# A Graph-theoretic Artin $L$-function

Daksh Aggarwal

September 24, 2020

## 1 Introduction

The goal of this expository report is to explain a beautiful connection between graph theory and algebraic number theory. Our exposition is based on Audrey Terras' wonderful *Zeta Functions of Graphs* [12]. We will explore three main analogues between graphs and algebraic number theory, each building on the previous: Galois theory, the Frobenius automorphism, and the Artin $L$-function. We have attempted to emphasize the remarkable similarities and significant differences between the theories for graph coverings and extensions of number fields. It has been our endeavour to make the exposition accessible to the reader who has taken a first course in abstract algebra. Therefore we include informal introductions and concrete examples for algebraic topics such as finite Galois theory and number fields because they are very much relevant to properly see the wonderful juxtaposition that exists between graph coverings and number fields. Even for graph coverings, we emphasize examples and include only a handful of proofs to illustrate the formal ideas. The interested reader is encouraged to refer to Terras' book for more details about proofs and such. Indeed, our exposition focuses on a small subset of the topics covered in Terras' book, and in particular we have almost entirely left out the rich analytic viewpoint of the connection between graph coverings and number theory. Thus, our hope is that this serves as something of a primer to the algebraic aspect of Terras' book, so that the interested reader might gain even more from Terras' brisk exposition.

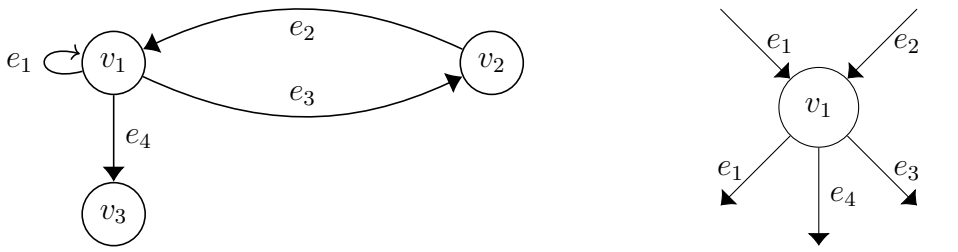
We first set our basic definitions pertaining to graphs, which might be slightly different from those with which the reader is familiar. A *graph* $X$ consists of a pair of sets $(V_X, E_X)$: $V_X$ is called the *vertex set* and $E_X$ is the *edge set*, consisting of an ordered pair of elements from $V_X$. All our graphs will be finite, so that $|V_X|, |E_X| < \infty$. A *path* $p$ in a graph $X$ from a vertex $a$ to vertex $b$ is a sequence of vertices $\langle v_1, v_2, \ldots, v_n \rangle$ such that $v_1 = a$, $v_n = b$, and for $2 \leq i \leq n$, $v_{i-1}$ and $v_i$ are *adjacent*, meaning that $(v_{i-1}, v_i) \in E_X$. As we will shortly see, we will be putting a sort of topology on our graphs, and therefore it will be useful to also think of an edge $(v_{i-1}, v_i)$ as a directed interval from $v_{i-1}$ to $v_i$. A *connected* graph is one in which there exists a path between any two vertices. Without exception, all the results in this report will be about connected graphs. Further, we also allow graphs to have loops and multiple edges, but all of our

examples will be focused on graphs without loops and multiple edges. We will not need much in the way of deep theorems from graph theory, and therefore a basic intuition about graphs will suffice.

# 2 Finite Unramified Coverings for Graphs

We start with the concept of a graph covering that will drive most, if not all, of the striking analogies we will draw with field theory and algebraic number theory. The notion of a covering—involving open sets, homeomorphisms, and such—belongs properly to topology. If the reader is familiar with basic topology, then they will recognize that a graph covering is a discretized version of a topological covering. By these remarks, we also want to indicate that we will be thinking about a graph much more as a topological object rather than a purely combinatorial one.

To define a graph covering, we need a notion of a neighborhood. A *neighborhood* $U$ of a vertex $v$ in a directed graph $X$ is created by taking half of every edge incident at $v$; since we are treating an edge as a directed interval, the notion of dividing an edge makes sense. The "half" is arbitrary and is meant to convey that we are concerned only with the locality of vertex $v$. For example, the neighborhood of vertex $v_1$ is shown in Figure 2.1.




