$ and we conclude that $\mathscr{A}$ and the integral closure of $\mathscr{D}$ in K are equal. □

There is an important distinction to note. Just because $\mathscr{D}$ is the integral closure of $\mathbb{Z}$ in F does not mean that $\mathscr{D}$ is integrally closed in K. $\mathscr{D}$ is not necessarily the integral closure in K of $\mathbb{Z}$ so we cannot conclude that $\mathscr{D}$ is already integrally closed in K. If $\mathscr{D}$ was integrally closed in K, then $\mathscr{A}$, the integral closure of $\mathscr{D}$, would in fact be $\mathscr{D}$. $\mathscr{D}$ is contained in $\mathscr{A}$ but in general they are not equal.

We will find a well-behaved relationship between ideals in an integrally closed ring and ideals in the integral closure of that ring embedded in a larger field. In particular, letting the second ring be the integral closure of the first ring reflects the situation where the rings are identical even though the rings are different.

Example 64. The ring of algebraic integers in a cyclotomic field $\mathbb{Q}(\zeta)$, where ζ is a primitive n^{th} root of 1, is $\mathbb{Z}[\zeta]$.

The ring of algebraic integers in a quadratic extension $K = \mathbb{Q}[\sqrt{d}]$, where d is a square-free integer, is $\mathbb{Z}[\omega] = \mathbb{Z} \cdot 1 + \mathbb{Z} \cdot \omega$, where

$$\omega = \begin{cases} \sqrt{d} & \text{if } d \equiv 2,3 \bmod 4 \\ \frac{1+\sqrt{d}}{2} & \text{if } d \equiv 1 \bmod 4 \end{cases}$$

[1, 698].

When we focus on the ring of integral elements of a field extension we are simultaneously taking the elements of the ring that behave cohesively as roots of polynomials and collecting the elements of the field that are representative of the structure of the extension. In statistics, for example, when taking samples rather than surveying the entire population, it can be more efficient and, due to the smaller data set, easier to ensure the reliability of the data. Focusing on the behavior

of the integral elements faithfully reflects the structure of the field but can be much more revealing than looking at the whole field. In particular, we find that in a ring of algebraic integers, ideals decompose into a unique product of prime ideals. A domain where all ideals decompose in such a way is called a Dedekind domain.

3.1.3 Dedekind Domains, Extensions of Dedekind Domains

As we build up our machinery for working with ideals, we would like to have an environment where any given ideal can be decomposed into basic components, similar to how any element of a unique factorization domain can be written uniquely as a product of prime factors.

Definition 65. Let R be a ring. If R is an integral domain and every proper, nonzero ideal in R is a product of prime ideals, then we say R is a *Dedekind domain*.

Example 66. A principal ideal domain is a Dedekind domain. For example, $\mathbb{Z}$ is a Dedekind domain [14, 270].

Claim 67. In a Dedekind domain, the factorization into prime ideals of any ideal is unique.

Many texts give the uniqueness of the factorization as part of the definition of a Dedekind domain. Zariski's sequence of theorems shows uniqueness is automatic if factorization into prime ideals exists for all ideals [14, 273].

Theorem 68. *If R is a Dedekind domain and there are finitely many proper prime ideals in R, then R is a principal ideal domain.*

Looking ahead to taking quotients of rings with ideals, this theorem leads to the following corollary.

Theorem 69. *Let R be a Dedekind domain, K the quotient field of R, and L a finite algebraic extension of K. Then the integral closure of R in L is a Dedekind domain [14, 278].*

We want to look specifically at the ring of algebraic integers.

Corollary 70. *Let F be a field extension of $\mathbb{Q}$ that is finite. Then the ring of algebraic integers $\mathscr{D}$ in F is a Dedekind domain. Furthermore, every proper, nonzero ideal I in $\mathscr{D}$ can be written as*

$$I = \mathfrak{P}_1^{e_1} \cdot \ldots \cdot \mathfrak{P}_n^{e_n}$$

where the $\mathfrak{P}_i$ are distinct prime ideals, $e_i \geq 1$ for all i, and the e_i and $\mathfrak{P}_i$ are uniquely determined up to rearrangement.

Recall that the motivation for finding Dedekind domains includes this property that ideals have a unique factorization. As Dummit and Foote write, "the unique factorization of nonzero *ideals* into a product of prime *ideals* replaces the failure of unique factorization of nonzero *elements* into products of prime *elements* in rings of integers of number fields [finite extensions of $\mathbb{Q}$]," [1, 767]. One benefit to the integers $\mathbb{Z}$ having a unique factorization is the divisibility properties that result. We form a similar interpretation for ideals.

Definition 71. Let A, B be ideals in an integral domain R. We say B *divides* A if there exists some ideal C such that $A = BC$.

As with principal ideals, the notion of containment with ideals is the opposite of the notion of divisibility of the integers. If $r, s \in \mathbb{Z}$ and r divides s, then $r \leq s$ but this means that $s = k \cdot r$ for some $k \in \mathbb{Z}$, $s \in (r)$, and so $(s) \subseteq (r)$. This idea is very counterintuitive since divisors in the integers are supposed to be smaller than the thing they divide. For ideals A, B, if B divides A, then A is contained in B. The expression: "To contain is to divide," summarizes this seemingly backward result. Among other results, we can define a greatest common divisor of two ideals if the ideals are in a Dedekind domain.

Definition 72. The *greatest common divisor* of A and B, denoted (A, B), is the ideal that divides A and B and furthermore, if any other ideal divides A and B, that ideal divides (A, B). We say A and B are *relatively prime* if $(A, B) = R$.

Proposition 73. *If R is a Dedekind domain, and A and B are nonzero ideals in R with prime factorizations $A = I_1^{e_1} \cdot \ldots \cdot I_n^{e_n}$ and $B = I_1^{f_1} \cdot \ldots \cdot I_n^{f_n}$, then $A \subseteq B$ if and only if B divides A if and only if $f_i \leq e_i$ for all i. Also $A + B = (A, B) = I_1^{\min(e_1, f_1)} \cdot \ldots \cdot I_n^{\min(e_n, f_n)}$ and $(A, B) = R$ if and only if A and B have no prime ideals in common.*

This exemplifies the adage that to contain is to divide.

Theorem 74. *Let I be an nonzero ideal in a Dedekind domain R. Then every ideal in the quotient ring R/I is a principal ideal.*

This last theorem hints at the process of localizing an ideal and is in fact provable using localization. We include a very brief introduction.

Definition 75. If R is a commutative ring with a 1, then R is called a *local ring* if it has a unique maximal ideal.

The localization of a ring R at a prime ideal I, denoted R_I is the product of what is called the fractional ideal of I, written I^{-1}, and R. It turns out R_I maintains much of the structure of R. If R is an integral domain, then R_I is an integral domain. There is a bijective correspondence between the prime ideals in R_I and the prime ideals of R contained in I [1, 718].

If R is a discrete valuation ring, a stronger form of a Dedekind domain, then R is a principal ideal domain and it has a unique maximal ideal so it is a local ring [1, 765]. Dedekind domains have the weaker result that for any nonzero prime ideal I, the localization R_I is a discrete valuation ring and consequently a local ring, though the domain itself need not be a discrete valuation ring [1, 758]. Dedekind domains turn up more often, however. The advantage of these observations is that in the right conditions, we can associate a ring with its localization and consequently assume that ideals in the ring are principally generated like the ideals in the quotient ring.

3.2 Ramification Theory of Ideals

The majority of the definitions, theorems, and proofs regarding ramification theory of ideals can be found in [14]. The occasional proof technique or theorem is included from [6] and [13] where noted.

3.2.1 Extended and Contracted Ideals

Now we examine the relationship between ideals in a ring and ideals in a corresponding residue ring.

Given a ring R and an ideal K, we can construct a natural homomorphism from R with kernel K by mapping from R to the ring of cosets R/K sending $r \to r+K$ for $r \in R$. Furthermore, if R' is the image of a homomorphism from R with kernel K, then R' is isomorphic to R/K. We refer to R/K as the residue class ring of R (or the quotient ring of R) with respect to K and call the elements $r+K \in R/K$ residue classes. We have the following analogue of the ideal correspondence theorem:

Theorem 76. *Let R and R' be rings and let $f : R \to R'$ be a homomorphism with kernel K. There is a one-to-one inclusion preserving correspondence between the ideals I of R which contain K and the ideals I' of R' [14, 142].*

We will see that this result is significantly stronger than if we included the other ideals of R that do not contain the kernel K. If we are given two rings R and S with identities and a homomorphism $f : R \to S$ where $f(1_R) = 1_S$, we want to examine the relationship between ideals of

R, denoted $\{I_\alpha\}$, and the ideals of S, denoted $\{J_\alpha\}$. The following definitions establish a form of correspondence between the two sets of ideals.

Definition 77. If J is an ideal of S, then the ideal $J^c = f^{-1}(J)$ is an ideal of R and is called the *contraction* of J or the *contracted ideal* of J. Given an ideal I in R, the ideal generated by $f(I)$ in S, $I^e = Sf(I)$, is called the *extension* of I or the *extended ideal* of I.

I^e can also be written $I^e = \{s_1 f(i_1) + ... + s_n f(i_n) : n \text{ is an arbitrary positive integer}, s_j \in S, i_j \in I\}$.

We note the following facts from [14] to provide context:

1. $S^c = R$, $R^e = S$, $(0_S)^c = 0_R$ and $(0_R)^e = \ker f$.
2. If $J_1 \subseteq J_2$, then $J_1^c \subseteq J_2^c$. If $I_1 \subseteq I_2$ then $I_1^e \subseteq I_2^e$.
3. $J^{ce} \subseteq J$ and $I^{ec} \supseteq I$.
4. $J^{cec} = J$ and $I^{ece} = I$.
5. $(J_1 + J_2)^c \supseteq J_1^c + J_2^c$ and $(I_1 + I_2)^e = I_1^e + I_2^e$.
6. $(J_1 \cap J_2)^c = J_1^c \cap J_2^c$ and $(I_1 \cap I_2)^e \subseteq I_1^c \cap I_2^c$.
7. $(J_1 J_2)^c \supseteq J_1^c J_2^c$ and $(I_1 I_2)^e = I_1^e I_2^e$.

Example 78. Let $R = \mathbb{Z}$, $S = \mathbb{Q}$ and $f : \mathbb{Z} \to \mathbb{Q}$ be defined by $f(z) = z$ for all $z \in \mathbb{Z}$. The only ideals in $\mathbb{Q}$ are 0 and $\mathbb{Q}$. Then $5\mathbb{Z} \subset \mathbb{Z}$ is an ideal of $\mathbb{Z}$ but $(5\mathbb{Z})^e = \mathbb{Z}^e = \mathbb{Q}$. In fact, given an integral domain R and its quotient field S, if I is a nonzero ideal of R then $I^e = R^e = S$ even if $I \neq R$. Thus, even if we assume strict inclusion in the hypothesis of (2), we still cannot claim strict inclusion in the conclusions.

Not every ideal of R need be a contracted ideal of S, nor is every ideal of S necessarily an extended ideal of R. In the example, $5\mathbb{Z}$ is not a contracted ideal since it is not the preimage of either ideal of $\mathbb{Q}$: 0 and $\mathbb{Q}$. If an ideal is not a contracted or extended ideal, then strict containment holds in (3).

Conversely, if an ideal is a contracted or extended ideal, then equality holds as shown in (4). For example, in (3), if we start with the ideal $5\mathbb{Z}$ of R that is not a contraction, we have $(5\mathbb{Z})^{ec} = \mathbb{Q}^c = \mathbb{Z} \supset 5\mathbb{Z}$. However, if we start with an the ideal $\mathbb{Z}$ of R that is a contraction, $\mathbb{Z} = \mathbb{Q}^c$, then $\mathbb{Z}^{ec} = (\mathbb{Q}^c)^{ec} = \mathbb{Q}^c = \mathbb{Z}$. As Zariski-Samuel notices: "if an ideal in S is an extended ideal, it is the

Figure 3.2.1: Commutative Diagram

$$\begin{array}{ccc} R & \xrightarrow{f} & S \\ {\scriptstyle g}\downarrow & & \downarrow{\scriptstyle h} \\ R' & \xrightarrow{f'} & S' \end{array}$$

extension of its contraction, and that if an ideal in R is a contracted ideal, it is the contraction of its extension" [14, 219].

Taking advantage of the equality in (4), we let C be the set of all contracted ideals in R and we let E be the set of all extended ideals in S. The mappings $I \mapsto I^e$ and $J \mapsto J^c$ are one-to-one, onto, and inverses of each other between C and E. We reiterate, however, that if we start with an ideal I of R that is not in C, extending and then contracting I will not give I. We observe from facts (5), (6), and (7) that C and E are closed under addition, multiplication, and intersection of ideals.

Not only are these mappings bijective when restricted to C and E, but they also respect direction in a commutative diagram of two homomorphisms f and g. Let R, S, T be rings, f a homomorphism that maps R to S, and g a homomorphism that maps S to T. If I is an ideal in R, then the ideal that is the extension under g of the extension under f of I is the ideal that is the extension under $g \circ f$ of I. Similarly, if we contract under $g \circ f$ an ideal of T, we get the same ideal as when we contract under g and then again under f.

Furthermore, extensions and contractions of ideals along different paths of functions still give the same ideal. If we have the commutative diagram as in Figure 3.2.1 , where $f' \circ g = h \circ f$, then for an ideal I in R, the extension under g followed by the extension under f' is the same ideal that is the extension under f followed by the extension under h [14, 218].

3.2.2 Decomposition of Prime Ideals in Extensions of Dedekind Domains: Introduction to Ramification

We showed that if we had a ring homomorphism between two rings R and S that we were able to associate ideals in one ring with ideals in the other in a natural way through the homomorphism by looking at the extension in S of an ideal in R or the contraction in R of an ideal in S. We also found that in a Dedekind domain, every ideal is a unique product of prime ideals. Combining these two topics, we look at the decomposition of ideals in the second domain S, where S is a subextension of the quotient field of the first ring R.

The setup is as follows: let R be a Dedekind domain with quotient field K and L a finite algebraic extension of degree n of K with R' the integral closure of R in L. R', the integral closure of a Dedekind domain, is also a Dedekind domain. We compare the ideals of R, now denoted $\{\mathfrak{a},\mathfrak{b},...\}$, and the ideals of R', denoted $\{\mathfrak{A},\mathfrak{B},...\}$, through the natural inclusion homomorphism $f : R \to R'$ given by $f(r) = r$ for all $r \in R$.

So in general, for an ideal $\mathfrak{a} \subseteq R$, the extension of $\mathfrak{a}$ in R' is $\mathfrak{a}^e = R'f(\mathfrak{a}) = R'\mathfrak{a}$ and for an ideal $\mathfrak{A}$ in R', the contraction of $\mathfrak{A}$ is $\mathfrak{A}^c = f^{-1}(\mathfrak{A}) = R \cap \mathfrak{A}$. In particular, if $\mathfrak{p}$ is a proper, nonzero prime ideal of R, then the ideal $\mathfrak{p}^e = R'\mathfrak{p}$ is not necessarily a prime ideal in R', but can at least be written uniquely as a product of prime ideals

$$\mathfrak{p}^e = \prod_i \mathfrak{P}_i^{e_i}$$

where the $\mathfrak{P}_i$ are pairwise distinct and $e_i > 0$. For each $\mathfrak{P}_i$, as a product of ideals including $\mathfrak{P}_i$, $\mathfrak{p}^e$ is contained in $\mathfrak{P}_i$. $\mathfrak{p}^e \subseteq \mathfrak{P}_i$ so $\mathfrak{p} \subseteq \mathfrak{p}^{ec} \subseteq \mathfrak{P}_i^c$. Then since $\mathfrak{p}$ is nonzero, prime in a Dedekind domain, $\mathfrak{p}$ is maximal so $\mathfrak{P}_i^c = \mathfrak{p}$ or $\mathfrak{P}_i^c = R$ [14].

