SJÄLVSTÄNDIGA ARBETEN I MATEMATIK

MATEMATISKA INSTITUTIONEN, STOCKHOLMS UNIVERSITET

The multiple occurances of the Galois correspondence

av

Oskar Frost

2017 - No 24

The multiple occurances of the Galois correspondence

Oskar Frost

Självständigt arbete i matematik 15 högskolepoäng, grundnivå

Handledare: Wushi Goldring

2017

The multiple occurances of the Galois correspondence

Oskar Frost
Supervisor: Wushi Goldring

June 7, 2017

Abstract

In this thesis, we will present two theorems with similar structures from the fields of algebra and topology. These theorems are commonly referred to as the Galois correspondence and focus on field extensions and covering spaces. Both field extensions and covering spaces can be assigned a group of automorphisms. The Galois correspondence then means that there is a 1-1 correspondence between subgroups of the automorphism group, and intermediate field extensions/covering spaces. The objective of this thesis is to highlight the similar background of both of these topics.
In the last section, the inverse Galois problem for $\mathbb{C}(t)$ will be solved as an application where the Galois correspondence of topology is used for results in the algebric counterpart.

Acknowledgements

I would like to thank my supervisor Wushi Goldring for his support and helpful advice during critical periods in the writing process.

Contents

Introduction

The field of Galois theory is situated in the topic of algebra. The name originates from the French mathematician Évariste Galois (1811-1832) who made this specific theory evolve. Galois theory originates in the study of fields and polynomial equations. Polynomials which do not have any roots in a given field exist. This naturally leads to the question whether larger fields exist that contain these roots. The answer to this question is yes. Hence as long as polynomials exist in a given field without roots, then there must be bigger fields that extend the original one. An additional question might be if fields exist that cointain the original field, but that are still is contained in the first extension. If so, how many intermediate fields are there and how do they structure? *The Galois correspondence* is the groundwork on which the whole Galois theory builds upon and answers these questions. The theorem uses sufficiently large field extensions called Galois extensions. These extensions are obtained by adding all the solutions of a polynomial without any multiple roots to a field. It is for these extensions that the theorem holds. Further on, this theorem will be referred to as theorem A.

Theorem 0.0.1 (Theorem A)**.** Let F be a field and $f(x)$ some polynomial in $F[x]$ without any multiple roots. Let K be the field obtained by adding all the roots of $f(x)$ to F. Then we can associate a group $\mathrm{Gal}(K/F)$ to K as an extension of F. Let $A = \{\text{Fields } M \text{ such that } F \subset M \subset K\}$. Then there is a 1-1 correspondence between the subgroups of $\mathrm{Gal}(K/F)$ and A. This correspondence has the properties that if M_1, M_2 are fields in A corresponding to the subgroups H_1, H_2 respectively, then $M_1 \subset M_2$ if and only if $H_1 \supset H_2$.

Chapter 1 will be devoted to thoroughly introduce the topic of Galois theory and to prove the Galois correspondence. In order to understand the concepts better, this study focuses on a relatively small number of proofs, and instead uses many examples.

The second part of this thesis is about a theorem in topology wich has a striking resemblance to theorem A. The main study of topology is topological spaces and what maps exist between them. Our interest here will be of open covers. They consist of two spaces X, Y with a continuous and surjective map $p : Y \to X$ with a certain property. Namely, each point in X has a neighbourhood such that its preimage consists of disjoint open sets in Y, so that each of

these sets is homeomorphic to the neighbourhood in X. An illustrative example is the real numbers and the circle with the exponential map $p(x) = \mathrm{e}^{2\pi ix}$.

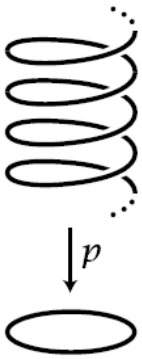


Figure 1. The real line projected down on a circle.

The real line is here presented as the upper spring-like curve and it is projected downwards onto the circle by the map p. It is easy to see that these spaces would satisfy the definition of a covering space. The theorem in topology that resembles theorem A will be called theorem B, and involves special covering spaces called Galois covers (by the resemblance to Galois theory). It is for these covers that the following hold.

Theorem 0.0.2 (Theorem B)**.** Let $p : Y \to X$ be a Galois cover. Then we can associate a group $\mathrm{Gal}(Y/X)$ to the open cover. Let B be the set of spaces Z so that the diagram below commutes and that each of the maps is an open cover.

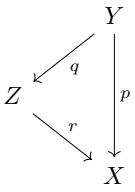


Figure 2. A commutative diagram of open covers.

Then there is a 1-1 correspondence between the subgroups of $\mathrm{Gal}(Y/X)$ and the set B. This correspondence has the property that if Z_1, Z_2 are spaces in B corresponding to the subgoups H_1, H_2 respectively, then there is a covering map $f : Z_1 \mapsto Z_2$ if and only if $H_1 \supseteq H_2$.

Chapter 2 properly introduce the concept of open covers and prove theorem B. The focus will be on similarities and differences between covering spaces and fields, so not many examples are discussed.

The third and last part will see an application of when Galois in topology is used to show a result for Galois in algebra. As we have seen, given a field F,

there are ways to extend this to a field K by adding roots of polynomials. Some of these extensions have the property of being Galois, to which we can associate a group. It is known that all fields have such Galois extensions. The question we want to answer is the opposite. That is, given a field F, do Galois field extensions exist so that each finite group is associated to them? This question is commonly referred to as *the inverse Galois problem*. The question is still unanswered for $F = \mathbb{Q}$. But when F is the field of complex rational functions, this holds true. We will in chapter 3 touch upon the necessary results to show that the inverse Galois is true for the field of complex rational functions, denoted $\mathbb{C}(t)$. The aim is to give a brief overview of the different results with a sufficient amount of attention paid to details.

Chapter 1

Galois Theory

Abstract algebra is one of the broadest fields in mathematics, often intersecting with many other areas. For example analysis, geometry and combinatorics to name a few. Some of the more fundamental objects of algebra are groups, rings and fields. In many cases, when given a group or field, we want to investigate the subgroups of this group. Galois Theory does the opposite from this point of view. Given a field, we do not so much ask about the subfields in it, but rather in what ways we are able to add elements to this field, thereby extending it. One may pose questions about these field extensions. Do they for instance all have the same properties, or do some differ from others?
One kind of extension is called Galois which will be introduced in section 1.3. These particular extensions play a vital role in the fundamental correspondence of Galois Theory, which will be the topic of section 1.4. But before that we first need to properly define field extensions, and further introduce some fundamental field extensions, which will be done in sections 1.1 and 1.2 respectively.

1.1 Field extensions

Definition 1.1.1. Let K be a field and F a subfield. Then K is called an extension of F, denoted by K/F, and F is called the base of the extension.

Remark. It will be useful in coming chapters to have a precise meaning of F being a subfield of K. F is a subfield of K if there exists an injective homomorphism $\varphi : F \to K$. The following diagram, where the hook symbolizes injectivity, will be in common practice throughout.

$$\begin{array}{c} K \\ \uparrow \\ F \end{array}$$

Figure 3. An injective field homomorphism.

The hypothesis that the homomorphism is injective is actually superfluous. Non-trivial homomorphisms of fields are always injective. For clarity, injective homomorphism will nonetheless be used throughout.

Example 1.1.2. If K/F is an extension, then it is clear that K/F fulfils the axioms of a vector space, when the elements of F are interpreted as scalars. This can be exemplified by the complex numbers $\mathbb{C}$, seen as an extension of the real numbers $\mathbb{R}$. All complex numbers can be written on the form $a + bi$, where $a, b \in \mathbb{R}$. So, the vector space $\mathbb{C}/\mathbb{R}$ has 1 and i as a basis. Hence, the space is of dimension two.

The fact that we can interpret K as a vector space over F motivates the following definition.

Definition 1.1.3. Let K/F be an extension. The degree of K/F is the dimension of K as a vector space over F, denoted by $[K : F]$. We say that an extension is finite if its degree is finite.

Proposition 1.1.4. If K/L and L/F are two finite field extensions, then K/F is also a finite extension where $[K : F] = [K : L][L : F]$.

Proof. See [1, p.523-524]. □

Example 1.1.5. In example 1.1.2, we saw that $\mathbb{C}/\mathbb{R}$ is a vector space of dimension two, hence it is a finite extension of degree two. On the other hand, the extension $\mathbb{R}/\mathbb{Q}$ is infinite.

Why is it that the extension $\mathbb{R}/\mathbb{Q}$ is infinite? In order to answer that question, we need to introduce some further concepts.

Definition 1.1.6. Let K/F be an extension. An element $\alpha \in K$ is said to be algebraic over F if there exists a polynomial $p(x) \in F[x]$ so that $p(\alpha) = 0$. If no such polynomial exists, then α is said to be transcendental over F.
If all elements of a field K are algebraic over some subfield F, then we say that K is algebraic over F, and transcendental otherwise.

Example 1.1.7. $\sqrt{2} \in \mathbb{R}$ is algebraic over $\mathbb{Q}$, since it is a root of the polynomial $x^2 - 2$ in $\mathbb{Q}(x)$. $i \in \mathbb{C}$ is also algebraic over $\mathbb{Q}$ by the polynomial $x^2 + 1$. On the other hand, there is no polynomial with coefficients in $\mathbb{Q}$ such that $\pi \in \mathbb{R}$ is a root (See [5, section 24.2]). Hence, π is transcendental over $\mathbb{Q}$.

Proposition 1.1.8. If an extension K/F is finite, then K is algebraic over F.

Proof. See [1, p.522] □

Example 1.1.9. Now we can justify our claim in example 1.1.5, namely that the extension $\mathbb{R}/\mathbb{Q}$ is of infinite degree. By example 1.1.7 we saw that this extension is transcendental, and so it must be of infinite degree by proposition 1.1.8. By the same proposition, we have that $\mathbb{C}/\mathbb{R}$ is an algebraic extension since we saw that the degree is finite.

Definition 1.1.10. Let F be a field. F is said to be algebraically closed if $K = F$ for every algebraic extension K/F.

As we have seen, polynomials play a central role when studying field extensions. We now introduce two properties of polynomials, irreducibility and separability, which will prove important in the later characterisation of Galois extensions.

Definition 1.1.11. A polynomial $f(x) \in F[x]$ is reducible in F if there exists polynomials $p(x), q(x) \in F[x]$ of degree greater than zero such that $f(x) = p(x)q(x)$. If f is not reducible, then we say that f is irreducible.

Notice that a polynomial may be irreducible in one field F, but reducible in some extension of F. For example $x^2 - 2$ is irreducible in $\mathbb{Q}$, but it is reducible in $\mathbb{R}$.