(a) A directed graph

(b) Neighborhood of $v_1$

Figure 2.1

A neighborhood is analogous to an $\epsilon$-radius ball centered at a point $p \in \mathbb{R}$ for some $\epsilon > 0$. While in $\mathbb{R}$ the choice of $\epsilon$ can make a difference, for graph vertices there is a unique neighborhood centered at each vertex, for our purposes at least; therefore we may speak of "the neighborhood" of a vertex $v$. While we won't require notions of "openness" and "closedness" for a graph neighborhood, the way we have defined neighborhoods puts a sort of topology on the graph.

Before we formally define a graph covering, consider the graph-theoretic analogue of the covering of the unit circle by the real line $\mathbb{R}$.

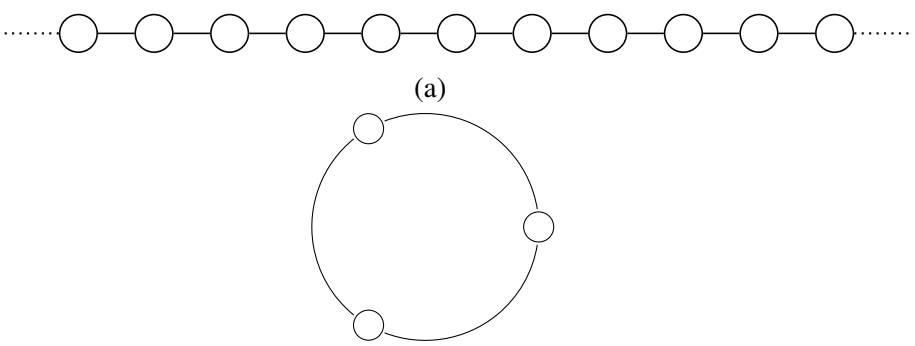



Figure 2.2: (a) An infinite path graph as a covering of (b) the cycle graph $C_3$

Notice that though the two graphs of Figure 2.2 are globally very different, the neighborhoods of a vertex in the infinite path graph and in $C_3$ are the "same" as the neighborhood pictured in Figure 2.3; this local "sameness" of the graphs is the defining feature of a graph covering.

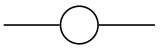
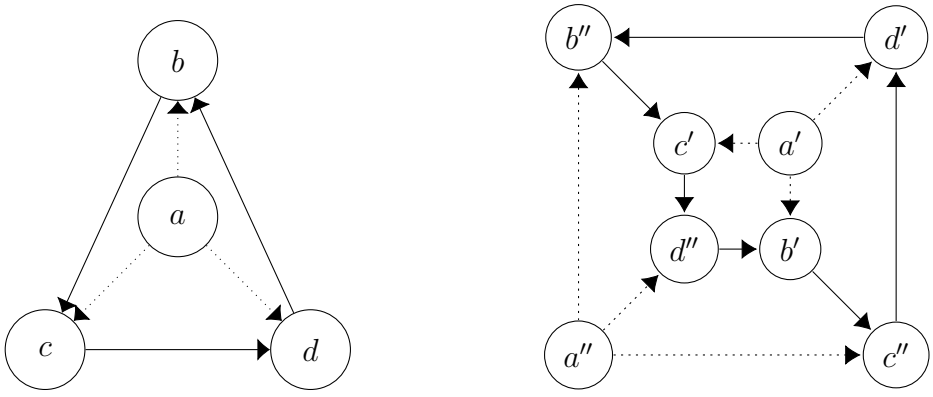


Figure 2.3: A neighborhood in the path graph and $C_3$

For example, the cube is a covering of the tetrahedron $K_4$ shown in Figure 2.4.




(a) The tetrahedron $K_4$ (b) The cube as a covering of $K_4$

Figure 2.4

The notion of "sameness" here can be formalized by the concept of a homeomorphism, the topological equivalent of an isomorphism. A *homeomorphism* is a bijective map that preserves the topology of its domain, i.e., it maps neighborhoods to neighborhoods and the preimage of a neighborhood is a neighborhood too. In the example of the cube and $K_4$, for each vertex $v$ in $X$,

the neighborhoods of $v'$ and $v''$ are *homeomorphic* to the neighborhood of $v$; for instance, $a$ has exactly three edges originating from it and so do $a'$ and $a''$. The concept of a graph covering is formalized as follows.