At this point, we would like to be able to definitely say whether $\mathfrak{P}_i^c = \mathfrak{p}$ or $\mathfrak{P}_i^c = R$. We can say that if $\mathfrak{P}$ is a prime ideal in R', then its contraction is prime in R. In general, however, a contraction of a maximal ideal need not be maximal, as evidenced by ideals that contract to be the ring R. But in a Dedekind domain, the contraction in R of a maximal ideal in S must either be maximal or R. Consequently, with integral ring extensions, contractions and extensions are much more predictable than in the general situation. In particular, maximality is maintained in contractions and extensions.

Theorem 79. *Let R be a subring of a commutative ring S and let S be integral over R. Let $\mathfrak{p}$ be a prime ideal in R. Then there exists a prime ideal $\mathfrak{P}$ in S such that $\mathfrak{p} = \mathfrak{P} \cap R$. Also, $\mathfrak{p}$ is maximal if and only if $\mathfrak{P}$ is maximal [1, 694].*

So in the above situation where $\mathfrak{p}^e = \prod_i \mathfrak{P}_i^{e_i}$, since we started with R' the integral closure of R, we know $\mathfrak{P}_i^c = \mathfrak{p}$. We call the integer e_i the *reduced ramification index* of $\mathfrak{P}_i$ over $\mathfrak{p}$.

Theorem 80. *R be a Dedekind domain, L a finite algebraic extension of the quotient field K of R, $\mathfrak{p}$ a proper prime ideal of R, R' an overring of R contained in L, and $\mathfrak{P}$ an ideal of R' such that $\mathfrak{P} \cap R = \mathfrak{p}$. Then the dimension of $R'/\mathfrak{P}$, viewed as a vector space over $R/\mathfrak{p}$, is at most $[L : K]$ [14, 285].*

When R' is the integral closure of R in L, the degree of $[R'/\mathfrak{P}_i : R/\mathfrak{p}]$ is called the *relative degree* of $\mathfrak{P}_i$ over $\mathfrak{p}$ and is denoted f_i. So, $\mathfrak{p}$ extended is a product of powers of distinct $\mathfrak{P}_i$ and each $\mathfrak{P}_i$ has a reduced ramification index e_i and a relative degree f_i.

Theorem 81. *The integer $\sum_i e_i f_i$ is equal to the dimension of the ring $R'/\mathfrak{p}^e$ when it is considered as a vector space over $R/\mathfrak{p}$. We have $\sum_i e_i f_i \leq [L:K]$. If L is a separable extension of K or if R is a finite integral domain, then $\sum_i e_i f_i = [L:K]$ [14, 287].*

Example 82. (The Gaussian integers) Consider the ring of integers $\mathbb{Z}$ and the quadratic field extension of their field of fractions $\mathbb{Q}$, given by $\mathbb{Q}(\sqrt{-1})$. Any element of $\mathbb{Q}(\sqrt{-1})$ has the form $a+ib$ for some $a,b \in \mathbb{Q}$. The integral closure of $\mathbb{Z}$ in $\mathbb{Q}(\sqrt{-1})$, which we have been referring to as the algebraic integers in $\mathbb{Q}(\sqrt{-1})$, is given by $R' = \mathbb{Z}+i\mathbb{Z}$ and is called the *ring of Gaussian integers*. The ring of Gaussian integers is also a Dedekind domain. We see that given a prime number p in the integers $\mathbb{Z}$, $\sum_i e_i f_i = 2 = [\mathbb{Q}(\sqrt{-1}):\mathbb{Q}]$ since $\mathbb{Q}(\sqrt{-1})$ is a separable extension of $\mathbb{Q}$.

Consequently, the ideal generated by the prime number p, $(p) = p\mathbb{Z}$, extended into R' has the following possible decompositions: either (a) it splits into two distinct ideals $R'(p) = \mathfrak{P}_1 \cdot \mathfrak{P}_2$ and $R'/\mathfrak{P}_1 = R'/\mathfrak{P}_2 = \mathbb{Z}/p\mathbb{Z}$, in which case it is said to be *decomposed*; (b) it is already a prime ideal $R'(p) = \mathfrak{P}$ and $[R'/\mathfrak{P} : \mathbb{Z}/p\mathbb{Z}] = 2$, in which case it is said to be *inertial*; or (c) it decomposes into a power of one prime ideal $R'(p) = \mathfrak{P}^2$ and $R'/\mathfrak{P} = \mathbb{Z}/p\mathbb{Z}$, in which case it is said to be *ramified*. We will give definitions of these terms in more general settings later.

In this case, the prime ideals which are inertial are those generated by odd primes of the form $4n-1$. Since they are inertial, their extensions are already prime and irreducible. The prime number 2 generates the only ramified prime in the extension. This is a fact we will make great use of later. The remaining primes split in the extension. For example, the ideals (3) and (7) are inertial, (2) is ramified, and (5) splits.

So far we have that if L is a separable extension of K, the sum $\sum_i e_i f_i = [L:K]$. If L is also a normal extension of K, we can say that the e_i, or the f_i, are all equal.

Theorem 83. *Let R be an integrally closed domain, and let R' be the integral closure of R in a finite normal extension L of the quotient field K of R. If $\mathfrak{p}$ is a prime ideal in R, then the prime ideals $\mathfrak{P}_i$ of R' which lie over $\mathfrak{p}$ are all images of any one of them by K-automorphisms of L.*

If, furthermore, R is a Dedekind domain, then the $\mathfrak{P}_i$ are the prime factors of $R'\mathfrak{p}$, $\mathfrak{p}$ extended in R', the integers e_i (or f_i) are all equal to the same integer e (or f) and if g is the number of prime ideals $\mathfrak{P}_i$, we have $efg \leq n = [L:K]$. If L is a separable extension of K, then $efg = n$.

This shows a surprising amount of uniformity for each ideal in R' lying over $\mathfrak{p}$. In such a case we can write

$$R'\mathfrak{p} = (\mathfrak{P}_1\mathfrak{P}_2...\mathfrak{P}_g)^e.$$

3.2.3 Decomposition Group, Ramification Group, and Inertia Group

In the following definitions, we let R be a Dedekind domain, L a finite, normal, and separable extension of K, the quotient field of R, where L contains the integral closure R' of R. Finally, we let $G = \mathrm{Gal}(L/K)$ which is possible because L is a normal and separable extension of K. We want to take advantage of the Fundamental Theorem of Galois Theory to locate subfields of L containing F and their associated subgroups in G. The majority of the following definitions and theorems, as well as their proofs, can be found in [14, 290ff].

Definition 84. Given a prime ideal $\mathfrak{p}$ of R and a prime ideal $\mathfrak{P}$ of R' that lies over $\mathfrak{p}$ (whose contraction is $\mathfrak{p}$), we define the *decomposition group* G_Z of $\mathfrak{P}$ to be the automorphisms $s \in G$ that fix $\mathfrak{P}$ (i.e. $s(\mathfrak{P}) = \mathfrak{P}$).

Each $\mathfrak{P}_i$ is an image of $\mathfrak{P}$ under an automorphism, so the size of G_Z is $|G|/g = ef$. And we have $t(\mathfrak{P}) = \mathfrak{P}'$ for some t in G. If s is in the decomposition group G_Z of $\mathfrak{P}$, then $s(\mathfrak{P}) = \mathfrak{P}$ and $t \circ s \circ t^{-1}(\mathfrak{P}') = t \circ s(\mathfrak{P}) = t(\mathfrak{P}) = \mathfrak{P}'$. Thus, the decomposition group of $\mathfrak{P}'$ is $t \circ G_Z \circ t^{-1}$, a conjugate subgroup of G_Z, the decomposition group of $\mathfrak{P}$.

The field fixed by G_Z is called the *decomposition field* of $\mathfrak{P}$ and is denoted K_Z. Since G_Z is a subgroup of G, K_Z is an extension of F that is contained in L, with L a normal and separable extension of K_Z and $\mathrm{Gal}(L/K_Z) = G_Z$. Since subgroups of G and the subfields of L maintain their associated indices with reverse inclusion, we also have that $[L : K_Z] = ef$ and $[K_Z : K] = g$.

If G is an abelian group, the extension L/K is called an *abelian extension* of K. Moreover, the decomposition group for $\mathfrak{P}$ lying over $\mathfrak{p}$ is isomorphic to the decomposition groups of every other prime ideal in R' lying over $\mathfrak{p}$. To reflect that every prime ideal lying over $\mathfrak{p}$ has the same decomposition group, we call G_Z the decomposition group of $\mathfrak{p}$ instead of the decomposition group of a specific $\mathfrak{P}$. Abelian extensions will be considered in greater detail in the proof of the Kronecker-Weber theorem.

Theorem 85. *Let K_Z be the decomposition field of the prime ideal $\mathfrak{P}$ in R', R_Z the integral closure of R in K_Z, and $\mathfrak{P}_Z = \mathfrak{P} \cap R_Z$ ($\mathfrak{P}$ contracted into R_Z). Then $\mathfrak{P}$ is the only prime ideal in R' lying over $\mathfrak{P}_Z$, its relative degree is f, and its reduced ramification index is e: so $R'\mathfrak{P}_Z = \mathfrak{P}^e$ (now e refers to taking $\mathfrak{P}$ to the eth power, not extending $\mathfrak{P}$).*

Furthermore, if the decomposition group G_Z of $\mathfrak{P}$ is a normal subgroup of G, then K_Z is a normal and separable extension of K and the factorization of $R_Z\mathfrak{p}$ in R_Z ($\mathfrak{p}$ extended into R_Z) consists of g distinct and conjugate prime factors, all of them with relative degree 1: i.e. $[R_Z/R_Z\mathfrak{p} : R/\mathfrak{p}] = 1$ and $R_Z\mathfrak{p} = \prod \mathfrak{P}_Z$.

Since the $\mathfrak{P}_Z$ in $\prod \mathfrak{P}_Z$ have exponent 1, we say the ramification index of $\mathfrak{P}$ is 1. We also have that $[R_Z/R_Z\mathfrak{p} : R/\mathfrak{p}] = 1$, so we can move to K_Z from K by splitting the extension of $\mathfrak{p}$ into g prime ideals $\mathfrak{P}_Z$ but without increasing either the ramification index or the index of the residue fields.

We showed above that we can extend the field K without changing the index of the residue fields. We now find another intermediate field and subgroup that again does not change the index of the residue field.

Definition 86. The *inertia group* G_T of a prime ideal $\mathfrak{P}$ of R' lying over $\mathfrak{p}$ is the group of automorphisms $s \in G$ such that $s(x) \equiv x \pmod{\mathfrak{P}}$ (i.e. $s(x) \in x + \mathfrak{P}$) for every $x \in R'$.

Given $s \in G_T$ and $x \in \mathfrak{P}$,

$$s(x) \in x + \mathfrak{P} = \mathfrak{P}$$

so $s(\mathfrak{P}) \subseteq \mathfrak{P}$. Also, $s^{-1} \in G_T$ and

$$s^{-1}(x) \in x + \mathfrak{P} = \mathfrak{P}$$

so $s^{-1}(\mathfrak{P}) \subseteq \mathfrak{P}$ and thus $\mathfrak{P} \subseteq s(\mathfrak{P})$. We conclude that $s(\mathfrak{P}) = \mathfrak{P}$ and $s \in G_Z$, the decomposition group of $\mathfrak{P}$, because s fixes $\mathfrak{P}$. The inertia group G_T is contained in the decomposition group G_Z.

Now given $s \in G_T$, $t \in G_Z$, and $x \in R'$, we have $t^{-1}(x) \in R'$ so by definition of s, $s(t^{-1}(x)) \equiv t^{-1}(x)$. Then $s \circ t^{-1}(x) - t^{-1}(x) \in \mathfrak{P}$ and

$$t \circ s \circ t^{-1}(x) - x = t \circ (s \circ t^{-1}(x) - t^{-1}(x)) \in t(\mathfrak{P}) = \mathfrak{P}.$$

We conclude that $t \circ s \circ t^{-1} \in G_T$ because $t \circ s \circ t^{-1}(x) = x + \mathfrak{P}$. So we have shown that G_T is a normal subgroup of G_Z because $t \circ G_T \circ t^{-1} = G_T$ for all t in G_Z.

The associated field for G_T is denoted K_T, and

$$K \subseteq K_Z \subseteq K_T \subseteq L,$$

L is a normal and separable extension of K_T with $\mathrm{Gal}(L/K_T) = G_T$ and K_T is a normal and separable extension of K_Z with $\mathrm{Gal}(K_T/K_Z) = G_Z/G_T$. We summarize this in the following theorem:

Theorem 87. *Let K_Z and K_T be the decomposition and inertia fields of the prime ideal $\mathfrak{P}$, R_Z the integral closure of R in K_Z, R_T the integral closure of R in K_T, and $\mathfrak{P}_Z$ and $\mathfrak{P}_T$ the contracted ideals $\mathfrak{P} \cap R_Z$ and $\mathfrak{P} \cap R_T$. Then $R'/\mathfrak{P}$ is a normal extension of $R/\mathfrak{p}$, and its Galois group is isomorphic to G_Z/G_T.*

If $f = f_0 p^s$, where f_0 is the degree over $R/\mathfrak{p}$ of the maximal separable extension of $R/\mathfrak{p}$ in $R'/\mathfrak{P}$ and where p is the characteristic of $R/\mathfrak{p}$, then K_T is a normal and separable extension of K_Z, of degree f_0, and $\mathfrak{P}_T$ is the only prime ideal of R_T lying over $\mathfrak{P}_Z$ and it has relative degree f_0 and reduced ramification index 1 (so $\mathfrak{P}_Z R_T = \mathfrak{P}_T$).

We have $R/\mathfrak{p} = R_Z/\mathfrak{P}_Z$, and $R_T/\mathfrak{P}_T$ is the maximal separable extension of $R/\mathfrak{p}$ in $R'/\mathfrak{P}$. The field L is a normal and separable extension of K_T, of degree ep^s, $\mathfrak{P}$ is the only prime ideal of R' lying over $\mathfrak{P}_T$, and it has relative degree p^s over $\mathfrak{P}_T$ and reduced ramification index e (so $\mathfrak{P}_T R' = \mathfrak{P}^e$).

Furthermore, if $R'/\mathfrak{P}$ is a separable extension of $R/\mathfrak{p}$, then $R'/\mathfrak{P} = R_T/\mathfrak{P}_T$, $[L : K_T] = e$, and the relative degree of $\mathfrak{P}$ over $\mathfrak{P}_T$ is 1.

$R'/\mathfrak{P}$ is not necessarily a separable extension of $R/\mathfrak{p}$. When R is a ring of algebraic integers, however, the extension is separable, and we will use this fact later.

Given our field extension L/K, we found that the degree of L over K is given by the product of e, the reduced ramification index of $\mathfrak{P}$ over $\mathfrak{p}$; f, the relative degree of $\mathfrak{P}$ over $\mathfrak{p}$; and g, the number of prime ideals lying over $\mathfrak{p}$. The factor g turned out to be the degree of the extension given by the intermediate field K_Z over K. The remaining ef factors into f_0 and ep^s where f_0 is the degree of another intermediate field K_T over K_Z and ep^s is the degree of L over K_T. The degree $f_0 = [K_T : K_Z]$ is called the reduced relative degree of $\mathfrak{P}$ over $\mathfrak{p}$ and is a factor of f, the relative degree of $\mathfrak{P}$ over $\mathfrak{p}$. The degree $ep^s = [L : K_Z]$ is called the ramification index of $\mathfrak{P}$ over $\mathfrak{p}$ and the reduced ramification index e is a factor of the ramification index. When a prime ideal $\mathfrak{P}$ of R' has ramification index greater than 1, we say $\mathfrak{P}$ is ramified.