Proposition 1.1.12. Suppose $f(x) \in F[x]$ and $\alpha \in F$. Then

$$f(\alpha) = 0 \text{ if and only if } (x - \alpha)|f(x) \text{ in } F[x].$$

Proof. Assume $(x - \alpha)|f(x)$ in $F[x]$. This is equivalent to $f(x) = (x - \alpha)g(x)$ for some $g(x) \in F[x]$. Now

$$f(\alpha) = (\alpha - \alpha)g(\alpha) = 0.$$

Assume $f(\alpha) = 0$. Then the Euclidian algorithm gives

$$f(x) = (x - \alpha)g(\alpha) + r(x)$$

for some $g(x), r(x) \in F[x]$ where deg $r(x) < 1$. So $r(x) = c$ for some $c \in F$. Then from the hypothesis we gather

$$f(\alpha) = (\alpha - \alpha)g(\alpha) + c = 0 \Leftrightarrow c = 0,$$

and so

$$f(x) = (x - \alpha)g(x) \Leftrightarrow (x - \alpha)|f(x),$$

which completes the proof. □

Definition 1.1.13. Let $f(x) \in F[x]$ for some field F. An element $\alpha \in F$ is a root of f of multiplicity $n \in \mathbb{Z}$ if

$$(x - \alpha)^n | f(x) \text{ but } (x - \alpha)^{n+1} \not| f(x) \text{ in } F[x].$$

If $n = 1$, then α is called a simple root, and if $n \geq 2$ then α is called a multiple root.

Definition 1.1.14. If $f(x) \in F[x]$ only has simple roots, then $f(x)$ is called separable.

Theorem 1.1.15. Let K/F be an extention, and $\alpha \in K$ an algebraic element over F. Then there exists a unique monic polynomial $f(x) \in F[x]$ such that $f(\alpha) = 0$ with the properties

a) $g(\alpha) = 0$ for $g(x) \in F[x]$ if and only if $f(x)|g(x)$ in $F[x]$.

b) $f(x)$ is irreducible in $F[x]$.

Proof. See [1, p.520] □

Definition 1.1.16. The polynomial $f(x)$ in the previous theorem is called the minimal polynomial for α over F and is denoted by $m_{\alpha,F}(x)$.

Example 1.1.17. (Minimal polynomials)

- $x^2 - 2$ is the minimal polynomial for $\sqrt{2}$ in $\mathbb{Q}$.
- $x^3 - 2$ is the minimal polynomial for $\sqrt[3]{2}$ in $\mathbb{Q}$.

1.2 Fraction fields and two extensions

In this section, we will introduce three common ways of creating fields, namely fraction fields, adding elements to existing fields and splitting fields.
First up is the creation of fields from rings. A ring may be viewed as an incomplete field, since it usually lacks multiplicative inverses for some elements. We further assume that the ring is an integral domain, since it is not possible to find an inverse to nilpotent elements.

Theorem 1.2.1. Let R be a ring which is an integral domain. Then there exists a field $Frac(R)$ so that

a) There exist an injective homomorphism $\iota : R \to Frac(R)$, i.e R is a subring of the field $Frac(R)$

b) $Frac(R)$ is the smallest field containing R.

Proof. See [1, section 7.5]. □

Definition 1.2.2. The field $Frac(R)$ is called the fraction field of R.

Example 1.2.3. $\mathbb{Q}$ is the fraction field of the ring $\mathbb{Z}$. Outline: Consider the set $G = \{(a, b) \in \mathbb{Z} \times \mathbb{Z} | b \neq 0\}$. Define a relation $\sim$ on G so that $(a, b) \sim (c, d)$ if $ad = bc$. $\sim$ is an equivalence relation on G, and we denote the equivalence classes as $[a, b]$. First we introduce two operators $+, \cdot$, defined as $[a, b] + [c, d] = [ad + bc, bd]$, $[a, b] \cdot [c, d] = [ac, bd]$. These operations are independent of which representatives $a, b, c, d \in \mathbb{Z}$ we use for the equivalence classes. From this construction it is easy to verify that this is actually the field $\mathbb{Q}$, even though its elements usually are represented as $\frac{a}{b}$ and not $[a, b]$.
Another fraction field, which will be our main interest in chapter 3, is the fraction field of the polynomial ring $\mathbb{C}[t]$. It is usually denoted by $\mathbb{C}(t)$. First, note that $\mathbb{C}$ is a subfield of $\mathbb{C}(t)$, represented by the constant functions. Second, it is also a transcendental extension over the field of complex numbers. This follows from the fact that $\mathbb{C}$ is algebraically closed, and so every polynomial with complex coefficients can be fully factorized into linear factors.

Next up is field extensions generated by adding an algebraic element to an existing field. Algebraic elements are by definition roots to some irreducible polynomial.

Definition 1.2.4. Let K/F be an extension and $\alpha \in K$ an algebraic element over F. Then we let $F(\alpha)$ be the smallets subfield of K containing F and α.

Proposition 1.2.5. Let K/F be an extension and $\alpha \in K$ an algebraic element over F. Define a function $\text{eval}_\alpha : F[x] \to K$ such that $f \mapsto f(\alpha)$ for $f \in F[x]$. Then:

- eval_α is a ring homomorphism
- $\text{Ker}(\text{eval}_\alpha) = (m_{\alpha,F}(x))$ (The ideal generated by $m_{\alpha,F}$)
- $\text{Im}(\text{eval}_\alpha)$ is the smallest subfield of K containing F and α.

Proof. See [1, p.517] □

Remark. Hence, we have got a description of $F(\alpha)$. By the isomorphism theorem we have $F(\alpha) \cong F[x]/(m_{\alpha,F}(x))$. Something interesting arises here. If α and β have the same minimal polynomial, then $F(\alpha) \cong F(\beta)$. We then say that these are algebraically indistinguishable.

Now that we have found a precise way of describing the field $F(\alpha)$, it would be useful to find a good representation of the elements as well. Here, the minimal polynomial plays a vital role. First of all, note that the minimal polynomial essentially is a relation between the newly added element and the base field (the field where the polynomial is defined). Consider $m_{\sqrt{2},\mathbb{Q}}(x) = x^2 - 2$ and assume that θ is the root of the polynomial. Then θ fulfils the relation $\theta^2 = 2$ (and we know that the roots of $m_{\sqrt{2},\mathbb{Q}}(x)$ are the only ones to do so). Thus, elements of the form $a + b\theta$, $a, b \in \mathbb{Q}$ would certainly be in $\mathbb{Q}(\alpha)$. These elements would also be minimal in the sense that powers of θ greater than 1 could always be reduced. Hence we would expect that 1 and θ are basis elements of $\mathbb{Q}(\theta)$ seen as a vector space over $\mathbb{Q}$. It turns out that these expectations are true.

Proposition 1.2.6. Let F be a field, $f(x) \in F[x]$ be an irreducible polynomial of degree n, and let θ be a root of $f(x)$ in some extension of F. Then

- $[F(\theta) : F] = n$
- $1, \theta, \theta^2, ..., \theta^{n-1}$ are a basis for $F(\theta)$

Proof. See [1, p.513] □

Example 1.2.7. (Bases of field extensions)

- The field extension $\mathbb{Q}(\sqrt{2})/\mathbb{Q}$ is of degree 2, and $(1, \sqrt{2})$ is a basis. So $\mathbb{Q}(\sqrt{2}) = \{a + b\sqrt{2} | a, b \in \mathbb{Q}, \sqrt{2}^2 = 2\}$.

- Consider the polynomial $p(x) = x^3 - 2x + 2$ in $\mathbb{Q}(x)$. By the rational root test we see that this is irreducible, hence proposition 1.2.6 is applicable. Let θ be a root of $p(x)$ in some extension of $\mathbb{Q}$. Then we get the relation $\theta^3 = 2\theta - 2$, which we can use to reduce powers of θ greater than 2. So a calculation might look like

$$\begin{aligned}(1+\theta^2)(3-\theta) &= 3 - \theta + 3\theta^2 - \theta^3 \\ &= 3 - \theta + 3\theta^2 - 3(2\theta - 2) \\ &= 9 - 7\theta + \theta^2\end{aligned}$$

- Let $f(x) = x^n - 1$ for some integer n. The roots of polynomials like these are called the nth roots of unity. They are easily described in their complex form $(1, e^{\frac{2\pi i}{n}}, e^{\frac{2\pi i}{n}\cdot 2}, ..., e^{\frac{2\pi i}{n}\cdot(n-1)})$. These elements are actually a cyclic group, and $e^{\frac{2\pi i}{n}}$ is a generator. In fact, $e^{\frac{2\pi i}{n}\cdot k}$ generates the group if and only if k and n are relatively prime. Hence, there are $\varphi(n)$ generators of this group that are usually called the nth primitive roots of unity. Let ζ_n be some primitive nth root of unity. The only roots of the minimal polynomial $m_{\zeta_n,\mathbb{Q}}(x)$ are actually all primitive nth roots. So by adding ζ_n to $\mathbb{Q}$, not only do $x^n - 1$ completely factor into linerar factors, but we know that $[\mathbb{Q}(\zeta_n) : \mathbb{Q}] = \varphi(n)$. This will be of further interesest in example 1.3.3.

Definition 1.2.8. A polynomial $f(x) \in F[x]$ is said to split completely over F if it can be factorized as a product of linear factors in $F[x]$.

Note that even though we extend a field F by adding an algebraic element α, this does not imply that the minimal polynomial $m_{\alpha,F}(x)$ splits completely in $F(\alpha)$. Consider the case when $\alpha = \sqrt[3]{2}$. Here we have that $m_{\sqrt[3]{2},\mathbb{Q}}(x) = x^3 - 2$, but in $\mathbb{Q}(\sqrt[3]{2})$ we have that $m_{\sqrt[3]{2},\mathbb{Q}}(x) = (x - \sqrt[3]{2})(x^2 + \sqrt[3]{2}x + \sqrt[3]{2^2})$. The missing roots are in this case the complex numbers $\sqrt[3]{2}e^{\frac{2\pi i}{3}}$ and $\sqrt[3]{2}e^{\frac{2\pi i\cdot 2}{3}}$. If we want to ensure that a polynomial splits completely in a field extension, then we turn to what is called splitting fields.

Definition 1.2.9. An extension K/F is a splitting field for some $f(x) \in F[x]$ if

a) $f(x)$ factors completely in K

b) If $f(x)$ factors completely in some subfield of K' of K ($F \subset K' \subset K$), then $K = K'$.

Remark. All polynomials do have some splitting field. These fields are isomorphic up to isomorphism. For further details, see [1, p.536; p.542]

Example 1.2.10. (Splitting fields)

- The extension $\mathbb{Q}(\sqrt{2})/\mathbb{Q}$ is a splitting field for the polynomial $x^2 - 2$, since it factors as $(x + \sqrt{2})(x - \sqrt{2})$.

- Let $f(x) = x^n - 1$. In example 1.2.7 we saw that the roots of $f(x)$ forms a cyclic group. Let ζ_n be a nth primitive root (equivalently a generator for the group). By adding this element to $\mathbb{Q}$ all other roots of $f(x)$ will also be included, hence $\mathbb{Q}(\zeta_n)$ is a splitting field for $f(x)$.

- Let $f(x) = x^3 - 2$. As noted, the roots of this polynomial are $\sqrt[3]{2}$, $\sqrt[3]{2}\zeta_3$ and $\sqrt[3]{2}\zeta_3^2$. Hence, $\mathbb{Q}(\sqrt[3]{2}, \sqrt[3]{2}\zeta_3, \sqrt[3]{2}\zeta_3^2)$ is a splitting field of $f(x)$. Yet we might want to find an easier way of describing this field. First note that $\sqrt[3]{2}$ and ζ_3 together can describe the roots of $f(x)$. So $\mathbb{Q}(\sqrt[3]{2}, \sqrt[3]{2}\zeta_3, \sqrt[3]{2}\zeta_3^2) \subset \mathbb{Q}(\sqrt[3]{2}, \zeta_3)$. Similarly we find that $\zeta_3 \in \mathbb{Q}(\sqrt[3]{2}, \sqrt[3]{2}\zeta_3, \sqrt[3]{2}\zeta_3^2)$. Thus, the splitting field of f is equivalent to $\mathbb{Q}(\sqrt[3]{2}, \zeta_3)$.