**Definition 2.1 (Covering)** An undirected finite graph $Y$ is a *covering* of an undirected graph $X$ if, after arbitrarily directing the edges of $X$, the edges of $Y$ can be suitably directed such that there exists an onto covering map $\pi : Y \to X$. That is, for any $v \in V_X$, if $\tilde{U}$ is the neighborhood of a vertex in $\pi^{-1}(v)$ and $U$ is the neighborhood of $v$, then $\pi$ restricts to a homeomorphism $\tilde{U} \to U$. A graph covering $Y$ of $X$ is denoted as $Y/X$.

Referring to Figures 2.4, in the notation of the definition, $\pi^{-1}(v) = \{v', v''\}$ for each vertex $v$ in $K_4$; we say $v'$ and $v''$ *lie above* $v$. So, since there are two local copies in the cube of each vertex of $K_4$, the cube is called a *2-sheeted* or *quadratic* covering of $K_4$.

In general, for some positive integer $d$, we can have a *d-sheeted* $Y$ covering of a graph $X$: for each vertex $v$ of $X$, $\pi^{-1}(v)$ contains exactly $d$ vertices of $Y$. It is natural to ask if for every $d \in \mathbb{Z}_{>0}$, there is a $d$-sheeted covering $Y$ for a graph $X$. The answer is yes, because we could just consider the graph $Y$ consisting of $d$ disjoint copies of $X$; here we note that henceforth we will not consider this kind of a construction or any disconnected graph a covering for our purposes. A more interesting construction arises from considering a spanning tree of $X$. A *spanning tree* $T$ of a graph $X$ is a subgraph of $X$ that is a tree and contains all the vertices of $X$. To get a $d$-sheeted covering of $X$, we make $d$ copies of a spanning tree $T$ of $X$, and then add edges between the copies of $T$ so that the definition of a covering is satisfied.

For instance, to obtain a quadratic covering of $K_4$, we make two copies of the spanning tree of $K_4$, indicated by dotted edges in Figure 2.4(a), and then "glue" them together by edges so that we have homeomorphic neighborhoods. This glueing is not necessarily unique; one way of glueing gives us the cube of Figure 2.4(b) and another way gives us the covering of Figure 2.5 below.

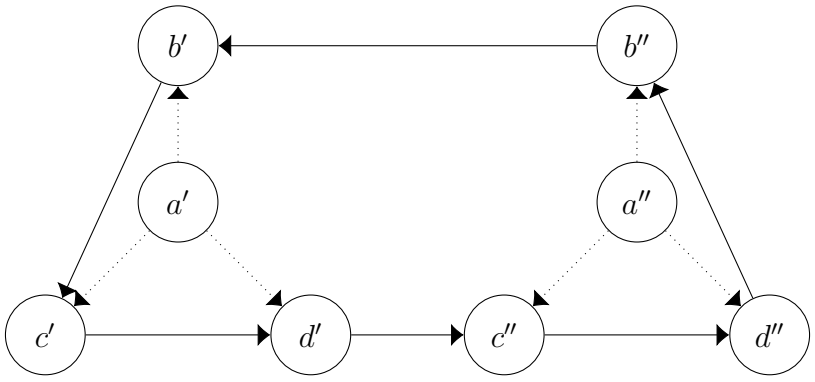



Figure 2.5: Another quadratic covering of $K_4$

The difference between the two coverings is that in the cube there are six edges between the two sheets while in the other there are only two. We will later see that the analogy drawn with

number theory will suggest results that will help us construct coverings of a graph that have specific properties.

The concept of a graph covering suggests an analogy with field extensions, which we now briefly introduce.

**Definition 2.2 (Field extension)** A field $K$ is a *field extension* of a field $L$ if $L \subseteq K$. More generally, $K$ is a field extension of $L$ if there is a nonzero ring homomorphism $L \to K$, called an *embedding* of $L$ in $K$. This relationship is denoted as $K/L$.