If $R'/\mathfrak{P}$ is separable over $R/\mathfrak{p}$, then $f_0 = f$ and $p^s = 1$. Then the ramification index and the reduced ramification index of $\mathfrak{P}$ over $\mathfrak{p}$ are both e. Similarly, the relative degree and the reduced relative degree of $\mathfrak{P}$ over $\mathfrak{p}$ are both f.

So far, two subgroups can be found in the Galois group, each explicitly related to the prime ideal $\mathfrak{P}$. The decomposition group of $\mathfrak{P}$ is the group of automorphisms contained in G that mapped $\mathfrak{P}$ to $\mathfrak{P}$. The automorphisms in the inertia group not only map $\mathfrak{P}$ to $\mathfrak{P}$ but limit the image of an element $x \in R'$ to be different from x only by a factor in $\mathfrak{P}$. Automorphisms that only allow the image of an element x to be different from x by a factor in $\mathfrak{P}^2$ would further restrict the potential range of x. We generalize this concept by defining such a collection of automorphisms for any power of $\mathfrak{P}$.

Definition 88. For $n \geq 1$, the group of automorphisms s in G such that $s(x) \equiv x \pmod{\mathfrak{P}^n}$ for every x in R' is called the *n-th ramification group* of $\mathfrak{P}$ over $\mathfrak{p}$ and is denoted G_{V_n}.

Note that $G_{V_1} = G_T$ and the subgroups G_{V_n} form a decreasing sequence of subgroups contained in G. Since $\bigcap_{i=1}^{\infty} \mathfrak{P}_i = 0$, the intersection of the G_{V_n} must be the identity function. And since G is a finite group, G_{V_n} is reduced to the identity for n large enough since there are only a finite number of distinct subgroups of G and, *a fortiori*, a finite number of distinct G_{V_n}. We call n such that $G_{V_{n+1}} \subsetneq G_{V_n}$ the ramification numbers of $\mathfrak{P}$ over $\mathfrak{p}$.

G_{V_n} is shown to be normal in G_Z by taking $s \in G_{V_n}$, $t \in G_Z$ and $x \in R'$. $t^{-1}(x) \in R'$ and since $s \in G_{V_n}$, then $s(t^{-1}(x)) = t^{-1}(x) \pmod{\mathfrak{P}^n} = t^{-1}(x) + p$ for some $p \in \mathfrak{P}^n$. Then

$$st^{-1}(x) - t^{-1}(x) = (t^{-1}(x) + p) - t^{-1}(x) = p \in \mathfrak{P}^n$$

and applying t gives

$$tst^{-1}(x) - x = t(st^{-1}(x) - t^{-1}(x)) = t(p) \in \mathfrak{P}^n.$$

Therefore $tst^{-1}(x) \equiv x \pmod{\mathfrak{P}^n}$ and thus $tst^{-1} \in G_{V_n}$. We conclude that the ramification group G_{V_n} is a normal subgroup of G_Z [14, 294].

Greenberg suggests an alternate but equivalent definition of G_{V_n}.

Definition 89. Consider that $s \in G_Z$ induces an automorphism $s_n : R'/\mathfrak{P}^n \to R'/\mathfrak{P}^n$ defined by $s_n(x + \mathfrak{P}^n) = s(x) + \mathfrak{P}^n$ for $x \in R'$. Then the mapping θ where $s \mapsto s_n$ is a homomorphism of G_Z, and G_{V_n} is defined as its kernel [4, 602].

We have immediately that as the kernel of a homomorphism of G_Z, G_{V_n} is a normal subgroup of G_Z. We need to show $\ker\theta$ gives the same group as the previous definition of G_{V_n}. Fix s in the kernel of θ and x in R'. Since $s \in \ker\theta$, $s_n \equiv \theta(s) = \mathrm{id}$ and

$$x + \mathfrak{P}^n = s_n(x + \mathfrak{P}^n) = s(x) + \mathfrak{P}^n$$

so $s(x) \equiv x \pmod{\mathfrak{P}^n}$. Therefore, $\ker\theta \subseteq G_{V_n}$. For $s \in G_{V_n}$, given $x + \mathfrak{P}^n$, $s(x) \equiv x \pmod{\mathfrak{P}^n}$ so $s(x) = x + p$ for $p \in \mathfrak{P}^n$. Then

$$s_n(x + \mathfrak{P}^n) = s(x) + \mathfrak{P}^n = x + p + \mathfrak{P}^n = x + \mathfrak{P}^n$$

and $s_n = \mathrm{id}$. We conclude $s \in \ker\theta$ so $\ker\theta = G_{V_n}$ and the definitions match.

The first definition shows the relationship between the decomposition group, the inertia group and the ramification groups from the standpoint of how an automorphism in one of these groups

affects an element of R' in relation to $\mathfrak{P}$. On the other hand, the second definition emphasizes the relationship between automorphisms of R' and automorphisms of the field $R'/\mathfrak{P}^n$ and has the advantage that showing G_{V_n} is normal in G_Z is an easy consequence.

Recall that G_Z and G_T formed a quotient group G_Z/G_T that is the Galois group of $R'/\mathfrak{P}$ over $R/\mathfrak{p}$. Since G_{V_n} is normal in G_Z, it is natural to look at the quotient groups $G_{V_i}/G_{V_{i+1}}$ in G_Z.

Theorem 90. *The factor groups $G_{V_n}/G_{V_{2n-1}}$ are abelian and the groups $G_{V_n}/G_{V_{n+1}}$ are also abelian for $n \geq 2$. The groups $G_1 = G_T/G_{V_2}$ and $G_n = G_{V_n}/G_{V_{n+1}}$ for $n \geq 2$ contain normal subgroups G_1' and G_n' with orders a power of the characteristic p of $R/\mathfrak{p}$. Furthermore, the factor group G_1/G_1' is isomorphic to a multiplicative subgroup of $R'/\mathfrak{P}$, and is thus cyclic. Similarly, the factor groups G_n/G_n' for $n \geq 2$ are isomorphic to additive subgroups of $R'/\mathfrak{P}$.*

And if $R'/\mathfrak{P}$ is separable over $R/\mathfrak{p}$, then the subgroups G_1' and G_n' are reduced to the identity.

We have already shown that the multiplicative group of a finite field is cyclic, so multiplicative subgroups of a finite field will also be cyclic.

Proof. Localizing, described on page 36, we assume that $\mathfrak{P}$ is a principal ideal: $\mathfrak{P} = (\pi)$. Since on one hand we need to map into the multiplicative group of $R'/\mathfrak{P}$ and on the other we need to map into an additive subgroup of $R'/\mathfrak{P}$, we begin by considering G_1 and G_n for $n \geq 2$ in different cases.

Given that an automorphism s is in G_T, we see what s does with the generator of $\mathfrak{P}$ as the argument. Since $\pi \in \mathfrak{P}$, $s(\pi) \in \mathfrak{P} = R'\pi$. Elements of $\mathfrak{P}$ have the form $r\pi$ for some $r \in R'$. Do there exist further conditions on r? Given any element t in G_Z, $t(\mathfrak{P}) = \mathfrak{P}$ by definition and in general, $t(\mathfrak{P}^n) = \mathfrak{P}^n$. In this case, $s^{-1} \in G_T \subseteq G_Z$ and $s^{-1}(\mathfrak{P}^2) \subseteq \mathfrak{P}^2$ because

$$s^{-1}(a_1b_1 + \ldots + a_nb_n) = s^{-1}(a_1)s^{-1}(b_1) + \ldots + s^{-1}(a_n)s^{-1}(b_n) \in \mathfrak{P}^2$$

for $a_1, b_1 \in \mathfrak{P}$. Replacing s^{-1} with s we get $s(\mathfrak{P}^2) \subseteq \mathfrak{P}^2$ which implies $\mathfrak{P}^2 \subseteq s^{-1}(\mathfrak{P}^2)$. So $s^{-1}(\mathfrak{P}^2) = \mathfrak{P}^2$.

Now, if $s(\pi) = r\pi$ for some $r \in R'$ and r is an element of $\mathfrak{P}$, then $s(\pi)$ is an element of $\mathfrak{P}^2$. Applying s^{-1} gives $\pi = s^{-1}s(\pi) \in \mathfrak{P}^2$ since $s^{-1}(\mathfrak{P}^2) = \mathfrak{P}^2$. Apparently, π is an element of $\mathfrak{P}^2$ but π generates $\mathfrak{P}$ itself, which is a contradiction. We conclude that $s(\pi) \notin \mathfrak{P}^2$ and we can therefore write

$$s(\pi) = r_s\pi$$

for some $r_s \in R'$ where r_s is not in $\mathfrak{P}$. We include the subscript to emphasize that r_s is dependent on the automorphism s and can differ with other automorphisms.

On the other hand, consider what becomes of $r_s \in R'$ when the quotient of R' by $\mathfrak{P}$ is taken. We went out of our way to ensure that r_s not be in $\mathfrak{P}$ and now, when we take the quotient, the residue of r_s modulo $\mathfrak{P}$ will be nonzero. In the residue field $R'/\mathfrak{P}$, the residue of r_s, $r_s + \mathfrak{P}$, is denoted $\bar{r}_s$. Any given s in G_T has an associated $\bar{r}_s \in R'/\mathfrak{P}$. This mapping from G_T to $R'/\mathfrak{P}$ will induce the automorphism from G_T/G_{V_1} into the multiplicative group of $R'/\mathfrak{P}$.

To see this, first consider the mapping $s \mapsto \bar{r}_s$ from G_T to $R'/\mathfrak{P}$. We show this mapping is a homomorphism. Consider $\bar{r}_s$ and $\bar{r}_t$ where s and t automorphisms in G_T.

$$st(\pi) = s(r_t\pi) = s(r_t)s(\pi) = s(r_t)r_s\pi$$

so

$$r_{st} = s(r_t)r_s.$$

Moreover, since $s \in G_T$, $s(r_t) = r_t \pmod{\mathfrak{P}}$ by definition of G_T. So

$$r_{st} \equiv r_t r_s \pmod{\mathfrak{P}}$$

and consequently,

$$\bar{r}_{st} = \bar{r}_s\bar{r}_t.$$

We have shown that the mapping $s \mapsto \bar{r}_s$ is a homomorphism from G_T into $\bar{K}\backslash 0$.

Let the kernel of this mapping be denoted H_1. H_1 is the group of elements s in G_T such that $r_s \equiv 1 \pmod{\mathfrak{P}}$. We claim that the kernel is equivalently given by the set of s in G_T such that $s(\pi) - \pi \in \mathfrak{P}^2$. Given s such that $s(\pi) - \pi \in \mathfrak{P}^2$, $s(\pi) - \pi$ can be written as a finite sum of the form

$$s(\pi) - \pi = a_1b_1 + ... + a_nb_n$$

where $a_i, b_i \in \mathfrak{P}$. Each $a_i, b_i \in \mathfrak{P}$ means $a_i = c_i\pi$ and $b_i = d_i\pi$ for some $c_i, d_i \in R'$. Replacing the a_i and b_i gives

$$s(\pi) - \pi = (c_1\pi)(d_1\pi) + ... + (c_n\pi)(d_n\pi)$$

and after moving π to the right hand side,

$$s(\pi) = (c_1\pi)(d_1\pi) + ... + (c_n\pi)(d_n\pi) + \pi = (c_1\pi d_1 + ... + c_n\pi d_n + 1)\pi.$$

As the coefficient of π, we find $r_s = c_1\pi d_1 + ... + c_n\pi d_n + 1$ and

$$r_s = c_1\pi d_1 + ... + c_n\pi d_n + 1 \equiv 1 \pmod{\mathfrak{P}}$$

since $c_i\pi d_i \in \mathfrak{P}$ for all i.

Alternatively, say we start with $s \in G_T$ such that $r_s \equiv 1 \pmod{\mathfrak{P}}$. Then

$$r_s = 1 + b = 1 + r\pi$$

for some $b \in \mathfrak{P}$ where $b = r\pi$ for some $r \in R$. And

$$s(\pi) = r_s\pi = (1 + r\pi)\pi = \pi + r\pi^2$$

which means

$$s(\pi) - \pi = r\pi^2 \in \mathfrak{P}^2.$$

To summarize our results so far, we have proved that the mapping $s \mapsto \bar{r}_s$ is a homomorphism of G_T into the multiplicative subgroup of $R'/\mathfrak{P}$ with kernel H_1, the group of automorphisms s such that $s(\pi) - \pi \in \mathfrak{P}^2$. Before further characterizing the kernel H_1, we find a similar kernel of G_{V_n} for $n \geq 2$.

For s in G_{V_n} ($n \geq 2$), s has the property that $s(x) \equiv x \pmod{\mathfrak{P}^n}$ for all $x \in R'$. In particular,

$$s(\pi) \equiv \pi \pmod{\mathfrak{P}^n} \text{ and therefore } s(\pi) - \pi \in \mathfrak{P}^n.$$

As before, we can write $s(\pi) - \pi$ of the form

$$s(\pi) - \pi = y_s\pi^n$$

where y_s is in R'. $s \mapsto \bar{y}_s$ is a mapping from G_{V_n} to $R'/\mathfrak{P}$ and it will be shown next that it is a homomorphism of an additive group.

Given s and t in G_{V_n}, $s(\pi) - \pi = y_s\pi^n$ and $t(\pi) - \pi = y_t\pi^n$. Then

$$y_{st}\pi^n = st(\pi) - \pi = s(y_t\pi^n + \pi) - \pi = s(y_t)s(\pi^n) + s(\pi) - \pi = s(y_t)s(\pi)^n + s(\pi) - \pi$$

$$= s(y_t)\,(y_s\pi^n + \pi)^n + (y_s\pi^n + \pi) - \pi = s(y_t)\,(y_s\pi^n + \pi)^n + y_s\pi^n.$$

If we factor out a π^n on the right to cancel with the one on the left, we get

$$y_{st}\pi^n = s(y_t)\,(y_s\pi^n+\pi)^n + y_s\pi^n = s(y_t)\left((y_s\pi^{n-1}+1)\cdot\pi\right)^n + y_s\pi^n = s(y_t)\left(y_s\pi^{n-1}+1\right)^n\cdot\pi^n + y_s\pi^n$$

$$= \left(s(y_t)\left(y_s\pi^{n-1}+1\right)^n + y_s\right)\cdot\pi^n$$

so

$$y_{st} = s(y_t)\left(y_s\pi^{n-1}+1\right)^n + y_s.$$

Since $n \geq 2$, π^{n-1} is defined.

Using the binomial formula, we can expand $\left(y_s\pi^{n-1}+1\right)^n$ to be

$$\left(y_s\pi^{n-1}+1\right)^n = \binom{n}{0}\cdot\left(y_s\pi^{n-1}\right)^n + \binom{n}{1}\cdot\left(y_s\pi^{n-1}\right)^{n-1} + \ldots + \binom{n}{n-1}\cdot\left(y_s\pi^{n-1}\right)^1 + \binom{n}{n}\cdot\left(y_s\pi^{n-1}\right)^0$$

but we need only note that every term is an element of $\mathfrak{P}$ except the final term. Using this, combined with the fact that $s(y_t) \equiv y_t \pmod{\mathfrak{P}^n}$,

$$y_{st} \equiv y_t + y_s \pmod{\mathfrak{P}}$$

and equivalently that

$$\bar{y}_{st} = \bar{y}_t + \bar{y}_s$$

as desired. It follows that the mapping $s \mapsto \bar{y}_s$ is a homomorphism of G_{V_n} into an additive subgroup of $R'/\mathfrak{P}$. The kernel of this mapping, H_n, is the group of all automorphisms $s \in G_{V_n}$ such that $\bar{y}_s = 0$ or $y_s \equiv 0 \pmod{\mathfrak{P}^n}$. As with H_1, another description is that H_n is the set of automorphisms s in G_{V_n} such that $s(\pi) - \pi \in \mathfrak{P}^{n+1}$.