1.3 Galois extensions

Polynomials and their roots are vital in the study of field extensions. What Galois brings to the table is to study how the roots of polynomials can permute. These permutations create automorphisms of the field extension, leaving the base field unchanged. The set of automorphisms of this kind creates a group. This reduces the study of fields to the study groups which are easier to work with because of their simple structure.

Definition 1.3.1. Let K/F be an extension. We then define $\mathrm{Aut}(K)$ as the set of automorphisms of K and $\mathrm{Aut}(K/F)$ as the set of automorphisms of K fixing F.

Remark. By the properties of automorphisms, it is evident that $\mathrm{Aut}(K)$ is a group under composition. Similarly one sees that $\mathrm{Aut}(K/F)$ is a subgroup.

Proposition 1.3.2. Let F be a field, α some algebraic element in an extension K/F and $m_{\alpha,F}(x)$ the minimal polynomial. If $\sigma \in \mathrm{Aut}(K/F)$, then $\sigma(\alpha)$ is a root of $m_{\alpha,F}(x)$.

Proof. See [1, p.559]. □

So, $\mathrm{Aut}(K/F)$ can only permute the roots of irreducible polynomials. This result will be of great use when trying to calculate the automorphism group for extensions.

Example 1.3.3. (Automorphism groups)

- Let $K = \mathbb{Q}(\sqrt{2})$ and $F = \mathbb{Q}$. The elements of K are on the form $a + b\sqrt{2}$, $a, b \in F$. Since any $\sigma \in \mathrm{Aut}(K/F)$ fixes F, the automorphism is only determined of where it maps $\sqrt{2}$. We have that $m_{\sqrt{2},F}(x) = (x-\sqrt{2})(x+\sqrt{2})$. By proposition 1.3.2, every automorphism maps $\sqrt{2}$ to either $\sqrt{2}$ or $-\sqrt{2}$. Both of these are automorphisms and they are the only ones. Hence $|\mathrm{Aut}(K/F)| = 2$.

- Let $K = \mathbb{Q}(\sqrt[3]{2})$ and $F = \mathbb{Q}$. The elements of K are on the form $a + b\sqrt[3]{2} + c\sqrt[3]{4},\ a, b, c \in F$. By the same argument as in the previous example, the automorphisms in $\mathrm{Aut}(K/F)$ are only determined by where they map $\sqrt[3]{2}$. But the roots of $m_{\sqrt[3]{2},F}$ are $\sqrt[3]{2}, \sqrt[3]{2}\zeta_3, \sqrt[3]{2}\zeta_3^2$. The last two are not in K, and so $\sqrt[3]{2}$ can not be mapped there. The only choice left is that $\sqrt[3]{2}$ maps to itself. Hence $\mathrm{Aut}(K/F) = \{e\}$.

- Let K be the splitting field of $x^3 - 2$ over $\mathbb{Q}$. In example 1.2.10 we saw that $K = \mathbb{Q}(\sqrt[3]{2}, \zeta_3)$. The elements of $\mathrm{Aut}(K/F)$ are determined by where they map $\sqrt[3]{2}$ and ζ_3. Consider the maps:

$$\sigma : \begin{cases} \sqrt[3]{2} \mapsto \sqrt[3]{2}\zeta_3 \\ \zeta_3 \mapsto \zeta_3 \end{cases} \qquad \tau : \begin{cases} \sqrt[3]{2} \mapsto \sqrt[3]{2} \\ \zeta_3 \mapsto \zeta_3^2 \end{cases}$$

  First we want to esatablish that σ and τ are automorphisms. We will do this by showing that the action of these maps on the basis vectors gives the same space. A basis for the extensions $\mathbb{Q}(\sqrt[3]{2})\mathbb{Q}$ is $(1, \sqrt[3]{2}, \sqrt[3]{4})$ by proposition 1.2.6. For now, we claim that $[\mathbb{Q}(\sqrt[3]{2}, \zeta_3) : \mathbb{Q}(\sqrt[3]{2})] = 2$ (this will be showed later in example 1.3.5). Then again by proposition 1.2.6, the extension $\mathbb{Q}(\sqrt[3]{2}, \zeta_3)/\mathbb{Q}$ has the basis $(1, \sqrt[3]{2}, \sqrt[3]{4}, \zeta_3, \zeta_3\sqrt[3]{2}, \zeta_3\sqrt[3]{4})$. σ maps these elements to $(1, \zeta_3\sqrt[3]{2}, \zeta_3^2\sqrt[3]{4}, \zeta_3, \zeta_3^2\sqrt[3]{2}, \sqrt[3]{4})$. It is easily shown that these two sets of elements can be expressed by each other. So since the first one was a basis, the other one must be too. In a similar fashion, we can show this for τ, and then easily check that σ and τ are homomorphisms. To better visualize σ and τ, we consider where they map the roots of $x^3 - 2$. If we let $\alpha_1 = \sqrt[3]{2}, \alpha_2 = \sqrt[3]{2}\zeta_3, \alpha_3 = \sqrt[3]{2}\zeta_3^2$, then σ and τ can be presented on cyclic notation. Then $\sigma = (123)$ and $\tau = (23)$. By some computation, we see that these elements generate the whole of S_3. So we conclude that $\mathrm{Aut}(K/F) \cong S_3$.

- Let K be the splitting field of $x^n - 1$ and $F = \mathbb{Q}$. As seen in example 1.2.10, $K = \mathbb{Q}(\zeta_n)$ where ζ_n is a primitive nth root of unity. In example 1.2.7, we noted that ζ_n^a too is a primitive nth root of unity when n and a are relatively prime. We also noted that the primitive nth roots of unity are the roots of the same irreducible polynomial. So then the automorphisms

$$\sigma_k : \zeta_n \mapsto \zeta_n^k, \quad \text{for} 1 \leq k \leq n \text{ and } (k, n) = 1$$

  are in $\mathrm{Aut}(K/F)$. These are in fact the only automorphisms, since ζ_n is mapped to each of the primitive nth roots, i.e the roots of $m_{\zeta_n,F}$.

  From here, it is not hard to verify that $\mathrm{Aut}(K/F) \cong (\mathbb{Z}/n\mathbb{Z})^\times$.

Definition 1.3.4. Let K/F be a finite extension. Then K/F is said to be Galois if $[K : F] = \mathrm{Aut}(K/F)$, in which case we denote the automorphism group by $\mathrm{Gal}(K/F) := \mathrm{Aut}(K/F)$.

Remark. In general, the automorphism group is smaller than the index.

Example 1.3.5. (Galois extensions)

- The extension $\mathbb{Q}(\sqrt[3]{2})/\mathbb{Q}$ is not Galois. From example 1.3.3 we saw that $|\mathrm{Aut}(\mathbb{Q}(\sqrt[3]{2})/\mathbb{Q})| = 1$, while $[\mathbb{Q}(\sqrt[3]{2}) : \mathbb{Q}] = 3$.
- Let K be the splitting field of $x^3 - 2$ and $F = \mathbb{Q}$. $|\mathrm{Aut}(K/F)| = 6$ by example 1.3.3. We have seen that $K\mathbb{Q}(\sqrt[3]{2}, \zeta_3)$, so we get the diagram:

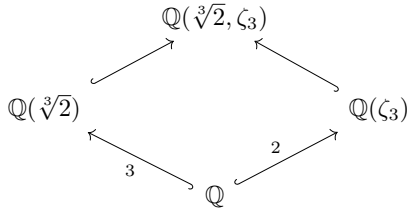


Figure 4. Diagram of field extensions.

Now we get that

$$[\mathbb{Q}(\sqrt[3]{2}, \zeta_3) : \mathbb{Q}(\sqrt[3]{2})] \cdot 3 = [\mathbb{Q}(\sqrt[3]{2}, \zeta_3) : \mathbb{Q}]$$
$$[\mathbb{Q}(\sqrt[3]{2}, \zeta_3) : \mathbb{Q}(\zeta_3)] \cdot 2 = [\mathbb{Q}(\sqrt[3]{2}, \zeta_3) : \mathbb{Q}].$$

The degree $[\mathbb{Q}(\sqrt[3]{2}, \zeta_3) : \mathbb{Q}(\sqrt[3]{2})]$ is equal to the degree of the minimal polynomial $g(x)$ of ζ_3 over $\mathbb{Q}(\sqrt[3]{2})$. But $\deg(m_{\zeta_3,\mathbb{Q}}) = 2$ and it must divide $g(x)$, so the degree of $g(x)$ is smaller or equal to 2. The equations above say that $[\mathbb{Q}(\sqrt[3]{2}, \zeta_3) : \mathbb{Q}]$ divides 2, so it must be that $[\mathbb{Q}(\sqrt[3]{2}, \zeta_3) : \mathbb{Q}(\sqrt[3]{2})] = 2$. Hence $[\mathbb{Q}(\sqrt[3]{2}, \zeta_3) : \mathbb{Q}] = 6$. Hence, $[\mathbb{Q}(\sqrt[3]{2}, \zeta_3) : \mathbb{Q}] = |\mathrm{Aut}(K/F)|$ and so the extension K/F is Galois.

Definition 1.3.6. Let $H \subset \mathrm{Aut}(K)$ be a finite subgroup. The we define $K^H = \{g \in K | \sigma(g) = g, \text{ for all } \sigma \in H\}$. K^H is a subfield of K and is called the fixed field of H.

Example 1.3.7. Let $K = \mathbb{Q}(\sqrt[3]{2})$, $F = \mathbb{Q}$ and $G = \mathrm{Aut}(K/F)$. In example 1.3.3, we saw that $G = \{e\}$. So, $K^G = K$, since the identity fixes all elements of K.

The definition of Galois extensions may at first seem cryptic. The two concepts of index and size of the automorphism group do not immediately relate in any meaningful way. Even so, this definition shows to be a connection of two fundamental building blocks of the Galois correspondence, namely, fixing field of the automorphism group, and splitting fields for separable polynomials. For example, note in example 1.3.5 that the splitting field of $x^3 - 2$ is Galois. We state the precise theorems.

Theorem 1.3.8. Let $G = \{\sigma_1 = 1, \sigma_2, \ldots, \sigma_n\}$ be a subgroup of automorphisms of a field K and let F be the fixed field. Then

$$[K : F] = |G| = n$$

Proof. See [1, p.570]. □

Corollary 1.3.9. Let K/F be any finite extension. Then

$$|\mathrm{Aut}(K/F)| \leq [K : F]$$

with equality if and only if F is the fixed field of $\mathrm{Aut}(K/F)$.

Proof. Let K/F be any finite extension and F' the fixed field of $\mathrm{Aut}(K/F)$. Then proposition 1.1.4 and theorem 1.3.8 together gives

$$\begin{aligned} |\mathrm{Aut}(K/F)| &= [K : F'] \\ [K : F] &= [K : F'][F' : F] \\ [K : F] &= |\mathrm{Aut}(K/F)|[F' : F]. \end{aligned}$$

Now $[K : F] = |\mathrm{Aut}(K/F)|$ if and only if $[F' : F] = 1$, i.e when F is the fixed field of $\mathrm{Aut}(K/F)$. □

Another useful property of fixing fields is that it is easy to find the automorphism group.

Corollary 1.3.10. Let K be a field, $H \subset \mathrm{Aut}(K)$ a finite subgroup and $K^H = M$. Then $\mathrm{Aut}(K/M) = H$.

Proof. We have that $H \subseteq \mathrm{Aut}(K/M) \subseteq \mathrm{Aut}(K)$. Then we get

$$|H| = [K : M] \leq |\mathrm{Aut}(K/M)| \leq |H|.$$

So $\mathrm{Aut}(K/M) = H$. □

Theorem 1.3.11. Let K/F be a finite extension. Then we have that K/F is Galois if and only if K is a splitting field of some separable polynomial $f(x) \in F[x]$ over F.

Proof. See [1, p.572-573] □

Proposition 1.3.12. Let $f(x) \in F[x]$ be an irreducible and separable polynomial in a field F and let K be the splitting field of $f(x)$ over F. Then the group $Gal(K/F)$ acts transitively on the roots of $f(x)$.

Proof. See [1, p.606]. □

Hence, we now have three ways of characterizing a Galois extension. We summarize: If the extension K/F is Galois, then the following are equivalent:

- $[K : F] = \mathrm{Aut}(K/F)$.
- K is a splitting field over F for some irreducible polynomial $f \in F[x]$.
- The fixing field of $\mathrm{Aut}(K/F)$ is F.

1.4 The Galois correspondence

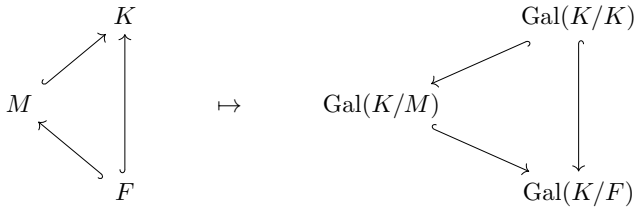
In this section we are able to properly state the Galois correspondence (Theorem A) in detail and prove the main part. Furthermore, we will look at some examples of how this structure unfolds. We end by analysing some applications of Galois theory, a generalization reaching to infinite field extensions and stating the inverse Galois problem.

Theorem 1.4.1. Let K/F be a finite Galois extension and $G = \mathrm{Gal}(K/F)$. Then there is a 1-1 correspondence between intermediate subfields $F \subset M \subset K$ and subgroups $G \supset H \supset \{e\}$

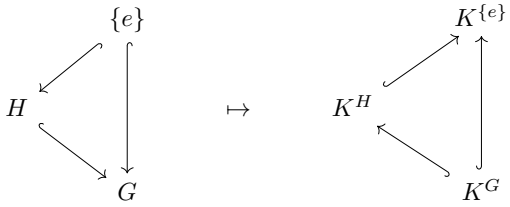
Figure 5. Commutative diagrams of corresponding fields and groups.

such that K/M is Galois. The correspondence is given by

- M correspond to $\mathrm{Gal}(K/M)$:



- H correspond to K^H:



Furthermore, this correspondence has the properties

a) Let M_1, M_2 be subfields of K and let H_1, H_2 be their corresponding subgroups of G. Then $M_1 \subseteq M_2$ if and only if $H_1 \supseteq H_2$.

b) The extension M/F is Galois if and only if H is normal in G.

Proof. We show is that the correspondence {Subgroup} $\to$ {Subfield}, given by $H \mapsto K^H$ is bijective.

- (Injectivity) Let H be a subgroup of $G = \mathrm{Gal}(K/F)$. Our correspondence maps H to K^H. The extension K/K^H is Galois by corollary 1.3.9. Assume that $K^H = K^{H'}$ for some subgroup H' of G. Corollary 1.3.10 then gives that

$$H = \mathrm{Aut}(K/K^H) = \mathrm{Aut}(K/K^{H'}) = H'.$$

  So this correspondence is injective.

- (Surjectivity) Let M be any subfield of K containing F. Our goal now is to find a subgroup $H \subset \mathrm{Gal}(K/F)$ so that $K^H = M$. K/F is Galois, so K is a splitting field over F for some separable polynomial $f(x) \in F[x]$. The polynomial $f(x)$ is also in $M[x]$ since $F \subset E$. Hence K is a splitting field for $f(x)$ over E, and so the extension K/E is Galois. $K^{\mathrm{Gal}(K/E)} = E$ and $\mathrm{Gal}(K/E) \subseteq \mathrm{Gal}(K/F)$, so we have found a subgroup of $\mathrm{Gal}(K/F)$ which fixing field is E.

□

Example 1.4.2. (Galois extensions)

- Let $K = \mathbb{Q}(\sqrt{2})$ and $F = \mathbb{Q}$. We saw in a previous example that $\mathrm{Gal}(K/F) = \{e, \sigma\}$, where $\sigma(\sqrt{2}) = -\sqrt{2}$. Hence, the diagram of subfields of K will be

Figure 6. Diagram of intermediate fields of $\mathbb{Q}(\sqrt{2})/\mathbb{Q}$.

- Let K be the splitting field of $x^5 - 1$ and $F = \mathbb{Q}$. Hence $K = \mathbb{Q}(\zeta_5)$ for some primitive 5th root of unity ζ_5. By previous example, $\mathrm{Gal}(K/F) = (\mathbb{Z}/5\mathbb{Z})^\times$. This is a cyclic group, with the only subgroup $< 4 >= \{1, 4\}$. Let M be the fixed field of $< 4 >$. Then we get the following diagram:

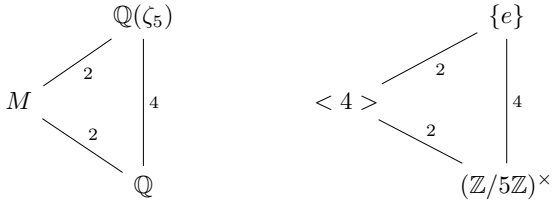


Figure 7. Diagram of intermediate fields and subgroups of the extensions $\mathbb{Q}(\zeta_5)/\mathbb{Q}$.

  In order to describe the field M, consider the element $\alpha = \zeta_5 + \zeta_5^{-1}$. It is fixed by $< 4 >$, so $\alpha \in M$. To show that $M = \mathbb{Q}(\alpha)$, we only need to

check that α is not a rational number. ζ_5 is a root of $x^5 - 1$, and if we remove the factor $(x - 1)$, we gather that ζ_5 is a root of the polynomial $x^4 + x^3 + x^2 + x + 1$. Thus we get the expression $\zeta_5 + \zeta_5^2 + \zeta_5^3 + \zeta_5^4 = -1$. Now we get

$$\begin{aligned}\alpha^2 + \alpha &= \zeta_5^3 + 2 + \zeta_5^{-2} + \zeta_5 + \zeta_5^{-1} \\ &= \zeta_5 + \zeta_5^2 + \zeta_5^3 + \zeta_5^4 + 2 \\ &= (-1) + 2.\end{aligned}$$

Hence, replacing α by x, we get that α is a root of the polynomial x^2+x-1. This is irreducible by the rational root test. Hence $M = \mathbb{Q}(\alpha)$. Here we note that M is a splitting field of $\mathbb{Q}$

Remark. This version of the Galois correspondence only handles the case where the extension is finite. Further generalizations to the infinte case exist, but are not covered here. For a brief introduction, see [1, p.645-652]. However, this constraint is not present in theorem B. This will be further discussed in section 2.2.

As we have seen, all fields have a Galois extension of some kind. The question now is if there is some limit of what groups can appear as a Galois group to some extension for a fixed field. In chapter 3 we will investigate, given a field F, if every finite group appears as a Galois group for some Galois extension of F. This is usually referred to as the inverse Galois problem. The case we will study, and show that it holds true, is when $F = \mathbb{C}(t)$. It is however not known if this is true when $F = \mathbb{Q}$, even though it is true for all finite solvable groups. Theorem A can be applied to solve several problems. It can be used to show that there is no general solution by radicals to polynomials of degree 5 and higher. It has also a significant use in proofs considering what geometrical objects can be constructed by straightedge and compass. For further details on these subjects, see [1, Section 14.7] and [1, Section 13.3] respectively.

Chapter 2

Covering spaces

The goal of this chapter is to investigate the similarities and differences of theorem A and theorem B from the introduction. Theorem A is stated in the context of algebra and deals with fields, while theorem B is stated in the context of topology and deals with what is called covering spaces. We must first find a way of associating groups to these covering spaces. The idea of connecting groups with topological spaces is not unfamiliar. The fundamental group is a prime example of when group theory goes a long way to broaden the insights how certain topological spaces differ and agree. The fundamental group does in fact play a greater role in a generalization of theorem B, but it is beyond the scope of this thesis. For further details, see [4, p.315].

In section 2.1 we will properly introduce covering spaces and discuss their similarities to field extensions. In section 2.3 we will state and prove theorem B. This theorem is only valid for certain covering spaces, called Galois covers. These Galois covers and the connection of covering spaces with group actions will be the topic of section 2.2. In section 2.4 we will present a specific cover of interest. This is not only a fundamental Galois cover, but it also plays a key role in chapter 3.

2.1 Covering spaces

Definition 2.1.1. Let $p : Y \to X$ be a continuous map. An open set $u \subset X$ is said to be evenly covered if $p^{-1}(u) = \bigcup_{i \in I} v_i$ such that

i. v_i are open subsets of Y

ii. $v_i \cap v_j = \emptyset$ for all $i \neq j$

iii. Each restriction $p|_{v_i} : v_i \to u$ is a homeomorphism.

Definition 2.1.2. A continuous, surjective map $p : Y \to X$ is said to be a covering map if each element $x \in X$ has an evenly covered neighbourhood. Y is said to be a covering space of X, and X is said to be the base of the cover.

Remark. A covering map of two covering spaces will sometimes be referred to as a cover.

Proposition 2.1.3. All covering maps are open and quotient maps.

Remark. Remember, a map $q : Y \to X$ is a quotient map if

- q is surjective.
- $U \subset X$ is open if and only if $q^{-1}(U) \subset Y$.

Example 2.1.4. (Covering maps)

- Homeomorphisms $\varphi : Y \to X$ are covering maps. Just choose any point x and corresponding neighbourhood U. $\varphi^{-1}(U)$ is a disjoint union of one open set, and it is trivially homeomorphic to U.
- The map $\epsilon : \mathbb{R} \to \mathbb{S}^1$, $r \mapsto \mathrm{e}^{2\pi i \cdot r}$ is a covering map. Given any $x_0 \in \mathbb{S}^1$, we may find an evenly covered neighbourhood u of x_0, as seen in the figure. This is only a visualisation, for further details see [4, p.218].

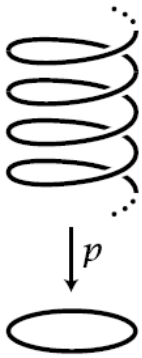


Figure 8. The real line projected down on the circle by a covering map

- A fundamental example of covers is the projection $p : X \times I \to X$, $(x, i) \mapsto x$ where X is any topological space and I a discrete space. For any open set $U \subset X$, it follows that $p^{-1}(U) = \coprod_{i \in I} U \times \{i\}$ which are all trivially homeomorphic to U and so the axioms of a cover are fulfiled. We call this the trivial cover. It even turns out that every covering space is locally equivalent to a trivial cover (see proposition 2.1.9).