At this point in the proof, we still need to find G_1' and G_n'. Automorphisms s in G_{V_2} have that

$$s(x) \equiv x \pmod{\mathfrak{P}^2}$$

for all $x \in R'$, π in particular, so $s(\pi) - \pi \in \mathfrak{P}^2$. If follows that G_{V_2} is contained in H_1. Similarly, $G_{V_{n+1}}$ is contained in H_n.

Characterizing the kernels as the automorphisms s such that $s(\pi) - \pi \in \mathfrak{P}^{n+1}$ helps show the connection between the kernels and the $(n+1)$th ramification group. The kernel has the weaker condition that the property needs to hold true for the specific element π while the property needs to hold true for all x in R' to be in the $(n+1)$th ramification group. We will see that if the property holds true for π, it does hold for all $b \in \mathfrak{P}$, but not necessarily for all $x \in R'$.

Judging by the statement of the theorem, G_{V_2} and $G_{V_{n+1}}$ should only be H_1 and H_n provided $R'/\mathfrak{P}$ is a separable extension of $R/\mathfrak{p}$. It is not guaranteed that $H_1 = G_{V_2}$ and $H_n = G_{V_n}$, but we know there exists H_1 and H_n such that the quotient group G_T/H_1 is isomorphic to a multiplicative subgroup of $R'/\mathfrak{P}$ and the quotient group G_{V_n}/H_n is isomorphic to an additive subgroup of $R'/\mathfrak{P}$.

From now on, results for $G_T = G_{V_1}$ are combined into the general G_{V_n}, $n \geq 1$ case. Consider the factor group $G_{V_n}/G_{V_{n+1}}$ for $n \geq 1$. $G_{V_n}/G_{V_{n+1}}$ has subgroup $H_n/G_{V_{n+1}}$ and

$$\frac{G_{V_n}/G_{V_{n+1}}}{H_n/G_{V_{n+1}}} \cong G_{V_n}/H_n$$

which is isomorphic to an additive subgroup of $R'/\mathfrak{P}$ (or multiplicative in the case of $n = 1$). Then $G'_1 = H_1/G_{V_2}$ and $G'_n = H_n/G_{V_{n+1}}$.

It remains to be seen that G'_1 and G'_n will have orders that are powers of the characteristic p of $R'/\mathfrak{P}$. Let s be an automorphism in G_{V_n} for $n \geq 1$ such that s is in H_n, or

$$s(\pi) - \pi \in \mathfrak{P}^{n+1}.$$

We have characterized what s does to π and now we expand the input to all of $\mathfrak{P}$. Given $b \in \mathfrak{P}$, $b = r\pi$ for some r in R' and

$$s(b) - b = s(r\pi) - r\pi = s(r)s(\pi) - r\pi.$$

Adding in $0 = -s(r)\pi + s(r)\pi$ allows us to collect similar terms.

$$s(b) - b = s(r)s(\pi) - s(r)\pi + s(r)\pi - r\pi = s(r)\left(s(\pi) - \pi\right) + \left(s(r) - r\right)\pi.$$

We examine each summand. Since s is in the kernel H_n, $s(\pi) - \pi \in \mathfrak{P}^{n+1}$ and so $s(r)\left(s(\pi) - \pi\right) \in \mathfrak{P}^{n+1}$. Since s is in G_{V_n}, $s(r) \equiv r \pmod{\mathfrak{P}^n}$ so $s(r) - r \in \mathfrak{P}^n$ and thus $\left(s(r) - r\right)\pi \in \mathfrak{P}^{n+1}$. Therefore

$$s(b) - b = s(r)\left(s(\pi) - \pi\right) + \left(s(r) - r\right)\pi \in \mathfrak{P}^{n+1}.$$

In other words, the fact that $s(\pi) - \pi \in \mathfrak{P}^{n+1}$ is sufficient to show that $s(b) - b \in \mathfrak{P}^{n+1}$ for all $b \in \mathfrak{P}$.

Can the same be said for any $x \in R'$? Not necessarily, but it is true for s^p and $x \in R'$. This will show that s has order p in $H_n/G_{V_{n+1}}$. Take any x in R'. Recall that s is an automorphism in G_{V_n}

such that $s(\pi) - \pi \in \mathfrak{P}^{n+1}$. We immediately have that $s(x) \equiv x \pmod{\mathfrak{P}^n}$ since $s \in G_{V_n}$.

$$s(x) \equiv x \pmod{\mathfrak{P}^n} \implies s(x) - x \in \mathfrak{P}^n$$

and $s(x) - x = b$ for some $b \in \mathfrak{P}^n$. Consider $s^p(x) - x$. Our goal is to show s^p is an element of $G_{V_{n+1}}$ by showing $s^p(x) - x \in \mathfrak{P}^{n+1}$.

While we know little about s^p, we know a lot about s, in particular that $s(x) - x \in \mathfrak{P}^n$. We add in extra terms to $s^p(x) - x$ to include the term $s(x) - x$:

$$s^p(x) - x = s^p(x) - s^{p-1}(x) + s^{p-1}(x) + \ldots - s(x) + s(x) + x$$

$$= s^{p-1}(s(x) - x) + s^{p-2}(s(x) - x) + \ldots + s(s(x) - x) + (s(x) - x).$$

The final term $s(x) - x$ is in $\mathfrak{P}^{n+1}$, but what about $s^{p-i}(s(x) - x)$? It has been established above that if restricted to $b \in \mathfrak{P}$, $s(b) \equiv b \in \mathfrak{P}^{n+1}$ and since $s(x) - x = b \in \mathfrak{P}^n$, $s(x) - x = b \in \mathfrak{P}$. Then

$$s(s(x) - x) = s(b) \equiv b \pmod{\mathfrak{P}^{n+1}} = s(x) - x \pmod{\mathfrak{P}^{n+1}}.$$

The equivalence $s(b) \equiv b \pmod{\mathfrak{P}^{n+1}}$ is particularly important. It implies $s(b) - b \in \mathfrak{P}^{n+1}$ and thus $s(b) - b \in \mathfrak{P}$ and we repeat the process with $s(b) - b$ instead of b.

$$s^2(b) - s(b) = s(s(b) - b) \equiv s(b) - b \pmod{\mathfrak{P}^{n+1}}.$$

Then using the identity $s(b) \equiv b \pmod{\mathfrak{P}^{n+1}}$, we find

$$s^2(b) \equiv 2s(b) - b \pmod{\mathfrak{P}^{n+1}} = 2b - b \pmod{\mathfrak{P}^{n+1}} = b \pmod{\mathfrak{P}^{n+1}}.$$

In general, $s^{p-i}(b) \equiv b \pmod{\mathfrak{P}^{n+1}}$.

The complicated formula for $s^p(x) - x$ becomes

$$s^p(x) - x = s^{p-1}(s(x) - x) + s^{p-2}(s(x) - x) + \ldots + s(s(x) - x) + (s(x) - x)$$

$$= s^{p-1}(b) + s^{p-2}(b) + \ldots + s(b) + b \equiv b + b + \ldots + b + b \pmod{\mathfrak{P}^{n+1}} = pb \pmod{\mathfrak{P}^{n+1}}.$$

We know $b \in \mathfrak{P}^n$. p is the characteristic of $R'/\mathfrak{P}$ so $0 + \mathfrak{P} = p(1 + \mathfrak{P}) = p + \mathfrak{P}$ and thus $p \in \mathfrak{P}$. Then $pb \in \mathfrak{P}^{n+1}$ which implies that $s^p(x) - x \in \mathfrak{P}^{n+1}$ or $s^p(x) \equiv x \pmod{\mathfrak{P}^{n+1}}$ as desired. This is true for all $x \in R'$, which shows that s^p is in $G_{V_{n+1}}$.

To summarize, given s in the kernel H_n, s^p is in $G_{V_{n+1}}$ which is a subgroup of H_n. Any s in the factor group $H_n/G_{V_{n+1}}$ has that s^p is the identity function so every element of $G'_n = H_n/G_{V_{n+1}}$ has order p and the order of G'_n is a power of p. This proves the theorem in the general case.

If the stipulation that $R'/\mathfrak{P}$ be separable over $R/\mathfrak{p}$ is added, it needs to shown that $H_n = G_{V_{n+1}}$ for $n \geq 1$. In the earlier part of the proof, it was shown that for all $b \in \mathfrak{P}$, $s \in H_n$ implied that $s(b) - b \in \mathfrak{P}^{n+1}$. But $s(x) - x$ was not necessarily in $\mathfrak{P}^{n+1}$ for all x in R'. To show that $H_n = G_{V_{n+1}}$ with the additional assumption, we need to show $s(x) - x$ is necessarily in $\mathfrak{P}^{n+1}$. If $R'/\mathfrak{P}$ is separable over $R/\mathfrak{p}$, $R'/\mathfrak{P}$ and $R_T/\mathfrak{P}_T$ of the inertia group are equal (see on page 43).

Given $x \in R'$,

$$x + \mathfrak{P} = y + \mathfrak{P}_T$$

for some $y \in R_T$. Equivalently,

$$x = y + b$$

for $b = b_1 + b_T \in \mathfrak{P}$ where $b_1 \in \mathfrak{P}$ and $b_T \in \mathfrak{P}_T$. Then

$$s(x) - x = s(y+b) - (y+b) = s(y) - y + s(b) - b.$$

$s(y) = y$ since $s \in H_n \subseteq G_T$ so s fixes elements of R_T. And $s(b) - b \in \mathfrak{P}^{n+1}$ so

$$s(x) - x = s(y) - y + s(b) - b = s(b) - b \in \mathfrak{P}^{n+1}.$$

So $H_n = G_{V_{n+1}}$ as required. □

One example where $R'/\mathfrak{P}$ is separable over $R/\mathfrak{p}$ is when $R'/\mathfrak{P}$ is a field of characteristic 0. In this case, not only are G'_1 and G'_n reduced to the identity but G_{V_n} itself is reduced to the identity for $n \geq 2$. In other words, the only distinct subgroups of G based on $\mathfrak{P}$ are the decomposition group G_Z and the inertia group G_T.

Theorem 91. *Let R be a Dedekind domain with integral closure R' in a finite, algebraic, separable extension K' of the quotient field K of R. Then there are only finitely many ramified prime ideals [14, 303].*

Let F be a finite extension of $\mathbb{Q}$ of degree n. There exists at least one prime ramified in F [6, 120].

Weiss gives the equivalent statement that there does not exist unramified extensions of $\mathbb{Q}$. This theorem is often refered to as Minkowski's Theorem.

We conclude this section with a proof that quadratic extensions of $\mathbb{Q}$ are cyclotomic extensions.

Theorem 92. *Every quadratic extension $\mathbb{Q}(\sqrt{\pm p})$, where p is a prime integer, is contained in an extension of $\mathbb{Q}$ obtained by adjoining roots of unity.*

Proof. The most common method for proving this theorem uses discriminants. Given the quadratic extension $\mathbb{Q}\left(\sqrt{p}\right)$, one considers the field given by adjoining the pth roots of unity, $\mathbb{Q}(\zeta_p)$. The Galois group $G = \mathrm{Gal}(\mathbb{Q}(\zeta_p)/\mathbb{Q})$ is cyclic of order $p-1$ and has a unique subgroup of index 2 with G. This subgroup has fixed field of degree 2 over $\mathbb{Q}$ so it is a quadratic extension of $\mathbb{Q}$.

To show that this quadratic extension of $\mathbb{Q}$ is $\mathbb{Q}\left(\sqrt{p}\right)$, it suffices to show that p is the only ramified prime in the quadratic extensions. Only primes that divide the discriminant are ramified. It turns out that p is the only prime ramified in $\mathbb{Q}(\zeta_p)$ and since discriminants are transitive with respect to subfields, p is the only prime in the quadratic subfield which restricts the quadratic subfield to either $\mathbb{Q}\left(\sqrt{p}\right)$ or $\mathbb{Q}(\sqrt{-p})$. The details of this proof can be found in Zariski and Samuel [14, 315].

Instead, we provide a proof found in [6, 76]. Let $\mathbb{Q}(\sqrt{\pm p})$ be a quadratic extension of $\mathbb{Q}$. We will show

$$\mathbb{Q}\left(\sqrt{\pm p}\right) \subseteq \mathbb{Q}(\zeta_{4p}).$$

However, we start by looking at the field $\mathbb{Q}(\zeta)$ where ζ is a primitive pth root of unity. Recall that we defined the Legendre symbol, also known as the quadratic symbol, to be

$$\left(\frac{z}{p}\right) = \begin{cases} 1 & \text{if } v \equiv x^2 \pmod{p} \\ -1 & \text{if } v \not\equiv x^2 \pmod{p}, \end{cases}$$

where $z \in \mathbb{Z}$ and $z \not\equiv 0 \pmod{p}$. If p is an odd prime, consider the element

$$S = \sum_z \left(\frac{z}{p}\right) \zeta^z,$$

where z runs through the $p-1$ nonzero residue classes of p. Note that S is an element of $\mathbb{Q}(\zeta_p)$.

We show

$$S^2 = \left(\frac{-1}{p}\right) p.$$

Note that $\left(\frac{z}{p}\right) \cdot \left(\frac{v}{p}\right) = \left(\frac{zv}{p}\right)$. This says that if two numbers have a quadratic residue or if two numbers both do not have a quadratic residue, then their product will have a quadratic residue. Similarly, the product of a number with a quadratic residue and a number that does not have a

quadratic residue will not have a quadratic residue. From the definition of S,

$$S^2 = \sum_{z,v} \left(\frac{zv}{p}\right) \zeta^{z+v}.$$

Reiterating the statement above, given a fixed v, the product zv will behave the same over non-zero residue classes as z will.

Replacing z with zv gives

$$S^2 = \sum_{z,v} \left(\frac{(zv)v}{p}\right) \zeta^{(zv)+v} = \sum_{z,v} \left(\frac{zv^2}{p}\right) \zeta^{v(z+1)}.$$

Since zv^2 contains a square, we can take it out $\left(\frac{zv^2}{p}\right) = \left(\frac{z}{p}\right)\left(\frac{v^2}{p}\right) = \left(\frac{z}{p}\right)$ and so,

$$S^2 = \sum_{z,v} \left(\frac{z}{p}\right) \zeta^{v(z+1)}.$$

Re-indexing and considering the term where $z = -1$ separately gives

$$S^2 = \sum_{z} \left(\sum_{v} \left(\frac{z}{p}\right) \zeta^{v(z+1)}\right) = \sum_{z=-1} \left(\sum_{v} \left(\frac{z}{p}\right) \zeta^{v(z+1)}\right) + \sum_{z\neq -1} \left(\sum_{v} \left(\frac{z}{p}\right) \zeta^{v(z+1)}\right)$$

$$= \sum_{v} \left(\frac{-1}{p}\right) \zeta^0 + \sum_{z\neq -1} \left(\left(\frac{z}{p}\right) \sum_{v} \zeta^{v(z+1)}\right).$$

Since v runs over the $(p-1)$ nonzero residue classes of p, $\sum_{v} \left(\frac{-1}{p}\right) = \left(\frac{-1}{p}\right)(p-1)$.