In order to address the claim that being a covering space is equivalent to the trivial cover, we first need a method to compare different coverings. In algebra, we already have an intuitive understanding of isomorphisms and automorphisms of fields as a tool to compare fields. The same is true in topology for topological spaces (when homeomorphisms are seen as isomorphisms). On the other hand, what tool should be used for covering spaces is not so obvious. In order to find a suitable structure, we first introduce the concept of lifts.

Definition 2.1.5. Let $p : Y \to X$ be a covering map and $\varphi : Z \to X$ a continuous map. A lift $\tilde{\varphi}$ of f is a continuous map $\tilde{\varphi} : Z \to X$ so that $\varphi = p \circ \tilde{\varphi}$, i.e the diagram commutes.

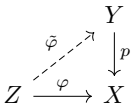


Figure 9. A lift of the function φ.

Example 2.1.6. Let $\varphi : I \to \mathbb{S}^1$ be the loop $\varphi(x) = e^{2\pi i \cdot x}$ at 1 going one lap around the circle. Define the paths $\tilde{\varphi}_1, \tilde{\varphi}_2 : I \to \mathbb{R}$ as $\tilde{\varphi}_1(x) = x$, $\tilde{\varphi}_2(x) = x + n$ ($n \in \mathbb{N}$). It follows that

$$p \circ \tilde{\varphi}_1(x) = p(x) = \mathrm{e}^{2\pi i x} = \varphi(x)$$
$$p \circ \tilde{\varphi}_2(x) = p(x + n) = \mathrm{e}^{2\pi i (x+n)} = \mathrm{e}^{2\pi i x} = \varphi(x).$$

So these are clearly lifts of φ.

Proposition 2.1.7 (Unique lifting property)**.** Let $q : Y \to X$ be a covering map and let Z be connected. Assume that $\varphi : Z \to X$ is a continuous map and that $\tilde{\varphi}_1, \tilde{\varphi}_2 : Z \to Y$ are lifts of φ that agrees at some point of Y. Then $\tilde{\varphi}_1 = \tilde{\varphi}_2$.

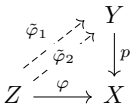


Figure 10. Two lifts of the same function.

Proof. See [4, p.220]. □

We can use the concepts of lifts as a comparative tool of covering spaces if we also let $\varphi : Z \to X$ be a covering space. A lift can then be viewed as a map between covers sharing the same base such that their structure as covering maps is preserved under composition.

Definition 2.1.8. Let $p : Y \to X$ and $q : Z \to X$ be two covers. A morphism between the covers is a lift $\varphi : Y \to Z$.

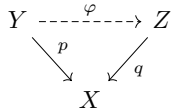


Figure 11. A morphism of covers.

An isomorphism of covers is a morphism of covers where φ is a homeomorphism. An automorphism of covers is an isomorphism of covers where $Z = Y$.

With these new concepts in mind, we are now able to properly make the claim stated in example 2.1.4.

Proposition 2.1.9. Let X, Y be topological spaces and $p : Y \to X$ a continuous surjective map. Y is a cover of X if and only if each point of X has a neighbourhood V such that the restriction $p|_{p^{-1}(V)} : p^{-1}(V) \to V$ is isomorphic to a trivial cover. That is, there exist a homemorphism $f : p^{-1}(V) \to V \times I$ (I is a discrete set) so that:

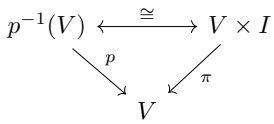


Figure 12. A local isomorphy of covers.

Proof. See [6, p.38]. □

Definition 2.1.10. Given a cover $p : Y \to X$, we define $\mathrm{Aut}(Y/X)$ as the set of automorphisms of this cover. This set is a group under composition.

Notice that we may apply the unique lifting property with the functions in $\mathrm{Aut}(Y/X)$.

Corollary 2.1.11. If we let $\varphi_1 = \phi$ for some $\phi \in \mathrm{Aut}(Y/X)$, $\varphi_2 = id_Y$, $q = \varphi$ and $Z = Y$, then the proposition implies that any automorphism having a fixing point is the identity.

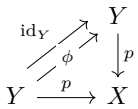


Figure 13. Two lifts with a shared fixed point.

Now we can start to notice the similarity between the theory of field extensions K/F and covering spaces $p : Y \to X$. In both cases the base field F and the base space X are our fixed reference points. From these we try to find other fields K and spaces Y so that they are compatible to their respective bases by some function. For fields, this function is an injective homomorphism $\varphi : F \to K$. For topological spaces this function is a covering map $p : Y \to X$. In algebra, the idea of intermediate fields is a simple one. Given an extension K/F, the field M is said to be an intermediate field if $F \subset M \subset K$. Formally, this means that injective homomorphisms exist so that the following diagram commutes.

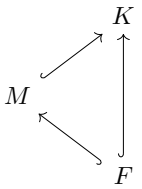


Figure 14. Commutative diagram of field extensions.

Here, each arrow represents a field extension. So it would be appropriate that this was the case for covering spaces as well. As it turns out, this is the case.

Proposition 2.1.12. Let Z be a connected space, $p : Y \to Z$ be a continuous map and $q : Z \to X$ a cover. If the composition $q \circ p : Y \to X$ is a covering map, then p is also a covering map.

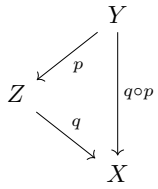


Figure 15. Commutative diagram of covering spaces.

Proof. See [6, p.42]. □

Definition 2.1.13. A space Z with the above mentioned properties is called an intermediate cover of the covering $p : Y \to X$.

Thus, this means that it is suitable to see intermediate covers as the topologic analogue of intermediate fields.

2.2 Group actions and Galois covers

In this section, we will first define Galois covers. Later, we will present a tool to specifically create these Galois covers. This tool is the analogue of fixing fields in algebra. That is, a way to map the automorphism group to a covering space. The use of groups in topology is common and the main way groups interact with topological spaces is through group actions. The orbits of these group actions can in turn be used to create quotient spaces. When the group action has certain properties (see 2.2.2), then it is the tool we are looking for.

Definition 2.2.1. Let $p : Y \to X$ be a cover and $G = \mathrm{Aut}(Y/X)$ the automorphism group. Consider the quotient map of the orbit space $p_G : Y \to Y/G$. Then there is a continuous map $r : Y/G \to X$ so that the following diagram commutes.

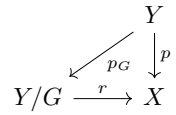


Figure 16. Commutative diagram of a quotient space.

The cover is said to be Galois if r is a homeomorphism, and then $\mathrm{Gal}(Y/X) := \mathrm{Aut}(Y/X)$.

There are several interesting aspects to note here that either will be elaborated on later, or are apparant immediately.

- The map $p_G : Y \to Y/G$ is a cover (corollary 2.2.5).
- The map $r : Y/G \to X$ is a cover (theorem 2.3.1).
- The covering map p is Galois when $X = Y/G$ with $\mathrm{Gal}(Y/X) \cong G$.

Hence, this definition bears a close resemblance to the algebraic characterisation of a Galois extension by fixing fields. In both cases, the automorphism group creates an intermediate field/space such that this extension/cover is Galois. It also has the similar property of fixing fields that $\mathrm{Aut}(K/K^G)) \cong G$. Now, we prove our claims about these orbit spaces.

Definition 2.2.2. Let G be a group acting continuously on a topological space Y. G is said to act evenly on Y if each point $y \in Y$ has a neighbourhood U so that $U \cap g \cdot U = \emptyset$ for all $g \in G,\ g \neq 1$.

Proposition 2.2.3. Let G be a group acting evenly on a connected space Y. Then the projection $q : Y \to Y/G$ is a covering map.

Proof. Remember that $q : Y \to Y/G$ is the map taking $y \in Y$ to the orbit of y, so $q(y_1) = q(y_2)$ if and only if $y_1 = g \cdot y_2$ for some $g \in G$.
First we want to show that each element in Y/G has a neighbourhood which preimage is a disjoint union of open sets. So let $x \in Y/G$ and say that $x = [y]$ for some representative $y \in Y$. G is acting evenly on Y so there is an open neighbourhood $U \subset Y$ of y so that $U \cap g \cdot U = \emptyset$ for all $g \in G,\ g \neq 1$. Let $V = q(U)$. Then $q^{-1}(V) = \bigcup_{g \in G} g \cdot U$. These are disjoint by the previous remark. The map $g : Y \to Y$ is a homeomorphism and U is an open set, so $g \cdot U$ is open for all $g \in G$. What remains to show is that the restriction $q|_U : U \to V$ is a homeomorphism. The map q is continuous and open, so this restriction must be too.

- Injectivity: Assume that $q(g \cdot y_1) = q(g \cdot y_2)$ for some $y_1, y_2 \in U$. This is equivalent to $q(y_1) = q(y_2)$, which in turn is equivalent with $y_1 = h \cdot y$ for some $h \in G$. But $y_1, y_2 \in U$ implies that $h = 1$. So $g \cdot y_1 = g \cdot y_2$.
- Surjectivity: V is defined as the image of U, so it is trivially surjective.

□

Proposition 2.2.4. Let $p : Y \to X$ be a covering space where Y is connected. Then the action of $\mathrm{Aut}(Y/X)$ on Y is even.

Proof. Let $y \in Y$ and $x = p(y)$. p is a covering map, so there exists a neighbourhood V of x so that $p^{-1}(V)$ is a disjoint union of open sets in Y. One of these sets, say U contain y. Take any non-trivial $\phi \in \mathrm{Aut}(Y/X)$. This ϕ maps U isomorphically onto some of the other disjoint open sets, say U'. Any automorphism having a fixed point is the identity by corollary 2.1.12, so $U \neq U'$. So we can conclude that $\phi(U) \cap U = \emptyset, \forall \phi \in \mathrm{Aut}(Y/X)$, where $\phi \neq id$. □

Corollary 2.2.5. Let $p : Y \to X$ be a covering space. Then the quotient $\pi : Y \to Y/\mathrm{Aut}(Y/X)$ is a covering map.

Proof. This follows immediately from propositions 2.2.3 and 2.2.4. □

Proposition 2.2.6. Let G be a group that acts evenly on a connected space Y and $p_G : Y \to Y/G$ the covering map defined by this action. Then $\mathrm{Aut}(Y/(Y/G)) = G$.

Proof. It is trivial that $G \subset \mathrm{Aut}(Y/(Y/G))$, since $p_G(y) = [y] = [g \cdot y] = p_G(g \cdot y)$ for all $g \in G$, and so g fits into the commutative diagram. Let $\phi \in \mathrm{Aut}(Y/(Y/G))$ and let $y \in Y$. Then $\phi(y)$ must be mapped (by p_G) to the orbit of y. So $\phi(y) = g \cdot y$ for some $g \in G$. Alas, ϕ and g has a fix point and fit into the commutative diagram

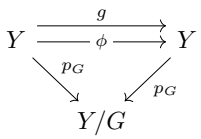


Figure 17. Two automorphisms with a fixed point.

so $\phi = g$ by proposition 2.1.5. Hence $G = \mathrm{Aut}(Y/(Y/G))$. □

Proposition 2.2.7. A connected cover is Galois if and only if $\mathrm{Aut}(Y/X)$ acts transitively on each fibre of p.

Proof.

- Assume that $p : Y \to X$ is a Galois cover with $G = \mathrm{Aut}(Y|X)$.

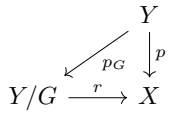


Figure 18. Commutative diagram of a quotient space.

  Let $x \in X$, and $y \in p^{-1}(x)$. We want to show that G acts transitively on $p^{-1}(x)$, which is equivalent to show that p_G maps $p^{-1}(x)$ to exactly one element in Y/G, that is one orbit.

  Let $\tilde{y} = r^{-1}(x)$. $p_G(y) = \tilde{y}$, so $[y] = \tilde{y}$. r is a bijection, so by commutativity p_G maps $p^{-1}(x)$ to $\tilde{y}$, and so G acts transitively.

- Assume that $G = \mathrm{Aut}(Y/X)$ acts transitively on each fibre of the cover p. We want to show that the induced map r is a homeomorphism. Surjectivity and continuity are already clear from the property of quotient maps. Let $x \in X$ and $[y] = p^{-1}(x)$. It is clear that there is a 1-1 correspondence between the elements of X and the elements of $G\backslash Y$, since each $x \in X$ maps to the fibre of x, which is equal to the orbit of the fibre. Lastly, we want to show that r is an open map. Let $U \subset Y/G$ be an open set. By definition of a quotient space $p_G^{-1}(U) \subset Y$ is open. Since p is open by proposition 2.1.3, we have that $p(p_G^{-1}(U)) \subset X$ is open. This together with

$$\begin{aligned} p &= r \circ p_G \\ p(p_G^{-1}(U)) &= r \circ p_G(p_G^{-1}(U)) = r(U) \end{aligned}$$

shows that $r(U)$ is open. Hence r is an open map.

□

We may note the similarity between this proposition and proposition 1.3.12. Even though there is no apparent correspondence of polynomials in topology, the roots and fibres in their respective theory do share some similarities. For one, the roots are algebraically indistinguishable (see note after proposition 1.2.5), just as all fibres have neighboroods that are pairwise homeomorphic. So in a sense, these fibres are locally the same. This analogy is not always available. Galois field extensions can be created from splitting fields of separable polynomials, but they do not necessarily need to be irreducible. So the Galois group does not act transitively on all added roots here, and so proposition 2.2.7 cannot be translated into an equivalence statement in algebra.

So, we have made a connection with two of the Galois characterisations from algebra, but not with the original one (definition 1.3.4). There is a connection here as well, but only in special cases. First, given a covering map $p : Y \to X$, the fibres $p^{-1}(x)$ have the same cardinality for all x (see [4, p.281]). This also means that the discrete set I in proposition 2.1.9 has the same cardinality for all neighbourhoods. The cardinality is called the number of sheets of the covering. The concepts of Galois in algebra and Galois in topology coincide in the finite case. We state it as a proposition.

Proposition 2.2.8. Let $p : Y \to X$ be a covering. If the number of sheets of the covering is finite, then $|p^{-1}(x)| = |\mathrm{Aut}(Y/X)|$ if and only if the cover p is Galois.

Proof.

- Assume that the cover is Galois. Let $x \in X$. The group $\mathrm{Gal}(Y/X)$ acts transitively on the fiber $p^{-1}(x)$ by proposition 2.2.7. If we fix $y \in p^{-1}(x)$ then this implies that for all $a \in p^{-1}(x)$, there exists some $g \in \mathrm{Gal}(Y/X)$ so that $y = g \cdot a$. So $|p^{-1}(x)| \leq |\mathrm{Gal}(Y/X)|$.
- For a condratiction, assume that $|\mathrm{Gal}(Y/X)| > |p^{-1}(x)|$. Then for some $y \in p^{-1}(x)$ there are $g, h \in \mathrm{Gal}(Y/X)$, $g \neq h$, so that $g \cdot y = h \cdot y$. Thus, equivalently $h^{-1}g \cdot y = y$. But then the maps $h^{-1}g$ and 1 share a common fix point. So by corollary 2.1.11 $h^{-1}g = 1$, which contradicts that $g \neq h$.

□

2.3 The Galois correspondence in topology

In this section we will properly state the Galois correspondence in topology, also referred to as theorem B. The theorem is purposely stated in a similar fashion as theorem A in order to clearly see that they are similar.

Theorem 2.3.1. Let $p : Y \to X$ be a Galois cover and $G = \mathrm{Gal}(Y/X)$. Then there is a 1-1 correspondence between intermediate connected covers Z and subgroups $G \supset H \supset \{e\}$

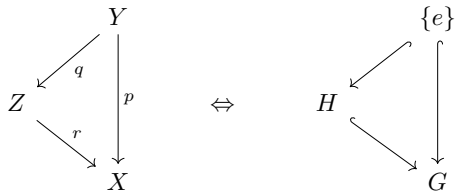
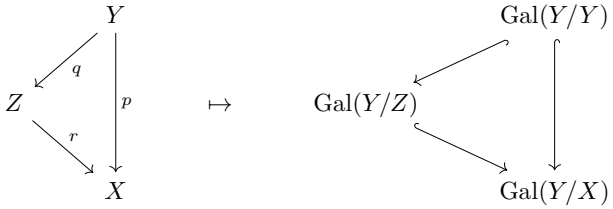


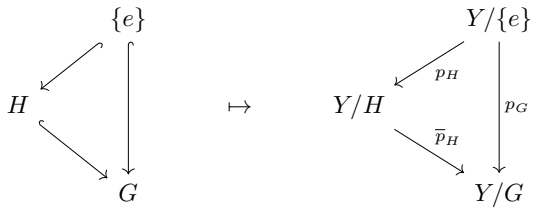
Figure 19. Commutative diagrams of corresponding covering spaces and groups.

so that $q : Y \to Z$ is Galois. The correspondence is given by

- Z corresponds to $\mathrm{Gal}(Y/Z)$:



- H corresponds to $p_H : Y \to Y/H$:



Further, this correspondence has the properties

a) Let Z_1, Z_2 be intermediate covers and let H_1, H_2 be their corresponding subgroups of G. Then there is a covering map $f : Z_1 \to Z_2$ if and only if $H_1 \supseteq H_2$.

b) The map $r : Z \to$ is Galois if and only if H is normal in G.

Proof. First we need to show that this correspondence is well defined.

- ($H \subset G$ maps to an intermediate field) Assume that H is a subgroup of G. Then the cover $p_H : Y \to Y/H$ is trivially Galois. So we only need to show that the map $\overline{p_G} : Y/H \to X$ is a covering map. Since $p : Y \to X$ is a covering, there exist neighborhoods $V \subset X$ such that $p^{-1}(V) \cong U \times I$ by proposition 2.1.9. Here I is a discrete subset representing the elements in the fibre of p, and $U \subset Y \cong V$. We have that $p_H(p^{-1}(V)) = \overline{p_H}^{-1}(V)$. H only acts on I in $U \times I$, so $p_H(U \times I) = U \times (I/H)$. Hence locally we have that $\overline{p_H}^{-1}(V) \cong U \times (I/H)$, so $\overline{p_H}$ is a covering map by proposition 2.1.9.

- (Intermediate covers maps to subgroup $H \subset G$) Assume that $r : Z \to X$ is a cover that fits into the commutative diagram below.

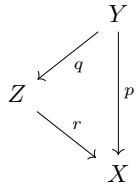


Figure 20. Commutative diagram of covering spaces.

Then $q : Y \to Z$ is a cover by proposition 2.1.12. Now we want to show that this is a Galois cover. That is to show that $Y/(\mathrm{Aut}(Y/Z)) \cong Z$. Furthermore we want to show that $\mathrm{Aut}(Y/Z) \subset \mathrm{Gal}(Y/X)$ in order for the correspondence to be well defined. We can clearly see that $\mathrm{Aut}(Y/Z) \subset \mathrm{Gal}(Y/X)$, since automorphisms commuting with Y over Z also commute with Y over X. The cover $q : Y \to Z$ is Galois if and only if $\mathrm{Aut}(Y/Z)$ acts transitively on the fibres of q. So take $z \in Z$ and let $y_1, y_2 \in q^{-1}(z)$. Then in particular $y_1, y_2 \in p^{-1}(r(z))$. p is a Galois cover, so $\phi(y_1) = y_2$ for some $\phi \in \mathrm{Gal}(Y/X)$. Now, $\phi \in \mathrm{Aut}(Y/Z)$ only when the diagram commutes.

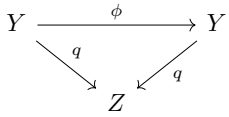


Figure 21. Automorphism of a covering space.

Equivalently, the diagram commutes only when the maps q and $q \circ \phi$ are equivalent. These maps may be seen as lifts in the following diagram:

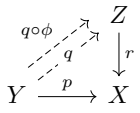


Figure 22. Two lifts of the map p.

We have a fixing point by $q(\phi(y_1)) = q(y_2) = q(y_1)$, so these maps are equal by proposition 2.1.7. Hence, $\phi \in \mathrm{Aut}(Y/Z)$ and this group acts transitively on the fibres of q.

The last thing to show is that this correspondence is bijective. The last point showed that the correspondence is surjective, so we only need to show that is is injective. But this is trivially so, since if $Y/H = Y/H'$, then $h \cdot y = h' \cdot y$ for $h \in H$, $h' \in H'$ and $y \in Y$. But then $h'^{-1}h \cdot y = y$, so $h' = h'^{-1}$ by 2.1.11. Hence $H = H'$.

□

2.4 Universal cover

Calculating the automorphism group of a cover is not always that easy. If we find a connection to other known groups, it would simplify the task. The universal cover is one such asset. For every connected and locally simply connected space X, there exists a Galois cover $p : Y \to X$ so that $\mathrm{Aut}(Y/X) \cong \pi_1(X, x_0)$. We begin with a proposition.

Proposition 2.4.1. Let $p : Y \to X$ be a cover and assume that Y is simply connected. If $q : Z \to X$ is another cover, then there exists a covering map $r : Y \to Z$.

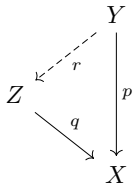


Figure 23. Commutative diagram of covering spaces.

Proof. See [4, p.297-298]. □

Corollary 2.4.2. Let Y, Y' be two simply connected spaces. If both Y and Y' are covers of the same space X, then Y and Y' are homeomorphic.

Remark. Remember that a space is simply connected if it is path connected and its fundamental group is trivial. In particular, a simply connected space is connected.

Definition 2.4.3. If $p : Y \to X$ is any cover and Y is simply connected, then Y is called a universal covering.

By these propositions, it makes sense to regard the universal cover as a maximal cover. This resembles what the algebraic closure is for the algebraic case. But note that the algebraic closure of $\mathbb{Q}$ is an infinite extension over $\mathbb{Q}$, and so it does not fit into our finite version of Galois theory. On the other hand, the universal cover does fit into the topological version.

Theorem 2.4.4. Assume that X is a connected and locally simply connected space. Then

- there exists a universal cover Y of X;
- $\mathrm{Aut}(Y/X) \cong \pi_1(X, x_0)$
- X is homeomorphic to the orbit space $Y/\pi_1(X, x_0)$.