Furthermore, since p is prime, ζ, and consequently ζ^{z+1} for the fixed z, satisfy the polynomial $x^{p-1} + \ldots + x + 1 = 0$. So $\sum_{v} \zeta^{v(z+1)} = \sum_{v} \left(\zeta^{z+1}\right)^v = \left(\zeta^{z+1}\right)^{p-1} + \ldots + \zeta^{z+1} = -1$. Thus

$$S^2 = \left(\frac{-1}{p}\right)(p-1) + (-1) \sum_{v\neq -1} \left(\frac{v}{p}\right) = p\left(\frac{-1}{p}\right) - \left(\frac{-1}{p}\right) - \sum_{v\neq -1} \left(\frac{v}{p}\right)$$

$$= p\left(\frac{-1}{p}\right) - \sum_{v} \left(\frac{v}{p}\right) = p\left(\frac{-1}{p}\right).$$

where $\sum_v \left(\frac{v}{p}\right) = 0$ because there are the same amount of quadratic residues as non-residues.

We have shown that for any odd prime p, $\pm p$ is the square of an element S of $\mathbb{Q}(\zeta)$, where p

is positive or negative depending on the quadratic residue of -1 with p. Since $\pm p$ is the square of the S in $\mathbb{Q}(\zeta)$, then $\sqrt{p}$ is contained in $\mathbb{Q}(\zeta)$ or $\mathbb{Q}(\zeta)(i)$ and the unique quadratic subfield must be $\mathbb{Q}(\sqrt{\pm p})$. The same analysis works for the even prime $p=2$ because $2i=(1+i)^2$, the square of an element of $\mathbb{Q}\left(\sqrt{2},i\right)$.

Greenberg concisely notices that $\mathbb{Q}\left(\zeta_p,\sqrt{-1}\right)$ is equivalently given by $\mathbb{Q}(\zeta_{4p})$ and it can be shown by a simple containment argument. Since 4 and p divide $4p$, the field generated by the primitive $(4p)$th root ζ_{4p} contains the primitive 4th roots and the primitive pth roots. Thus $\mathbb{Q}\left(\zeta_p,\sqrt{-1}\right)\subseteq\mathbb{Q}(\zeta_{4p})$. Conversely, the primitive nth root of unity that generates the group generated by ζ_p and $\zeta_4=\sqrt{-1}$ is given by $n=\operatorname{lcm}(p,4)=4p$ since p is an odd prime. Thus $\mathbb{Q}(\zeta_{4p})\subseteq\mathbb{Q}\left(\zeta_p,\sqrt{-1}\right)$. Thus the extension $\mathbb{Q}(\sqrt{\pm p})$ is contained in the extension $\mathbb{Q}\left(\zeta_{4p}\right)$. □

3.3 Greenberg's Proof of The Kronecker-Weber Theorem

3.3.1 Application of Background Information to Kronecker-Weber Theorem Setup:

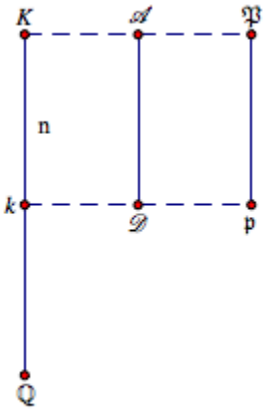
So far, we have explored how prime ideals factor into other prime ideals as the ring in which the ideal is considered is expanded to include more elements. Additionally, the condition of the ideal in different rings is strongly linked to specific Galois subgroups given by the fields that naturally contain said rings. The goal of this section is to provide a proof of the Kronecker-Weber theorem which gives results for field extensions of $\mathbb{Q}$. The natural rings to look at in field extensions of $\mathbb{Q}$ are the rings of algebraic integers and the proof will focus on these rings while applying the results found in the previous section.

The setup, as depicted in Figure 3.3.1, is as follows: let k be a finite extension of $\mathbb{Q}$ and K a finite Galois extension of k that has degree n and Galois group $G=\operatorname{Gal}(K/k)$. Let $\mathscr{A}$ be the ring of algebraic integers contained in K and $\mathscr{D}$ be the corresponding ring of algebraic integers contained in k. Given a prime ideal $\mathfrak{P}$ in $\mathscr{A}$, its contraction into $\mathscr{D}$ is a prime ideal $\mathfrak{p}=\mathfrak{P}\cap\mathscr{D}$. $\mathfrak{P}$ and $\mathfrak{p}$ will each form a residue field in their respective rings which are denoted $\bar{K}=\mathscr{A}/\mathfrak{P}$ and $\bar{k}=\mathscr{D}/\mathfrak{p}$. As before, the bar signifies the cosets given by the ideals $\mathfrak{P}$ or $\mathfrak{p}$ depending on the context.

While K and k, field extensions of $\mathbb{Q}$, are not finite fields, the residue fields $\bar{K}=\mathscr{A}/\mathfrak{P}$ and $\bar{k}=\mathscr{D}/\mathfrak{p}$ are finite fields and $\bar{K}/\bar{k}$ is a field extension of degree f, where $f=[\mathscr{A}/\mathfrak{P}:\mathscr{D}/\mathfrak{p}]$ is the relative degree of $\mathfrak{P}$ over $\mathfrak{p}$. If $\mathscr{D}/\mathfrak{p}$ has size q, then $\mathscr{A}/\mathfrak{P}$ has order q^f by theorem on page 31. The field extension $\mathscr{A}/\mathfrak{P}$ over $\mathscr{D}/\mathfrak{p}$ is referred to as the residue extension.

The term ramified, as of now, has strictly referred to ideals. However, in the context of rings of

Figure 3.3.1: Proof Setup



algebraic integers over $\mathbb{Q}$, any prime ideal is principal and written (p) for some prime integer p. Consequently, the terminology for ideals is broadened to apply to integers z where the meaning is actually applied to the ideal (z). For example, for any prime $p \in \mathbb{Z}$, p is said to be ramified if the ideal (p) is ramified.

The first step will be to establish the relationship between $\mathfrak{P}$ and $\mathfrak{p}$ in their respective fields. Since $\mathfrak{p}$ is the contraction of $\mathfrak{P}$ in $\mathscr{D}$, extending $\mathfrak{p}$ back into $\mathscr{A}$ gives us an ideal contained in $\mathfrak{P}$ since a contraction followed by an extension is contained in the original ideal. We found that the possible components of the ideal given by the extension of $\mathfrak{p}$ into $\mathscr{A}$ are very predictable if the ring containing $\mathfrak{p}$ is integrally closed, the ring containing the extension of $\mathfrak{p}$ is the integral closure of the ring containing $\mathfrak{p}$, and the field containing the ring with $\mathfrak{P}$ is a normal extension of the field containing the ring with $\mathfrak{p}$.

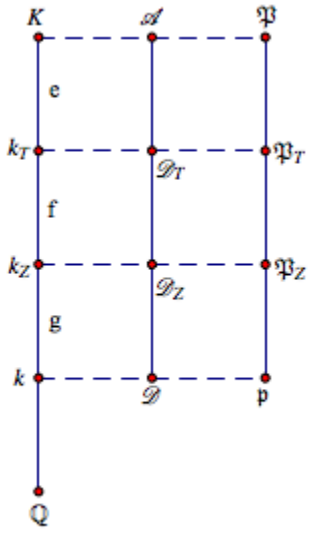
The algebraic integers $\mathscr{D}$ in k are, in fact, integrally closed and K is actually a Galois extension of k, both normal and separable. So, it is immediate that there are finitely many ideals $\mathfrak{P}_1, ..., \mathfrak{P}_g$ contained in $\mathscr{A}$ that lie over $\mathfrak{p}$, where g is the number of such ideals and without loss of generality $\mathfrak{P}_1 = \mathfrak{P}$. Each ideal $\mathfrak{P}_i$ has the same ramification index e over $\mathfrak{p}$,

$$\mathscr{A}\mathfrak{p} = (\mathfrak{P}_1\mathfrak{P}_2...\mathfrak{P}_g)^e,$$

all $\mathfrak{P}_i$ are images of $\mathfrak{P}$ under automorphisms of $G = \mathrm{Gal}(K/k)$. Finally, where $f = [\mathscr{A}/\mathfrak{P} : \mathscr{D}/\mathfrak{p}]$ is the relative degree of $\mathfrak{P}$ over $\mathfrak{p}$,

$$efg = n.$$

Figure 3.3.2: Decomposition and Inertia Groups



Greenberg collects this information as Fact 0 in the setup of the proof.

The next step is to find the decomposition group and the inertia group for this specific pair of extensions and rings. Part of this process will include identifying the ramification index of $\mathfrak{P}$. Given the prime ideal $\mathfrak{P}$ lying over $\mathfrak{p}$, the Galois group of the field extension K/k has as subgroups the decomposition group G_Z and the inertia group G_T. G_Z and G_T have corresponding fields k_Z and k_T, and corresponding rings $\mathfrak{D}_Z$ and $\mathfrak{D}_T$. $\mathfrak{P}$ in $\mathscr{A}$ lies over $\mathfrak{P}_T$ in $\mathscr{D}_T$, $\mathfrak{P}_T$ in $\mathscr{D}_T$ lies over $\mathfrak{P}_Z$ in $\mathscr{D}_Z$, and $\mathfrak{P}_Z$ lies over $\mathfrak{p}$ in $\mathscr{D}$. Figure 3.3.2 summarizes this.

Going the other direction, if $\mathfrak{p}$ is extended from $\mathscr{D}$, where it is prime, into $\mathscr{D}_Z$, it factors into

$$\mathfrak{p}\mathscr{D}_Z = \prod \mathfrak{P}_Z$$

where the $\mathfrak{P}_Z$ are prime ideals in $\mathscr{D}_Z$ lying over $\mathfrak{p}$. The extension of a given $\mathfrak{P}_Z$ in $\mathscr{D}_Z$ into $\mathscr{D}_T$ is given by

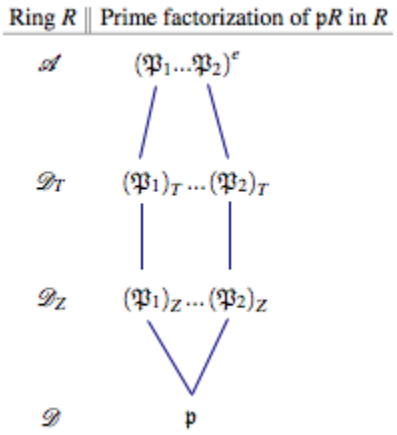
$$\mathfrak{P}_Z\mathscr{D}_T = \mathfrak{P}_T$$

so $\mathfrak{p}$ in $\mathscr{D}$ extended into $\mathscr{D}_T$ factors as

$$\mathfrak{p}\mathscr{D}_T = \prod \mathfrak{P}_T$$

where $\mathfrak{P}_T$ is the only prime ideal in $\mathscr{D}_T$ lying over $\mathfrak{P}_Z$ in $\mathscr{D}_Z$. The extension of a given $\mathfrak{P}_T$ in $\mathscr{D}_T$

Figure 3.3.3: Prime Factorization of (p)



into $\mathscr{A}$ is given by

$$\mathfrak{P}_T \mathscr{A} = \mathfrak{P}^e$$

where $\mathfrak{P}$ is the only prime ideal in $\mathscr{A}$ lying over $\mathfrak{P}_T$, so $\mathfrak{p}$ in $\mathscr{D}$ extended into $\mathscr{A}$ factors as

$$\mathfrak{p}\mathscr{A} = \prod \mathfrak{P}^e.$$

To conclude, passage from $\mathscr{D}$ into $\mathscr{D}_Z$ splits $\mathfrak{p}$ into g distinct prime factors $\mathfrak{P}_Z$. Passage from $\mathscr{D}_Z$ into $\mathscr{D}_T$ does not change the form of the decomposition of $\mathfrak{p}$ and passage from $\mathscr{D}_T$ into $\mathscr{A}$ does not add new distinct prime factors, but $\mathfrak{p}$ factors into a product of e of each distinct prime factor, of which there are still g. In particular, $\mathfrak{P}_T$ is unramified over $\mathfrak{p}$ but $\mathfrak{P}$ is fully ramified over $\mathfrak{P}_T$. Figure 3.3.3 summarizes these results which are Fact 2 in Greenberg's proof. As before, a line connecting two ideals signifies that the first ideal lies over the second ideal.

Using the second definition given for the inertia group, G_T is given as the kernel of the homomorphism that takes $s \in G_Z$ to $s_1 : R'/\mathfrak{P} \to R'/\mathfrak{P}$ where $s_1(x+\mathfrak{P}) = s(x)+\mathfrak{P}$. If k is a finite extension of $\mathbb{Q}$, K a finite Galois extension of k with Galois group G, $\mathfrak{p}$ a prime ideal in $\mathfrak{D}$, the ring of algebraic integers of k, and $\mathfrak{P}$ a prime ideal in $\mathscr{A}$, the ring of algebraic integers lying over K, according to Lang, there exists a unique automorphisms s_1 of $\bar{K} = \mathscr{A}/\mathfrak{P}$ over $\bar{k} = \mathscr{D}/\mathfrak{p}$ which generates $\mathrm{Gal}(\bar{K}/\bar{k})$.

Furthermore, since $\mathrm{Gal}(\bar{K}/\bar{k}) \cong G_Z/G_T$, and since the automorphisms of $\bar{K}/\bar{k}$ are induced by automorphisms of K/k, there exists an automorphism s of K over k that induces the automorphism s_1 of $\bar{K}$ over $\bar{k}$. Specifically, if q is the order of $\mathscr{D}/\mathfrak{p}$, then $s_1(x) \equiv x^q$, and equivalently there exists

s such that

$$s(\alpha) \equiv \alpha^q \pmod{\mathfrak{P}}$$

which induces the s_1 that generates G_Z/G_T. Consequently, G_Z/G_T is cyclic [6, 17]. In the proof of the Kronecker-Weber theorem, Greenberg refers to this as Fact 1.

In addition to the decomposition group and the inertia group, $\mathfrak{P}$ also has associated ramification subgroups. Since the ramification groups G_{V_n} are abelian in G_Z, we focused on factor groups and found the groups $G_{V_n}/G_{V_{n+1}}$ to be abelian for $n \geq 2$. Furthermore, these factor groups $G_{V_n}/G_{V_{n+1}}$, which were named $G_1 = G_T/G_{V_2}$ and $G_n = G_{V_n}/G_{V_{n+1}}$ for simplicity, contain their own respective subgroups G_1' and G_n'. When an additional quotient of G_1 is taken by its subgroup G_1', the result is cyclic and surprisingly isomorphic to a multiplicative subgroup of $\mathscr{A}/\mathfrak{P}$. And taking the quotient group of G_n with G_n' gives groups isomorphic to additive subgroups of $\mathscr{A}/\mathfrak{P}$.

Since $\mathscr{A}/\mathfrak{P}$ is a separable extension of $\mathscr{D}/\mathfrak{p}$, G_1' and G_n' are reduced to the identity and we make the following stronger statements: G_1 is isomorphic to a multiplicative subgroup of $\mathscr{A}/\mathfrak{P}$, and for $n \geq 2$, the G_n themselves are isomorphic to additive subgroups of $\mathscr{A}/\mathfrak{P}$. Since $\mathscr{A}/\mathfrak{P}$ is a finite field of order q^f, the nonzero elements of $\mathscr{A}/\mathfrak{P}$ form a multiplicative group of order $q^f - 1$. This multiplicative group is cyclic. If G_1 is isomorphic to a multiplicative subgroup of $\mathscr{A}/\mathfrak{P}$, G_1 must be isomorphic to a subgroup of the multiplicative group of order $q^f - 1$ and so its order divides $q^f - 1$ [14, 83].