Proof. See [4, p.298] and [3, p.71-72] □

Theorem 2.4.5. Let $p : Y \to X$ be a covering map. If Y is simply connected, then $\mathrm{Aut}(Y/X) \cong \pi_1(X, x_0)$.

Proof. See [4, p.310-311]. □

Putting these theorems together, we see that if Y is the universal cover of X, then it is a Galois cover.

To conclude, given a space and its fundamental group, we know that there exists a Galois cover, with the automorphism group isomorphic to the fundamental group. This will be of great use in section 3.5, where we will show the inverse Galois for $\mathbb{C}(t)$.

Chapter 3

Inverse Galois for $\mathbb{C}(t)$

All fields, which are not algebraically closed, have a non trivial Galois extension. They can be created as splitting fields for some separable polynomial. Thus we can associate a Galois group to every field. The same is true when considering covering spaces, where existence of a Galois covering is secured by the universal cover.
Starting the other way around and fixing a field F, Galois extensions K/F exist so that every finite group appears as a Galois group $\mathrm{Gal}(K/F)$? This problem is commonly referred to 'the inverse Galois problem'. In the case where $F = \mathbb{Q}$ it is still an unsolved problem, but offers a partial solution for all finite abelian groups. In this chapter we prove that this is true for $F = \mathbb{C}(t)$. What is interesting is even though that this claim is purely algebraic, the proof uses topological techniqes and the Galois correspondence in topology. This chapter contains the necessary concepts and results to show that every finite group appears as a Galois group for an extension of $\mathbb{C}(t)$.
In section 3.1 we introduce Riemann surfaces. They are a way of locally attaching the structure of $\mathbb{C}$ on two-dimensional manifolds. Section 3.2 and 3.3 will present maps of Riemann surfaces which preserve their complex structure. These maps are the analogue of holomorphic and meromorphic maps in complex analysis. For both maps there are important 1-1 correspondences crucial for our proof of the inverse Galois. Holomorphic and proper maps of connected Riemann surfaces correspond to finite covering spaces. Meromorphic maps of connected and compact Riemann surfaces coorespond to field extensions. In section 3.4 we introduce free groups. These groups have an important property, namely that every finite group appears as a quotient of a free group. This is the key we use to show in section 3.5 that every finite group appears as a Galois group for any field extension of $\mathbb{C}(t)$.

3.1 Riemann surfaces

Definition 3.1.1. Let X be a two-dimensional manifold, i.e X is Hausdorff, second countable and locally isomorhpic to $\mathbb{R}^2$.

- A complex chart on X is a homeomorhpism $\varphi : U \to V$ of open subsets $U \subset X$ and $V \subset \mathbb{C}$.
- Two complex charts $\varphi : U \to V$, $\psi : U' \to V'$ are said to be holomorphically compatible if the map

  $$\psi \circ \varphi^{-1} : \varphi(U \cap U') \to \psi(U \cap U')$$

  is biholomorphic, i.e $\psi \circ \varphi^{-1}$ is bijective, holomorphic, and its inverse is also holomorphic.
- A complex atlas on X is a system of charts $\mathfrak{U} = \{\varphi_i : U_i \to V_i | i \in I\}$ which are holomorphically compatible and cover X, i.e $\bigcup_{i\in I} U_i = X$.
- Two atlases $\mathfrak{U}, \mathfrak{U}'$ are said to be analytically equivalent if every chart of $\mathfrak{U}$ is holomorphically compatible with every chart of $\mathfrak{U}'$.

Note that analytical equivalence of atlases is an equivalence relation on the set of atlases, since the composite of biholomorphic functions are biholomorphic. This motivates the following definition.

Definition 3.1.2. A complex structure on a two-dimensional manifold X is an equivalence class of analytically equivalent atlases on X.

Definition 3.1.3. A Riemann surface is a two-dimensional manifold together with a complex structure Σ on X.

Example 3.1.4. (Riemann surfaces)

- The space $\mathbb{C}$ is trivially a Riemann surface. Just consider the atlas with only one complex chart $\mathrm{id}_{\mathbb{C}} : \mathbb{C} \to \mathbb{C}$, $z \mapsto z$. So the complex structure on $\mathbb{C}$ would be the equivalence class of atlases analytically equivalent to $\{\mathrm{id}_{\mathbb{C}}\}$.
- The Riemann sphere P^1 is a Riemann surface. The sphere is defined as the space $P^1 = \mathbb{C} \cup \{\infty\}$ with the one-point compactification topology. The only open sets of P^1 are
  - V, where $V \subset \mathbb{C}$ is open.
  - $V \cup \{\infty\}$, where $V \subset \mathbb{C}$ is open and the complement of V is compact.

  This topology makes P^1 into a compact, Hausdorff space, which is isomorhpic to the sphere S^2.

  The atlas $\mathfrak{U}$ we define on P^1 consists of two charts. Let $U_1 = \mathbb{C}$ and $U_2 = P^1 \backslash \{0\} = \mathbb{C}^\star \cup \{\infty\}$.

– $\varphi_1 : U_1 \to \mathbb{C}, \quad z \mapsto z$

– $\varphi_2 : U_2 \to \mathbb{C}, \quad z \mapsto \begin{cases} 1/z & \text{if } z \in \mathbb{C}^\star \\ 0 & \text{if } z = \infty \end{cases}$

These are clearly homemorphisms. If φ_1 and φ_2 are going to constitute a complex atlas of P^1, then these maps must be holomorphically compatible. $U_1 \cap U_2 = \mathbb{C}^\star$, so $\varphi_1(U_1 \cap U_2) = \varphi_2(U_1 \cap U_2) = \mathbb{C}^\star$. We have that $\varphi_1 \circ \varphi_2(z) = \varphi_2 \circ \varphi_1(z) = 1/z$ and that they have domain and target $\mathbb{C}^\star$. Hence they are biholomorphic. The equivalence class of atlases analytically equivalent to $\mathfrak{U} = \{\varphi_1, \varphi_2\}$ is the complex structure on P^1 making it into a Riemann surface.

3.2 Holomorphic maps

With Riemann surfaces defined, we would like to define maps on them taking use of their complex structure. The idea is first to define maps from Riemann surfaces to the complex plane, but locally observe these maps as maps purely complex functions going through the complex charts. When the maps are considered like these, then we can impose properties on these maps from complex analysis such as being holomorphic. In the same manner we can define maps from Riemann surfaces to Riemann surfaces, and impose that they are holomorphic when locally viewved as complex maps.

Definition 3.2.1. Let X be a Riemann surface and $Y \subset X$ an open subset. A map $f : Y \to \mathbb{C}$ is said to be holomorphic if, for every complex chart $\psi : U \to V$ on X, the mapping

$$f \circ \psi^{-1} : \psi(U \cap Y) \to \mathbb{C}$$

is holomorphic as a complex map.

Definition 3.2.2. Let X, Y be Riemann surfaces. A continuous map $f : X \to Y$ is said to be holomorphic, if for every pair of charts $\psi_1 : U_1 \to V_1$, $\psi_2 : U_2 \to V_2$ on X and Y respectively with $f(U_1) \subset U_2$, the mapping

$$\psi_2 \circ f \circ \psi_1^{-1} : V_1 \to V_2$$

is holomorphic as a complex map.

Theorem 3.2.3. Let X, Y be Riemann surfaces and $f : X \to Y$ a non-constant holomorphic map. Let $a \in X$ and set $b = f(a)$.

Then there exists an integer $k \geq 1$ and charts $\varphi : U \to V$ on X and $\psi : U' \to V'$ such that

- $a \in U$, $\varphi(a) = 0$; $b \in U', \psi(b) = 0$.
- $f(U) \subset U'$
- The map $F := \psi \circ f \circ \varphi^{-1} : V \to V'$ is given by

$$F(z) = z^k \text{ for all } z \in V.$$

Proof. See [2, p.10]. □

Definition 3.2.4. The integer k in the theorem is called the ramification index of f at a. The points a where $k > 1$ are called branch points and we let S_f denote the set of branch points.

Corollary 3.2.5. Any holomorphic map between Riemann surfaces are open.

Proof. Let $g = z^k$. Then this follows immediately from that $f = \psi^{-1} \circ g \circ \varphi$, i.e f is written as a composition of open maps. □

Corollary 3.2.6. The fibres of f and the set S_f are discrete closed subsets of X.

Proof. See [6, p.76]. □

Definition 3.2.7. A map $f : Y \to X$ is called proper if the preimage of all compact subsets of X are compact in Y.

Remark. The map f is closed when Y is locally compact and Hausdorff.

Proposition 3.2.8. Let X be a connected Riemann surface and $f : Y \to X$ a proper holomorphic map. Then the map f is surjective with finite fibres, and its restriction $f : Y \backslash f^{-1}(f(S_f)) \to X \backslash f(S_f)$ is a covering map.

Idea of proof: Why is it that we must remove the pre-image of the branch points to get a cover? The reason is that neighbourhoods around these points are not evenly covered. The map f is locally equivalent to z^n, so no neighbourhood $U \subset Y$ of 0 is 1-1 to $f(U) \subset X$, and so they are not homeomorphic. By removing the branch points, then the fibres of f are finite by corollary. To show that f is surjective, coinsder that it is both open by corollary 3.2.5 and closed by the note of 3.2.7. So $f(Y) \subset X$ is both open and closed. The space X is connected, so then $f(Y) = X$.
Lastly, for each preimage of $x \in X \backslash f(S_f))$, we can find a neighbourhood and complex maps as in theorem 3.2.3 such that f locally is equivalent to the identity map. Hence a homeomorphism. By taking the intersection of these we gather the desired evenly covered neighbourhood. For details of this proof, see [6, p.77].

Definition 3.2.9. Let $f : Y \to$ be a proper holomorphic map of Riemann surfaces as above. Then it is called a finite branched cover.

This correspondence of holomorphic proper maps and finite covers is in fact even stronger, as stated by the following theorem.

Theorem 3.2.10. Let X be a connected Riemann surface and $S \subset X$ a discrete closed subset. Then there is a 1-1 correspondence of

- Finite topological covers $p : Y' \to X \backslash S$.

- Riemann surfaces Y with proper maps $f : Y \to X$ such that $f(x) \in S$ for all branch points $x \in Y$.

In the correspondence we have that $Y' \subset Y$ and p is a restriction of the map f. Furthermore, let Y and Z be Riemann surfaces equipped with proper maps q, r mapping to X. Assume that Y and Z correspond to the finite covers Y', Z' of X' such that there exist a covering morphism $\varphi' : Y' \to Z'$. Then φ' extends to a unique holomorphic map from Y to Z.

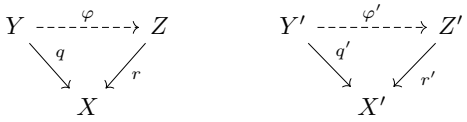


Figure 24. Corresponding morphism of holomorphic maps and covering spaces.

Remark. In the field category theory, this correspondence is called an equivalence of categories. However, further details of this area lies beyond the scope of this thesis. For details of the definition and proof, see [6, p.77-79] and [6, chapter 1.4] respectively.

Corollary 3.2.11. $\mathrm{Aut}(Y/X) \cong \mathrm{Aut}(Y'/X')$

Since these two objects can be considered as equivalent, then it is suitable to make the following definition.