For $n \geq 2$, if G_n is not the zero subgroup of $\mathscr{A}/\mathfrak{P}$, the size of $G_{V_n}/G_{V_{n+1}}$ is a power of p, the characteristic of $\mathscr{D}/\mathfrak{p}$, since G_n is an additive subgroup of $\mathscr{A}/\mathfrak{P}$, a finite extension of $\mathscr{D}/\mathfrak{p}$. And $G_{V_n}/G_{V_{n+1}}$ is isomorphic to a direct product of finitely many cyclic groups of order p [**?**, 158]. G_n is the trivial subgroup of $\mathscr{A}/\mathfrak{P}$ if $G_{V_n} = G_{V_{n+1}}$. There are only finitely many ramification groups anyway, so $G_{V_n} = G_{V_{n+1}}$ and $G_n = 0$ for all $n \geq N$ for some integer N. It is the n such that G_n is not trivial that provide the interesting results and the n such that $G_{V_n} \neq G_{V_{n+1}}$ were referred to as the ramification numbers of $\mathfrak{P}$ over $\mathfrak{p}$. The existence and properties of the G_n as subgroups of $\mathscr{A}/\mathfrak{P}$ are Fact 3 in Greenberg's proof.

Near the end of the previous section on page 51, we gave two theorems. First, if K is a finite extension of $\mathbb{Q}$ and $K \neq \mathbb{Q}$, then there exist ramified primes in K. Secondly, there are only finitely many ramified primes in K. This result is known as Minkowski's Theorem and is Fact 4 in the proof.

Fact 5 collects the various facts we have proved about cyclotomic extensions into one fact. If ζ is an mth root of unity, a cyclotomic extension of $\mathbb{Q}$ is defined to be a subfield of $\mathbb{Q}(\zeta)$. Among other properties, composites of cyclotomic extensions are cyclotomic, $\mathbb{Q}(\zeta)$ is an abelian extension of $\mathbb{Q}$ and $\mathrm{Gal}(\mathbb{Q}(\zeta)/\mathbb{Q})$ is isomorphic to the multiplicative group $(\mathbb{Z}/n\mathbb{Z})^\times$. If $p \neq 2$

is prime, $\mathrm{Gal}(\mathbb{Q}(\zeta_{p^n})/\mathbb{Q}) \cong (\mathbb{Z}/p^n\mathbb{Z})^\times$ which has order $p^{n-1}(p-1)$. Furthermore, if $p = 2$ and $n \geq 3$, then the Galois group has is isomorphic to the direct product of two cyclic groups: on with order 2^{n-1} and the other of order 2. The second group can be generated by the automorphism sending $\zeta_{2^n} \mapsto \zeta_{2^n}^{-1}$. Finally, if p is a prime, then p is the only ramified prime contained in $\mathbb{Q}(\zeta_{p^n})$ and it is fully ramified. The only exception is $\mathbb{Q}(\zeta_2) = \mathbb{Q}$. For general m, the primes dividing m are the ramified primes in $\mathbb{Q}(\zeta_m)$.

The last fact, Fact 6, given by Greenberg in preparation for the proof of the Kronecker-Weber theorem was stated on page 14 regarding the composite of two Galois extensions. If K and L are Galois extensions of a field k, then KL is Galois over k with Galois group isomorphic to a subgroup of $\mathrm{Gal}(K/k) \times \mathrm{Gal}(L/k)$. In particular, it contains the pairs of automorphisms (σ, τ) such that $\sigma \in \mathrm{Gal}(K/k)$, $\tau \in \mathrm{Gal}(L/k)$ and σ and τ match on $K \cap L$.

3.3.2 Proof Proper:

The general structure of the proof is to narrow down the vast number of abelian extensions that we need to consider to a specific type of abelian extensions: namely cyclic extensions of a prime power order λ^m where λ is the only ramified prime. In the second lemma, we show that if any cyclic abelian extension of order a prime power is cyclotomic, then the result can be extended to any abelian extension. In the third lemma, we show that we can further assume that there is only the one ramified prime in the cyclic extension of prime power order.

The second half of the proof is devoted to showing that such an extension is cyclotomic. The proof is divided into two cases: the order of the extension is a power of an odd prime, or the order of the extension is the even prime 2. If both cases are cyclotomic, the proof is completed by the first part of the proof.

We continue to use the conditions that k is a finite extension of $\mathbb{Q}$ and K a finite Galois extension of k that has degree n with Galois group $G = \mathrm{Gal}(K/k)$. $\mathscr{A}$ is the ring of algebraic integers contained in K and $\mathscr{D}$ is the ring of algebraic integers contained in k. $\mathfrak{P}$ is a given prime ideal in $\mathscr{A}$, its contraction into $\mathscr{D}$ is a prime ideal $\mathfrak{p} = \mathfrak{P} \cap \mathscr{D}$. $\mathfrak{P}$ and $\mathfrak{p}$ each form a residue field in their respective rings which are denoted $\bar{K} = \mathscr{A}/\mathfrak{P}$ and $\bar{k} = \mathscr{D}/\mathfrak{p}$.

Greenberg starts the proper proof by expanding Fact 3 to create a lemma. We have established in Fact 3 that $G_1 = G_T/G_{V_2}$, as a multiplicative subgroup contained in $\mathscr{A}/\mathfrak{P}$, must be cyclic and of order that divides $q^f - 1$ where $\mathscr{A}/\mathfrak{P}$ has order q^f and $\mathscr{D}/\mathfrak{P}$ has order q. We have also established that G_n/G_{n+1} are abelian for $n \geq 2$. However, G_Z/G_T and G_T/G_{V_1} are not necessarily abelian. Consequently, the first lemma will be based on the condition that G_Z/G_T is abelian.

Lemma 93. *If G_Z/G_T is abelian, then G_T/G_{V_2} is a cyclic subgroup of $\mathscr{A}/\mathfrak{P}$ of order dividing $q-1$.*

Proof. We can associate the ring of integers $\mathscr{A}$ with the quotient ring $\mathscr{A}/\mathfrak{P}$ through localization. We have also already established that $\mathscr{A}/\mathfrak{P}$ is a principal ideal domain because the residue class ring of a Dedekind domain by a proper ideal is a principal ideal domain. Consequently, this localization process allows us to view $\mathfrak{P}$ as a principal ideal so $\mathfrak{P} = \mathscr{A}\pi$ for some generator π. See the proof of theorem 90 for another example or on page 36 for the introduction to the idea of localization.

Given an automorphism s in G_Z, the group of automorphism of G that maps $\mathfrak{P}$ to $\mathfrak{P}$, we define a mapping from G_Z to $\mathscr{A}$ by examining how s acts on π, the generator of $\mathfrak{P}$. We can write

$$s(\pi) = a_s\pi$$

for some $a_s \in \mathscr{A}$ where a_s is not an element of $\mathfrak{P}$. The mapping $s \mapsto a_s$ induces a homomorphism $s \mapsto \bar{a}_s$ from G_T into $\bar{K}\backslash 0$, the multiplicative group of $\bar{K}$. We will examine two special automorphisms of G_Z.

First, since G_T/G_{V_2} is cyclic, there exists $t \in G_T$ such that $t + G_{V_2}$ generates G_T/G_{V_2}. t is one of the two automorphisms we will consider.

From Fact 1 on page 58, we showed G_Z/G_T is cyclic by finding a unique automorphism s_1 of $\bar{K}$ over $\bar{k}$ which generates $\mathrm{Gal}(\bar{K}/\bar{k})$ and an automorphism s of K over k that induces s_1. In particular, if q is the order of $\mathscr{D}/\mathfrak{p}$, the automorphism s of K over k such that

$$s(a) \equiv a^q \pmod{\mathfrak{P}},$$

for $a \in K$, induces s_1 where

$$s_1(x) \equiv x^q$$

for $x \in \bar{K}$. This $s \in G_Z$ the other automorphism we will consider.

Since both s and t are elements of G_Z,

$$s(\pi) = a_s\pi \text{ and } t(\pi) = a_t\pi$$

for $a_s, a_t \in \mathscr{A}$ and $a_s, a_t \notin \mathfrak{P}$. Moreover,

$$\pi = s^{-1}(a_s\pi) = s^{-1}(a_s)\cdot s^{-1}(\pi) \implies s^{-1}(\pi) = s^{-1}(a_s^{-1})\pi.$$

Also, recall that G_T is a normal subgroup of G_Z so we can consider a third automorphism sts^{-1} and

$$sts^{-1}(\pi) = a_{sts^{-1}}\pi$$

for $a_{sts^{-1}} \in \mathscr{A}$, $a_{sts^{-1}} \notin \mathfrak{P}$. sts^{-1} looks like a tempting function on which we can apply our assumption that G_Z/G_T is abelian. Unfortunately, automorphisms in G_Z/G_T are automorphisms with domain $\mathscr{A}/\mathfrak{P}$ as opposed to s and t which have domain $\mathscr{A}$. However, automorphisms in G_Z can be converted to automorphisms on $\mathscr{A}/\mathfrak{P}$ as in Fact 1, and in fact, G_T is the kernel of that mapping.

Since $t \in G_T$, t_1 is the identity function on $\mathscr{A}/\mathfrak{P}$ so clearly $s_1 t_1 s_1^{-1} = t_1$ and consequently,

$$a_{sts^{-1}}\pi + \mathfrak{P} = s_1 t_1 s_1^{-1}(\pi) + \mathfrak{P} = s_1 t_1 s_1^{-1}(\pi + \mathfrak{P}) = t_1(\pi + \mathfrak{P}) = t_1(\pi) + \mathfrak{P} = a_t\pi + \mathfrak{P}$$

so

$$\bar{a}_{sts^{-1}} = \bar{a}_t.$$

Alternatively, we can compute $\bar{a}_{sts^{-1}}$ explicitly by computing $a_{sts^{-1}}$ and finding the residue modulo $\mathfrak{P}$:

$$\begin{aligned} sts^{-1}(\pi) &= st\left(s^{-1}(a_s^{-1})\pi\right) = s\left(ts^{-1}(a_s^{-1}) \cdot t(\pi)\right) = s\left(ts^{-1}(a_s^{-1}) \cdot a_t\pi\right) \\ &= sts^{-1}(a_s^{-1}) \cdot s(a_t) \cdot s(\pi) = \left(sts^{-1}(a_s^{-1}) \cdot s(a_t) \cdot a_s\right)\pi. \end{aligned}$$

By definition of $a_{sts^{-1}}$,

$$a_{sts^{-1}} = sts^{-1}(a_s^{-1}) \cdot s(a_t) \cdot a_s.$$

To get $\bar{a}_{sts^{-1}}$, we reduce modulo $\mathfrak{P}$.

$$\bar{a}_{sts^{-1}} = sts^{-1}(a_s^{-1}) \cdot s(a_t) \cdot a_s + \mathfrak{P} = \left(sts^{-1}(a_s^{-1}) + \mathfrak{P}\right)(s(a_t) + \mathfrak{P})(a_s + \mathfrak{P}).$$

Equivalently, this is

$$\bar{a}_{sts^{-1}} = \left(sts_1^{-1}(a_s^{-1} + \mathfrak{P})\right)(s_1(a_t + \mathfrak{P}))(a_s + \mathfrak{P})$$

Since $t \in G_T$, the kernel of the mapping that takes t to t_1, t_1 must be the identity so

$$\bar{a}_{sts^{-1}} = \left(a_s^{-1} + \mathfrak{P}\right)(s_1(a_t + \mathfrak{P}))(a_s + \mathfrak{P}) = s_1(a_t + \mathfrak{P}).$$

Using the definition of s_1, we get

$$\bar{a}_{sts^{-1}} = s_1(a_t + \mathfrak{P}) = (a_t + \mathfrak{P})^q = \bar{a}_t^q.$$

And using the fact that $\bar{a}_{sts^{-1}} = \bar{a}_t$,

$$\bar{a}_t = \bar{a}_{sts^{-1}} = \bar{a}_t^q \implies 1 = \bar{a}_t^{q-1}.$$

If we were not so careful in observing that the $a_s, a_t, a_{sts^{-1}}$ are definitely not contained in $\mathfrak{P}$, then reducing modulo $\mathfrak{P}$ would have given very little information. As is, we see that the assignment

$$t \mapsto \bar{a}_t$$

that induces the isomorphism from G_T/G_{V_2} into the multiplicative group $\bar{K}\backslash 0$ has t mapping to an element with order dividing $q-1$. Furthermore, we chose t such that its coset actually generates G_T/G_{V_2}, so G_T/G_{V_2} is isomorphic to a multiplicative group in $\bar{K}\backslash 0$ of order dividing $q-1$. □

To give some idea of the direction of our proof, Greenberg's next lemma will narrow down the type of extension for which the Kronecker-Weber theorem needs to be proved from all abelian extensions to just cyclic ones with a prime power order.

Lemma 94. *If the results of Kronecker-Weber theorem can be proved for cyclic extensions with order a prime power, then the results hold for all abelian extensions.*

Proof. The Galois group G of the abelian extension $K/\mathbb{Q}$ is a finite abelian group, so G is isomorphic to a unique direct product of cyclic subgroups G_i such that each G_i has order a power of a prime. The field extension of $\mathbb{Q}$ with G_i as a Galois group is exactly the fixed field of the other G_j. In other words, if K_i is the fixed field of $\prod_{j\neq i} G_j$, then $K_i/\mathbb{Q}$ has Galois group G_i. Given that the Kronecker-Weber theorem holds true for cyclic extensions with order a prime power, each $K_i/\mathbb{Q}$ is a cyclotomic extension. Since K is the composite of the K_i, and since we know from Fact 5 that the composite of a finite number of cyclotomic fields is cyclotomic, we conclude that K must be a cyclotomic extension.

□

This lemma not only narrows down the type of extension that we need to consider, but also narrows it down to a type that we know a lot about (see Fact 6 for example). The next lemma further simplifies what we need to prove by proposing that in any abelian extension of $\mathbb{Q}$ with

degree a power of a prime, we can assume that every prime except the degree of the extension is unramified.

Lemma 95. *Let K be an abelian extension of $\mathbb{Q}$ such that the degree of K over $\mathbb{Q}$ is λ^m for a prime λ and some integer m. To show K is cyclotomic, it is sufficient to show K is cyclotomic with the assumption that every prime $p \neq \lambda$ is unramified in K.*

Proof. Recall that in a general Galois extension K/k, where k is in turn a finite extension of $\mathbb{Q}$, and $G = \mathrm{Gal}(K/k)$, the degree $ep^s = [K : k_Z]$, where k_Z is the field fixed by the decomposition subgroup of G, is called the ramification index of $\mathfrak{P}$ over $\mathfrak{p}$. The reduced ramification index e (the power to which the prime factors of the ideal $\mathfrak{p}R'$ must be raised to get $\mathfrak{p}R'$) is a factor of the ramification index. When a prime ideal $\mathfrak{P}$ of R' has ramification index greater than 1, we say $\mathfrak{P}$ is ramified.

If $R'/\mathfrak{P}$ is separable over $R/\mathfrak{p}$, we have the much simpler case where $p^s = 1$ and the ramification index and the reduced ramification index of $\mathfrak{P}$ over $\mathfrak{p}$ are both e. When considering the rings of algebraic integers $\mathscr{D}$ and $\mathscr{A}$ in the extension L/K, $\mathscr{A}/\mathfrak{P}$ is separable over $\mathscr{D}/\mathfrak{p}$. The case where the lower field k is $\mathbb{Q}$ instead of being an extension of $\mathbb{Q}$ is even more straightforward.

In using the facts and lemmas thus far developed for this situation, we are examining K as a Galois extension of $\mathbb{Q}$ itself. For the proof of this lemma, $k = \mathbb{Q}$ and $\mathscr{D}$, the algebraic integers in $\mathbb{Q}$ are just the rational integers $\mathbb{Z}$ (this was an immediate result of the theorem on page 32). Let $p \neq \lambda$ be ramified in K and $\mathfrak{P}$ a prime ideal of K lying over (p). Then $\bar{k} = \mathscr{D}/\mathfrak{p} = \mathbb{Z}/(p) = \mathbb{Z}_p$ and the order q of $\bar{k}$ is $q = p$. And since $\bar{k}$ is itself a finite field, it has order a power of its characteristic so p is not only the size of $\bar{k}$ but also the characteristic of $\bar{k}$.

Prime numbers p are said to be ramified over finite extensions of $\mathbb{Q}$ if the prime ideal (p) is ramified over $\mathbb{Q}$. In other words, if $\mathscr{A}$ is the ring of algebraic integers in K and

$$(p) = p\mathscr{A} = \mathfrak{p}_1^{e_1} \cdot \ldots \cdot \mathfrak{p}_g^{e_g},$$

then p is ramified provided $e_i > 1$ for some i. If $e_i = 1$ for all i, then p is unramified. Abelian extensions were introduced on page 41. Since an abelian extension is Galois, (p) is more explicitly written as

$$(p) = \mathscr{A}p = (\mathfrak{p}_1 \cdot \ldots \cdot \mathfrak{p}_g)^e.$$

Since the order of the extension $K/\mathbb{Q}$ is λ^m, the Galois group of the extension has size λ^m and any subgroup of the Galois group G must have order dividing λ^m. Moreover, the quotient of any two subgroups of the G must have order $\lambda^i/\lambda^j = \lambda^{i-j}$, $(j \leq i)$. Consequently p, a different prime, cannot divide the order of the quotient of those two groups. Remember that we gave special

emphasis to the ramification numbers n of $\mathfrak{P}$ over $\mathfrak{p}$ such that $G_{V_n} \neq G_{V_{n+1}}$, or n such that $G_{V_n}/G_{V_{n+1}}$ is not trivial.

In 3.3.1, it was stated that $G_{V_n}/G_{V_{n+1}}$ is either trivial or, in the case of a ramification number, a direct product of cyclic groups of order p, the characteristic of $\bar{k}$. But if $G_{V_n}/G_{V_{n+1}}$ is a direct product of cyclic groups of order p, p must divide the order of $G_{V_n}/G_{V_{n+1}}$ which is impossible. So $G_{V_n}/G_{V_{n+1}}$ must be trivial for all $n \geq 2$. Recall also that there are only finitely many nontrivial nth ramification groups G_{V_n}. For some j sufficiently large enough, G_{V_j} is trivial. Combining this with the fact that not only are some of the $G_{V_n}/G_{V_{n+1}}$ trivial, but all of them are trivial, it must be that G_{V_n} is trivial for all $n \geq 2$, not just after a certain point. For if G_{V_n} was not trivial for some $n \geq 2$, then there must be some $j \geq n$ where $G_{V_j}/G_{V_{j+1}}$ is nontrivial.

Fact 3 also gives that G_T/G_{V_2} is cyclic with order dividing $q^f - 1$ where q is the size of $\bar{k}$ and is also p in this case. As a subgroup of G, G_T has order λ^u for some $u \leq m$ (and so the ramification index of p is λ^u). We just showed $G_{V_2} = 0$, so we could conclude that G_T itself has order dividing $q^f - 1$, or equivalently that

$$q^f \equiv 1 \pmod{\lambda^u}.$$

However, provided G_Z/G_{V_2} is abelian, we have on page 59 the stronger result that the order of G_T/G_{V_2} divides $q-1$. Then since $p = q$,

$$p = q \equiv 1 \pmod{\lambda^u}.$$

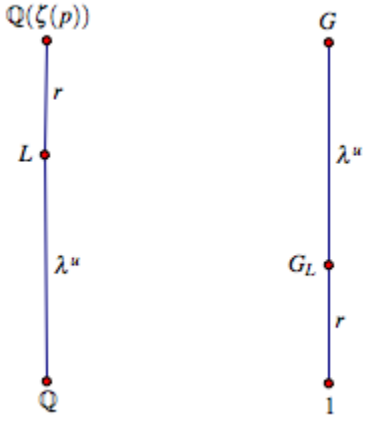
Keeping this in mind, consider the cyclotomic extension of $\mathbb{Q}$ given by the prime p: $\mathbb{Q}(\zeta(p))$. By 3.3.1, this extension gives a cyclic Galois group H of order $p-1$. Also, p is the only ramified prime in $\mathbb{Q}(\zeta(p))$ and it is fully ramified. Since H is cyclic generated by some s, and λ^u divides its order: $q - 1 = r\lambda^u$ for some r, H has a unique subgroup H_L of size r generated by s^{λ^u}. The unique corresponding subfield L of $\mathbb{Q}(\zeta(p))$ is an extension of degree λ^u over $\mathbb{Q}$. See Figure 3.3.4.

Since p is fully ramified in the tower of extensions $\mathbb{Q}(\zeta(p))/\mathbb{Q}$, p is fully ramified in a step of the tower $L/\mathbb{Q}$. Since p is the only prime ramified in $\mathbb{Q}(\zeta(p))$, no other primes are ramified in L.

Using L and K, we will form a field K' where p is no longer ramified in K', yet if K' is cyclotomic, then so is K. Consider the composite extension KL of $\mathbb{Q}$. If K and L intersect, then the intersection must have order a power of λ less than v and less than m. The degree of the extension KL over $\mathbb{Q}$ is given by

$$[KL : \mathbb{Q}] = \frac{[K : \mathbb{Q}][L : \mathbb{Q}]}{[K \cap L : \mathbb{Q}]} = \frac{\lambda^m \cdot \lambda^u}{[K \cap L : \mathbb{Q}]} = \lambda^{m+v}$$

Figure 3.3.4: Lemma 3 Setup



where $v \leq u$. The Galois group of KL over $\mathbb{Q}$ is given by $\text{Gal}(KL/\mathbb{Q}) = \{(\sigma,\gamma) : \sigma\,|_{K\cap L} = \gamma\,|_{K\cap L}\}$, the subgroup of $\text{Gal}(K/\mathbb{Q}) \times \text{Gal}(L/\mathbb{Q}) = G \times H$ where $\sigma \in \text{Gal}(K/\mathbb{Q})$ and $\gamma \in \text{Gal}(L/\mathbb{Q})$ match when restricted to the intersection $K \cap L$. (see Fact 6 or on page 14).

Now the ideal $\mathfrak{P}$ extends into the larger field KL. If $\mathfrak{P}'$ is a prime ideal in KL lying over $\mathfrak{P}$, then $\text{Gal}(KL/\mathbb{Q})$ has subgroup G'_T, the inertia group of $\mathfrak{P}'$ over $\mathfrak{p}$. The inertia group reflects the ramification index of $\mathfrak{P}'$ over $\mathfrak{p}$, and we are trying to find a field where the prime p is unramified. Applying the same analysis we did for K, the higher ramification groups G'_{V_n}, $n \geq 2$, must be trivial so G'_T is cyclic. Since G'_T is a a subgroup of $\text{Gal}(KL/\mathbb{Q})$, G'_T is clearly a subgroup of $G \times H$.

Recall that the isomorphism that shows $\text{Gal}(KL/\mathbb{Q})$ is isomorphic to a subgroup of $G \times H$ is given by the restriction of $\tau \in \text{Gal}(KL/\mathbb{Q})$ to $(\tau\,|_K, \tau\,|_L) \in \text{Gal}(KL/\mathbb{Q})$. If $\tau \in G'_T$, then $\tau\,|_K \in G_T$. So G'_T is not only a subgroup of $G \times H$ but also a subgroup of $G_T \times H$. Furthermore, the ramification index of $\mathfrak{P}'$ over $\mathfrak{p}$ must be greater than or equal to the ramification index of $\mathfrak{P}$ over $\mathfrak{p}$ so the order of G'_T is greater than or equal to λ^u, the order of G_T. On the other hand, G'_T is a subgroup of $G_T \times H$ so the order G'_T is less than or equal to λ^u. We conclude that G'_T has order λ^u and consequently that $[KL : K'] = \lambda^u$.

G'_T has associated field K', a subfield of KL, and G'_T has an associated ideal $\mathfrak{P}'_T = \mathfrak{P}' \cap K'$. In 3.3.1 we established that ramification of an ideal occurs entirely after between the over field and the inertia field. In any subfields of the inertia field, no ramification occurs. The ideal $\mathfrak{P}'_T$ is unramified over p while $\mathfrak{P}'$ is fully ramified over $\mathfrak{P}'_T$. On the other hand, $\mathfrak{P}'_T \cap L$ lies over (p) and (p) is fully ramified in L. The only way for $\mathfrak{P}'_T$ unramified over (p) and $\mathfrak{P}'_T \cap L$ to be fully ramified over (p) is for the intersection of K' and L to be $\mathbb{Q}$, $K' \cap L = \mathbb{Q}$. Otherwise, the intersection has an ideal that is both unramified and fully ramified over (p).

So far it has been shown that $[KL : K'] = \lambda^u = [L : \mathbb{Q}]$ and $[K' : L] = 1$. If the composite $K'L$ is taken instead of KL, $[K'L : \mathbb{Q}]$ is

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

and so $K'L = KL$! Clearly K and K' do not have to be equal, but since L is a cyclotomic extension we at least have that K is cyclotomic if K' is.

There are no primes that ramify in K' that do not ramify in K; otherwise they would ramify in KL and have inertia groups. These inertia groups would have to be contained in the inertia groups of K and L (just as Fact 6 showed G'_T is contained in G_T) but since said primes do not ramify in K or L, the inertia groups in K and L would be trivial. And even though (p) ramifies in K, (p) does not ramify in K'. Since K has finitely many ramified primes (Fact 4, Minkowski's theorem), this process can be repeated to find a field where every prime $p \neq \lambda$ is unramified. □

Two corollaries are consequences of the above proof.

Corollary 96. *If K is an abelian extension of $\mathbb{Q}$ of degree a power m of a prime λ and $p \neq \lambda$ is the only prime ramified in K, then p is fully ramified in K,*

$$p \equiv 1 \pmod{\lambda^m},$$

and K is the unique subfield of $\mathbb{Q}(\zeta(p))$ having degree λ^m. Consequently, $Gal(K/\mathbb{Q})$ is cyclic.

Proof. If K has only one ramified prime, then the field K' constructed through the proof is unramified over $\mathbb{Q}$ since no additional primes will be ramified and the one prime ramified in K will not be ramified in K' by construction. If no primes ramify in K', K' must be the ground field $\mathbb{Q}$ and since $\mathbb{Q}$ is a subfield of L, the smallest field containing $\mathbb{Q}$ and L is $K'L = L$. Since $KL = K'L = L$, L must also contain K. K and L have the same degree, however, so $K = L$. The facts that p is fully ramified in K, $p \equiv 1 \pmod{\lambda^m}$ and $\mathrm{Gal}(L/\mathbb{Q}) = \mathrm{Gal}(K/\mathbb{Q})$ is cyclic are direct results of the proof. □

Corollary 97. *If K is an abelian extension of $\mathbb{Q}$ and K has odd degree over $\mathbb{Q}$, then in K, 2 is unramified over $\mathbb{Q}$.*

Proof. Let K be an abelian extension of $\mathbb{Q}$ of degree λ^m where $\lambda \neq 2$. In the proof of lemma 3, it was found that the nth ramification subgroups G_{V_n}, in particular G_{V_2}, are trivial. Since K is an abelian extension, in the proof, the result from lemma 1 was applied to show that G_T/G_{V_2}, which equals G_T in this case, is cyclic of order dividing $q-1$. In the case of the prime 2, G_T has order dividing 1, so G_T itself is trivial and consequently 2 is unramified over $\mathbb{Q}$. □

The second lemma and the third lemma have narrowed down the domain of possible abelian extensions to be considered to prove the Kronecker-Weber theorem from all abelian extensions to just cyclic extensions of prime power order λ^m, and then just cyclic extensions of prime power order λ^m where λ is the only ramified prime in the field. The next phase of the proof is divided into two cases: if λ is an odd prime, or if $\lambda = 2$, the only even prime. In the case of $\lambda = 2$ we will consider quadratic extensions of $\mathbb{Q}$. We start, however, with the case where λ is odd and show that the Galois group given by this extension is cyclic.

Lemma 98. *Let K be an abelian extension of $\mathbb{Q}$ of degree λ^m where λ is an odd prime. Assume further that every prime $p \neq \lambda$ is unramified in K. Then $Gal(K/\mathbb{Q})$ is cyclic.*

Proof. Let $\mathfrak{P}$ be a prime ideal in K lying over (λ). Even if λ is ramified over $\mathbb{Q}$, λ is unramified over $\mathbb{Q}$ in the inertia field K_T. By fact 4, there must exist some prime ramified in $\mathbb{Q}$. This prime must be λ and since it is the only prime ramified in $\mathbb{Q}$, G_T is all of the Galois group G. But then $|G_T| = |G| = \lambda^m$ so λ is not just ramified, but fully ramified. By fact 0,

$$\lambda^m = efg = \lambda^m fg$$

so $f = 1 = g$. By fact 3, where q is the size of $\mathscr{D}/(\lambda)$, λ, the size of G_T/G_{V_2} divides $q^f - 1 = \lambda - 1$. But G_T has size λ^m and G_{V_2} has size λ^u for $u \leq m$ so the size of G_T/G_{V_2} is a power of λ. The only way for the size of G_T/G_{V_2} to be a power of λ and divide $\lambda - 1$ is for G_T/G_{V_2} to be of size 1 which only occurs when $G_{V_2} = G_T$. Fact 3 also gives that $G_{V_n}/G_{V_{n+1}}$ is trivial or a direct product of cyclic groups of order λ.

To complete the proof of lemma and show $\mathrm{Gal}(K/\mathbb{Q})$ is cyclic, Greenberg inserts the following sub-lemma: *If K is an abelian extension of $\mathbb{Q}$ of degree λ (i.e. $[K : \mathbb{Q}] = \lambda^m$, $m = 1$), then G_{V_3} is trivial.*

The sub-lemma by applying a valuation associated with a prime ideal lying over λ to the derivative of the minimal polynomial of the generator of that prime ideal. It turns out that for any n, if G_{V_n} has nontrivial elements, then the following inequality holds:

$$2\lambda - 1 \geq (n)(\lambda - 1) = n\lambda - n.$$

The greatest n which satisfies this equation, for $\lambda > 2$, is $n = 2$. Since $n = 3$ does not satisfy the equation for any $\lambda > 2$, G_{V_3} cannot have nontrivial elements.

Returning to the proof of the lemma, we find a unique subgroup of G of index λ over $\mathbb{Q}$ that consequently generates all of G. We start with any subgroup H such that $[G : H] = \lambda$ (at least one

such subgroup exists by the Sylow theorems). H has a corresponding field K' which has Galois group $G' = \text{Gal}(K'/\mathbb{Q}) \cong G/H$ and nth ramification subgroups G'_{V_n} in G'. The homomorphism where $g \in \text{Gal}(K/F)$ maps to the restriction of g in K' has kernel H and induces the isomorphism. Therefore, G_{V_n} maps to G'_{V_n} under the restriction and $G_{V_3}/H \cong G'_{V_3}$. Since H has index λ in G, K' is a degree λ extension of $\mathbb{Q}$ and the sub-lemma shows G'_{V_3} is trivial. $G'_{V_3} = G_{V_3}/H$ trivial implies G_{V_3} is a subgroup of H.