Definition 3.2.12. Let $f : Y \to X$ be a proper holomorphic map which correspond to a finite cover $f' : Y' \to X'$. If the cover Y' over X' is Galois, then we say that Y is a finite Galois branched cover of X.

3.3 Meromorphic functions

Meromorphic functions on Riemann surfaces have the same properties as regular meromorphic functions on the complex plane. For our purposes, one important aspect is that the set of meromorphic funtions on a connected Riemann surface is a field. Further, holomorphic maps between connected Riemann surfaces extend these fields. There is in fact a 1-1 correspondence between Galois covers of connected and compact Riemann surfaces and Galois field extensions of the field of meromorphic functions.

Definition 3.3.1. Let D be an open and connected subset of the complex plane. A function $f : D \to \mathbb{C}$ is meromorphic if for all points $x \in D$ it holds that

- f is analytic at x
- or f has a pole at x.

Definition 3.3.2. Let X be a Riemann surface. A function $f : X \to \mathbb{C}$ is meromorphic if

1) There exist a closed discrete subset $S \subset X$ such that the restriction $f : X \backslash S \to \mathbb{C}$ is holomorphic

2) The map $f \circ \phi^{-1} : \phi(U) \to \mathbb{C}$ is meromorphic, for all complex charts $\phi : U \to \mathbb{C}$.

If X is a Riemann surface, then we let $\mathcal{M}(X)$ be the set of all meromorphic functions on X. It is easily seen that $\mathcal{M}(X)$ is a ring under addition and multiplication. What is more useful is the following proposition.

Proposition 3.3.3. Let X be a Riemann surface. If X is connected, then $\mathcal{M}(X)$ is a field.

Proof. See [6, p.80]. □

Proposition 3.3.4. Let P^1 be the Riemann sphere. The set of meromorphic functions on P^1 are only the rational functions, i.e $\mathcal{M}(P^1) = \mathbb{C}(t)$.

Proof. See [2, p.11-12] □

Proposition 3.3.5. Let X, Y be Riemann surfaces and $\phi : Y \to X$ a non-constant holomorphic map. Then ϕ induces a ring homomorphism $\phi^\star : \mathcal{M}(X) \to \mathcal{M}(Y)$ by $f \mapsto f \circ \phi$. In particular, $\phi^\star$ is an injective field homomorphism when X and Y are connected. Hence $\mathcal{M}(Y)/\phi^\star\mathcal{M}(X)$ is a field extension.

There is a correspondence, similar to the one in theorem 3.2.10, between field extensions of $\mathcal{M}(X)$ and holomorphic maps mapping to X.

Proposition 3.3.6. Let X be a connected and compact Riemann surface. Then there exist a 1-1 correspondence of

- Connected and compact Riemann surfaces Y being a finite Galois cover cover over X by the proper holomorphic map $\phi : Y \to X$.
- Galois field extensions $\mathcal{M}(Y)/\phi^\star\mathcal{M}(X)$.

Further, let Y and Z be connected and compact Riemann surfaces equipped with holomorphic maps mapping to X, such that both of them are finite Galois branched covers. Assume that Y, Z correspond to the fields $\mathcal{M}(Y), \mathcal{M}(Z)$ and that there exist an injective homomorphism $\varphi^\star : \mathcal{M}(Z) \to \mathcal{M}(Y)$. Then there exist a continuous function $\varphi : Y \to Z$.

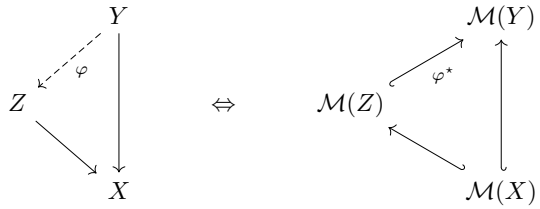


Figure 25. Corresponding morphism of Riemann surfaces and fields.

Corollary 3.3.7. $\mathrm{Aut}(Y/X) \cong \mathrm{Gal}(\mathcal{M}(Y)/\phi^\star\mathcal{M}(X))$.

3.4 Free group

One problem arises when studying groups in an abstract way. We would like to describe them and their structure without drawing out a whole multiplication table. On the other hand we do not want their descriptions to be too general, beacause then they could lack the detail necessary for our purposes. The way we approach this is by defining groups on which there are no relations except the ones given by the group axioms. These are called free groups. We begin by formally defining how these groups are created.

Definition 3.4.1. Let S and S^{-1} be sets such that there exist a bijection between them, and let $\{1\}$ be the singleton set. If $s \in S$ corresponds to $t \in S^{-1}$ by the bijection, then we say that $s^{-1} = t$. Similarly, if $t \in S^{-1}$ corresponds to $s \in S$, we say that $t^{-1} = s$. Then $(s^{-1})^{-1} = s$ for all $s \in S \cup S^{-1}$, and we define $1^{-1} := 1$. A word on S is a sequence of elements $(s_1, s_2, s_3, ...)$ in $S \cup S^{-1} \cup \{1\}$ such that there exist an integer N so that $s_n = 1$ for all $n \geq N$. We say that a word is reduced if

- $s_{i+1} \neq s_i^{-1}$ for all i such that $s_i \neq 1$.
- $s_i = 1$ implies that $s_{i+1} = 1$.

We denote $F(S)$ as the set of reducible words of S.

Proposition 3.4.2. Let S be a set. Then one can define a group structure on $F(S)$ by concatenation and cancelation. If $|S| = n$, then we call $F(S)$ the free group on n generators.

The cancelation rules are the following:

- $a^{-1} \cdot a = a \cdot a^{-1} = 1$
- $1 \cdot a = a \cdot 1 = a$

Example 3.4.3.

- Let $S = \{a\}$. Then $F(S)$ is the free group on one generator. The sequences a, aaa, a^{-1} and 1 are reduced words. Usual convention is to write aaa as a^3. Multiplication is done by concatenation and cancelation. So aaa multiplied with a^{-1} is the product $aaaa^{-1}$, which is then reduced to $aa = a^2$. From this is easily follows that $F(S) \cong \mathbb{Z}$.
- Let $S = \{a, b\}$. Then $F(S)$ is the free group on two generators. The sequences ab, ba, $a^3b^{-1}a^2$ are distinct reduced words. Note that $ab \neq ba$, so this is not a commutative group.

Even thought that the free groups are easy to describe, they do not seem do resemble many other common groups. Their usefulness comes from what is called the universal property of free groups.

Proposition 3.4.4. Let S be a set, G a group, $f : S \to G$ a function and $i : S \to F(S)$ the inclusion map. Then there exist a unique group homomorphism $\varphi : F(S) \to G$ such that the diagram commutes.

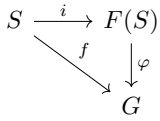


Figure 26. Universal property of free groups.

Proof. See [1, p.217] □

The real strength of this property is realised in the following proposition.

Proposition 3.4.5. Every finite group appears as the quotient of a free group.

Proof. Let G be a finite group and let S be a set of the same cardinality, thus there exist a bijective function $f : S \to G$. By the universal property of free groups, there is a homomorphism $\varphi : F(S) \to G$ such that $f = \varphi \circ i$. By the isomorphism theorem, we have that $\mathrm{Im}(\varphi) \cong F(S)/\mathrm{Ker}(\varphi)$. The map f is surjective, so φ must be as well. Hence $\mathrm{Im}(\varphi) = G$, and so $G \cong F(S)/\mathrm{Ker}(\varphi)$. □

The connection of the free group to Riemann surfaces comes thorugh the following proposition.

Proposition 3.4.6. Let $X = S^1$ and $\{x_1, ..., x_{n+1}\}$ a finite set of points on X. Then $\pi_1(X \backslash \{x_1, ..., x_{n+1}\}) \cong F(a_1, ..., a_n)$.

Proof. See [6, p.87]. □

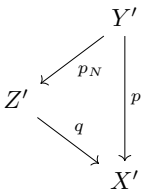
3.5 Application on $\mathbb{C}(t)$

Now we have gathered the necessary results to prove the inverse galois for $\mathbb{C}(t)$.

Theorem 3.5.1 (Inverse Galois for $\mathbb{C}(t)$)**.** Let $\mathbb{C}(t)$ be the field of rational polynomials in $\mathbb{C}$ and G any finite group. Then there exist a Galois extension $K/\mathbb{C}(t)$ such that $\mathrm{Gal}(K/\mathbb{C}(t)) \cong G$.

Proof.

- Let G be a finite group. Then $G \cong F(a_1, ..., a_n)/N$ for some normal subgroup N of the free group $F(a_1, ..., a_n)$ by proposition 3.4.5.
- Let $X = P^1$ and $X' = P^1 \backslash \{x_1, ..., x_{n+1}\}$ for some points $\{x_1, ..., x_{n+1}\} \subset P^1$. Then $\pi_1(X', x_0) \cong F(a_1, ..., a_n)$ by proposition 3.4.6.
- X' is locally simply connected and connected, so by theorems 2.4.4 and 2.4.5 there exist a universal cover $p : Y' \to X'$ such that
  - The cover is Galois.
  - $\mathrm{Gal}(Y'/X') \cong \pi_1(X', x_0) \cong F(a_1, ..., a_n)$.
  - Y' is connected.
- Let $Z' = Y'/N$. Z' is connected since it is a quotient of a connected space. By the Galois correspondence in topology, all covers in the diagram below are Galois since $N \subset \mathrm{Gal}(Y'/X')$ is normal.



  In particular, $\mathrm{Gal}(Z'/X') \cong F(a_1, ..., a_n)/N \cong G$, so this is a finite cover.
- The finite cover $q : Z' \to X'$ corresponds to a proper holomorphic map q of Riemann surfaces X, Y by theorem 3.2.9. In fact, Y is a finite Galois cover of X. So $\mathrm{Aut}(Y/X) \cong \mathrm{Gal}(Y'/X')$.
- Both X and Y are connected Riemann surfaces. X is compact, and Y is also compact because q is a proper map. So the finite Galois cover $q : Y \to X$ corresponds to a Galois field extension $\mathcal{M}(Y)/q^\star\mathcal{M}(X)$ by theorem 3.3.7. It also holds that $\mathrm{Gal}(\mathcal{M}(Y)/q^\star\mathcal{M}(X)) \cong \mathrm{Aut}(Y/X) \cong G$.
- The field of meromorphic functions on P^1 is the field of complex rational functions by 3.3.4. That is, $q^\star\mathcal{M}(X) \cong \mathbb{C}(t)$.

Hence, the field extension $\mathcal{M}(Y)/\mathbb{C}(t)$ is Galois with Galois group G. □

Bibliography

[1] Dummit, D. and Foote, R. [2004] *Abstract Algebra* [3rd Ed.]. Hoboken: John Wiley and Sons, Inc.

[2] Forster, O. [1981] *Lectures on Riemann Surfaces*. New York: Springer-Verlag New York, Inc.

[3] Hatcher, A. [2001] *Algebraic Topology*. E-book version, retrieved from http://www.math.cornell.edu/~hatcher.

[4] Lee, M. [2010] *Introduction to Topological Manifolds* [2nd Ed.]. New York: Springer.

[5] Stweart, I. [2015] *Galois Theory* [4th Ed.]. London: CRC Press Taylor & Francis Group.

[6] Szamuely, T. [2009] *Galois Groups and Fundamental Groups*. Cambridge: Cambridge University Press.