G_{V_3} is a subgroup of H and H is a subgroup of $G = G_T = G_{V_2}$. Eventually, there is an nth ramification group such that G_{V_n} is not all of G. Since $G_{V_2} = G_T$, such an n must be greater than 2 and since G_{V_3} is a subgroup of H, n must be less than or equal to 3. Hence

$$H = G_{V_3},$$

the first nth ramification group that is not all of G. Since this is true for any subgroup H of index λ, G_{V_3} is the unique subgroup of G of index λ.

Showing that G has a unique subgroup of index λ is sufficient to show that G is cyclic. Since G is abelian, the structure theorem of finitely generated abelian groups, G is either isomorphic to $\mathbb{Z}_{\lambda^m}$, in which case G is cyclic, or G is isomorphic to $\mathbb{Z}_{\lambda^{e_1}} \times ... \times \mathbb{Z}_{\lambda^{e_s}}$ for some $s > 1$ and where $\lambda^{e_1} \cdot ... \cdot \lambda^{e_s} = \lambda^m$. If $s > 1$, then

$$\mathbb{Z}_{\lambda^{e_1-1}} \times \mathbb{Z}_{\lambda^{e_2}} ... \times \mathbb{Z}_{\lambda^{e_s}} \text{ and } \mathbb{Z}_{\lambda^{e_1}} \times ... \times \mathbb{Z}_{\lambda^{e_s-1}} \times \mathbb{Z}_{\lambda^{e_s-1}}$$

are two distinct subgroups of G with size $\lambda^{e_1-1} \cdot \lambda^{e_2} \cdot ... \cdot \lambda^{e_s} = \lambda^{e_1-1+e_2+...+e_s} = \lambda^{m-1} = \lambda^{e_1} \cdot ... \cdot \lambda^{e_{s-1}} \cdot \lambda^{e_s-1}$, or index λ. G has only one subgroup of index λ so we conclude that $s = 1$ and G is cyclic. □

Given this fourth lemma, we have enough material to show that the Kronecker-Weber theorem holds when λ is an odd prime.

Lemma 99. *If K is an abelian extension of $\mathbb{Q}$ of degree λ^m, where λ is an odd prime, then the Kronecker-Weber theorem holds for K.*

Proof. As before, it can be assumed that λ is ramified in K and is the only ramified prime in K (fact 4 and the third lemma). Consider the cyclotomic extension $\mathbb{Q}(\zeta)$, where ζ is a primitive λ^{m+1}th root of unity. $\mathbb{Q}(\zeta)$ has a cyclic Galois group of size $\lambda^m(\lambda - 1)$ over $\mathbb{Q}$ and has a unique subfield K' of degree λ^m over $\mathbb{Q}$. λ is the only ramified prime in K'.

We will show that K' and K are equivalent. If $K \neq K'$, then the composite extension KK' has degree strictly greater than λ^m because K and K' have the same degree over $\mathbb{Q}$ so inequality

implies neither is contained in the other. Then the smallest field containing K and K' must be a strictly larger extension of $\mathbb{Q}$ and so has degree greater than λ^m. Consequently, the Galois group of KK' over $\mathbb{Q}$, $\text{Gal}(KK'/\mathbb{Q})$ has size greater than λ^m. Also, λ is still the only ramified prime in KK'. With lemma 4, we can further say that $\text{Gal}(KK'/\mathbb{Q})$ is cyclic and thus some generator of order greater than λ^m. On the other hand, by fact 6, $\text{Gal}(KK'/\mathbb{Q})$ is isomorphic to a subgroup of $\text{Gal}(K/\mathbb{Q}) \times \text{Gal}(K'/\mathbb{Q})$ and every element of $\text{Gal}(K/\mathbb{Q}) \times \text{Gal}(K'/\mathbb{Q})$ has order less than or equal to λ^m. We have a contradiction and conclude that $K = K'$. In other words, K is a subfield of a cyclotomic extension. □

We have proved a partial result of the Kronecker-Weber theorem: the Kronecker-Weber theorem holds for abelian extensions of degree λ^m where λ is an odd prime. The proof depended on the fact that the degree of the extension of $\mathbb{Q}$ given by the λ^{m+1}th roots of unity is $\lambda^m(\lambda - 1)$. What if $\lambda = 2$? Then we have a different degree formula. Instead, we naturally look at quadratic extensions of $\mathbb{Q}$ and then apply the results for an extension of degree a power of 2.

Lemma 100. *If K is a quadratic extension of $\mathbb{Q}$, then K is contained in a cyclotomic extension.*

The results were proved on page 52. Specifically, we showed that

$$\mathbb{Q}\left(\sqrt{\pm p}\right) \subseteq \mathbb{Q}(\zeta_{4p})$$

for all p prime (including the prime 2). If m is not prime, m has a prime factorization

$$m = p_1 \cdot \ldots \cdot p_s$$

and $\mathbb{Q}(\sqrt{m}) \subseteq \mathbb{Q}\left(\sqrt{p_1}, \ldots, \sqrt{p_s}\right)$. Alternatively, $\mathbb{Q}\left(\sqrt{p_1}, \ldots, \sqrt{p_s}\right)$ is the minimal field containing all $\mathbb{Q}\left(\sqrt{p_i}\right)$ so $\mathbb{Q}\left(\sqrt{p_1}, \ldots, \sqrt{p_s}\right)$ is the composite of the $\mathbb{Q}\left(\sqrt{p_i}\right)$. Each $\mathbb{Q}\left(\sqrt{p_i}\right)$ is contained in the cyclotomic field $\mathbb{Q}\left(\zeta_{4p_i}\right)$. And the composite of cyclotomic fields is cyclotomic so the composite K of the $\mathbb{Q}\left(\zeta_{4p_i}\right)$ is cyclotomic. We conclude that

$$\mathbb{Q}\left(\sqrt{m}\right) \subseteq \mathbb{Q}(\sqrt{p_1}, \ldots, \sqrt{p_s}) \subseteq K$$

which shows $\mathbb{Q}(\sqrt{m})$ is contained in a cyclotomic extension.

Recall that in the second lemma, we showed it was only necessary to show the results of the Kronecker-Weber theorem hold for cyclic extensions of $\mathbb{Q}$. Using the latest lemma, we can show a cyclic extension of $\mathbb{Q}$ of degree 2^m are cyclotomic.

Lemma 101. *If K is a cyclic extension of $\mathbb{Q}$ of degree 2^m, then K is a cyclotomic extension of $\mathbb{Q}$.*

Proof. This proof is by induction on m. If $m = 1$, the extension is quadratic and by lemma 6 it is contained in a cyclotomic extension. Assume that a cyclic extension of degree 2^{m-1} is a cyclotomic extension of $\mathbb{Q}$ and consider a cyclic extension of degree 2^m. As usual, assume 2 is the only ramified prime in K (third lemma and fact 4).

We are taking extensions of $\mathbb{Q}$ so the field extension $K/\mathbb{Q}$ is contained in the greater field extension $\mathbb{C}/\mathbb{Q}$. If elements of K have complex components then complex conjugation is a nontrivial automorphism of K that fixes $\mathbb{Q}$ and has order 2. If K has no complex components, then complex conjugation is the identity function on K. Regardless, the subgroup of $\mathrm{Gal}(K/\mathbb{Q})$ generated by complex conjugation has a corresponding fixed field in K over $\mathbb{Q}$. In the first case where complex conjugation has order 2, the fixed field has degree 2^{m-1} over $\mathbb{Q}$ and in the second case, the fixed field is all K.

By assumption $\mathrm{Gal}(K/\mathbb{Q})$ is cyclic of order 2^m, so it has a unique subgroup of index 2 with $\mathrm{Gal}(K/\mathbb{Q})$ and consequently, K has a unique quadratic subfield K' (degree 2) over $\mathbb{Q}$. In particular, K' is contained in the fixed field of the subgroup of $\mathrm{Gal}(K/\mathbb{Q})$ so K' is fixed under complex conjugation. In other words, K' is real valued. Also, 2 is still the only ramified prime in K'. According to Zariski, in the quadratic field $\mathbb{Q}(\sqrt{m})$, where m is a square-free integer, the only ramified primes are 2, if $m \equiv 2$ or $3 \pmod 4$, and the odd prime divisors of m. [14, 314]. m cannot be a power of 2 because it is square-free. If m is anything other than 2, then some prime other than 2 divides m and that prime will be ramified. Since 2 is the only ramified prime, $K' = \mathbb{Q}\left(\sqrt{2}\right)$.

Let ζ be a primitive $(4 \cdot 2^m)$th root of unity. We will take a subset of $\mathbb{Q}(\zeta)$ that has the same degree over $\mathbb{Q}$ as K does. In particular, the cyclic subfield $L = \mathbb{Q}(\zeta + \zeta^{-1})$ has degree 2^m over $\mathbb{Q}$. As with K, it has a unique quadratic subfield. Since ζ is a primitive 2^{m+2}th root of unity, 2 is the only ramified prime in $\mathbb{Q}(\zeta)$ and *a fortiori*, in L. As with K, since 2 is the only ramified prime in L, the unique quadratic subfield is given by $\mathbb{Q}\left(\sqrt{2}\right)$. We will show that the composite KL is cyclotomic and thus K is cyclotomic.

Both K and L contain $\mathbb{Q}\left(\sqrt{2}\right)$ and

$$[K : \mathbb{Q}\left(\sqrt{2}\right)] = 2^{m-1} = [L : \mathbb{Q}\left(\sqrt{2}\right)].$$

Since the minimal subfield containing L and $\mathbb{Q}\left(\sqrt{2}\right)$ is L and has degree 2^{m-1} over $\mathbb{Q}\left(\sqrt{2}\right)$, and $\mathbb{Q}\left(\sqrt{2}\right) \subseteq K$, the minimal field containing K and L cannot be of degree greater than 2^{m-1}, the degree of L over $\mathbb{Q}\left(\sqrt{2}\right)$. Then the degree of KL must be less than 2^m over K and less than 2^{2m} over $\mathbb{Q}$. Since KL is an abelian extension, fact 6 gives that $\mathrm{Gal}(KL/\mathbb{Q})$ is isomorphic to a subgroup

of $\mathrm{Gal}(K/\mathbb{Q}) \times \mathrm{Gal}(L/\mathbb{Q})$ and is isomorphic to

$$\{(\sigma,\tau) : \sigma\,|_{K\cap L} = \tau\,|_{K\cap L}\}$$

where $\sigma \in \mathrm{Gal}(K/\mathbb{Q})$ and $\tau \in \mathrm{Gal}(L/\mathbb{Q})$.

Pick $\sigma \in \mathrm{Gal}(K/\mathbb{Q})$ and $\tau \in \mathrm{Gal}(L/\mathbb{Q})$ such that σ and τ match on $K \cap L$. Both $\mathrm{Gal}(K/\mathbb{Q})$ and $\mathrm{Gal}(L/\mathbb{Q})$ have order 2^m so σ and τ both have order 2^m. $(\sigma,\tau) \in \mathrm{Gal}(KL/\mathbb{Q})$ and the order of (σ,τ) is the least common multiple of the orders of σ and τ, 2^m. The cyclic subgroup $\langle(\sigma,\tau)\rangle$ has a fixed field F of index 2^r where $r < m$ since it has index less than $2^{2m}/2^m$. Furthermore, 2 is still the only ramified prime in F. Since $r < m$, the inductive hypothesis implies F is a subextension of a field obtained by adjoining a root of unity.

Consider the composite FL. As the composite of two cyclotomic extensions, FL is cyclotomic. Since F and L are contained in KL, FL is a subfield of KL. Then $\mathrm{Gal}(KL/FL)$ is the subgroup of $\mathrm{Gal}(KL/F)$ such that $\gamma \in \mathrm{Gal}(KL/F)$ is in $\mathrm{Gal}(KL/FL)$ if γ fixes the composite of F and L in addition to just fixing F. In particular, γ must fix L since L is contained in KL. But if γ also fixed L for some nontrivial γ, we would have $L \subseteq F$ since $\mathrm{Gal}(KL/F)$ cyclic which is a contradiction by degree of the extensions of L and F. Thus only the identity function in $\mathrm{Gal}(KL/F)$ is contained in $\mathrm{Gal}(KL/FL)$. Then $\mathrm{Gal}(KL/FL)$ is index 1 so $[KL : KF] = 1$ and $KL = KF$. We conclude that KF is cyclotomic and consequently, that K is cyclotomic. □

The series of lemmas given above are sufficient to proof the Kronecker-Weber Theorem. Let K be a cyclic extension of order a prime power λ^m such that every prime $p \neq \lambda$ is unramified in K. If λ is an odd prime, then K is a cyclotomic extension of $\mathbb{Q}$ by the lemma on page 68. If $\lambda = 2$, then K is a cyclotomic extension of $\mathbb{Q}$ by the lemma on page 69. Since any cyclic extension K of $\mathbb{Q}$ of order a prime power λ^m under the assumption that every prime $p \neq \lambda$ is unramified in K is cyclotomic, we conclude that any cyclic extension of $\mathbb{Q}$ of order a prime power λ^m is cyclotomic by the lemma on page 63. And since we now have that any cyclic extension of $\mathbb{Q}$ of a prime power order is cyclotomic, any abelian extension of $\mathbb{Q}$ is cyclotomic by the lemma on page 62. Thus the proof of the Kronecker-Weber Theorem is complete.

Bibliography

[1] David S. Dummit and Richard M. Foote. *Abstract algebra*. John Wiley & Sons Inc., Hoboken, NJ, third edition, 2004.

[2] Ervin Fried and János Kollár. Automorphism groups of algebraic number fields. *Math. Z.*, 163(2):121–123, 1978.

[3] M. Fried. A note on automorphism groups of algebraic number fields. *Proc. Amer. Math. Soc.*, 80(3):386–388, 1980.

[4] M. J. Greenberg. An elementary proof of the Kronecker-Weber theorem. *Amer. Math. Monthly*, 81:601–607, 1974.

[5] M. J. Greenberg. Correction to: "An elementary proof of the Kronecker-Weber theorem" (Amer. Math. Monthly **81** (1974), 601–607). *Amer. Math. Monthly*, 82(8):803, 1975.

[6] Serge Lang. *Algebraic number theory*, volume 110 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, second edition, 1994.

[7] Gunter Malle and B. Heinrich Matzat. *Inverse Galois theory*. Springer Monographs in Mathematics. Springer-Verlag, Berlin, 1999.

[8] Alexander Schmidt and Kay Wingberg. Safarevic's theorem on solvable groups as galois groups. 1998.

[9] John G. Thompson. Some finite groups which appear as $\mathrm{Gal}\,L/K$, where $K \subseteq \mathbf{Q}(\mu_n)$. *J. Algebra*, 89(2):437–499, 1984.

[10] Jean-Pierre Tignol. *Galois' theory of algebraic equations*. Longman Scientific & Technical, Harlow, 1988. Translated from the French by the author.

[11] Helmut Völklein. [review of the book inverse galois theory], 2001.

[12] Steven Weintraub. *Galois Theory*. Springer, 2005.

[13] Edwin Weiss. *Algebraic number theory*. McGraw-Hill Book Co., Inc., New York, 1963.

[14] Oscar Zariski and Pierre Samuel. *Commutative algebra. Vol. 1*. Springer-Verlag, New York, 1975. With the cooperation of I. S. Cohen, Corrected reprinting of the 1958 edition, Graduate Texts in Mathematics, No. 28.