In a field extension $K/L$, we can view $K$ as a vector space over $L$ – the axioms for a vector space are directly implied by the field axioms. So we then have a notion of a basis for $K$ when viewed as a $L$-vector space and can therefore talk about the dimension of $K$. The *degree* of a field extension $K/L$ is the dimension $\dim_L K$ of $K$ as a $L$-vector space and is denoted $[K : L]$. We will care only about finite field extensions $K/L$ here, i.e., $[K : L] < \infty$. A familiar example of a finite field extension is $\mathbb{C}/\mathbb{R}$, which has degree 2 since $\{1, i\}$ form a $\mathbb{R}$-basis for $\mathbb{C}$. Notice that the degree of a field extension corresponds to the number of sheets in a graph covering $Y/X$.

When $K/L$ is a finite field extension and $L = \mathbb{Q}$, then $K$ is called a *number field*. Important examples of number fields are *quadratic number fields*, which are of form $\mathbb{Q}(\sqrt{d})$ where $d$ is a squarefree integer. What is meant by $\mathbb{Q}(\sqrt{d})$? The field $\mathbb{Q}(\sqrt{d})$ is the smallest field that contains both $\mathbb{Q}$ and $\sqrt{d}$. Since $\mathbb{Q}(\sqrt{d})$ is a ring, it must have all elements of the form $p + q\sqrt{d}$ for any $p, q \in \mathbb{Q}$. Because we also want it to be field, we must include all elements of the form $(p + q\sqrt{d})^{-1}$ for $p, q \in \mathbb{Q}$, which is the same as $(p - q\sqrt{d})/(p^2 - q^2 d)$ and this is again of the form $p' + q'\sqrt{d}$, for some $p', q' \in \mathbb{Q}$. So $\mathbb{Q}(\sqrt{d}) = \{p + q\sqrt{d} : p, q \in \mathbb{Q}\}$. We will be constructing analogues for coverings of some of the fundamental objects associated with a number field (especially ones which are Galois). The reader might also wonder why they are called "number fields"; we will be discussing the answer to this and more soon.

At first glance, the analogy between graph coverings and field extensions might seem less than perfect. For instance, there is no obvious notion of a local homeomorphism in a field extension and there is no canonical inclusion map in a graph covering. However, we will have to wait until we have discussed the Fundamental Theorem of Galois Theory for coverings before we see its striking similarity with field extensions. We now begin to build up to this theorem now.

# 3 Galois Theory

## 3.1 Galois Coverings and Extensions

To define what it means for a finite field extension $K/L$ to be Galois, we need a little terminology. We will be assuming throughout that $K$ has characteristic 0 so as to avoid separability issues. This doesn't constitute any disadvantage for us since we will eventually be working over $\mathbb{Q}$, whose field extensions always have characteristic 0.

We define the group of *$L$-automorphisms of $K$*, denoted $\mathrm{Aut}(K/L)$, to consist of all automorphisms of $K$ that leave $L$ pointwise fixed: i.e., $\sigma \in \mathrm{Aut}(K/L)$ if and only if $\sigma(l) = l$ for all $l \in L$. For instance, consider $\mathrm{Aut}(\mathbb{Q}(\sqrt{2})/\mathbb{Q})$. If $\sigma$ is an automorphism in $\mathrm{Aut}(\mathbb{Q}(\sqrt{2})/\mathbb{Q})$, then $\sigma(\sqrt{2})^2 = \sigma(\sqrt{2}^2) = \sigma(2) = 2$, and so $\sigma(\sqrt{2}) \in \{\sqrt{2}, -\sqrt{2}\}$. Once $\sigma(\sqrt{2})$ has been determined, the action of $\sigma$ on every element $p + q\sqrt{2} \in \mathbb{Q}(\sqrt{2})$ has been determined since $\sigma(p + q\sqrt{2}) = p + q\sigma(\sqrt{2})$. Therefore, there are precisely two elements in $\mathrm{Aut}(\mathbb{Q}(\sqrt{2})/\mathbb{Q})$: one is the identity automorphism and the other exchanges $\sqrt{2}$ with $-\sqrt{2}$. So, $\left|\mathrm{Aut}(\mathbb{Q}(\sqrt{2})/\mathbb{Q})\right| = 2 = [\mathbb{Q}(\sqrt{2}) : \mathbb{Q}]$. This observation can be taken to be the definition of a finite Galois extension, but we defer this for a little and instead use it as motivation for the definition of a Galois graph covering.

Recall that a *graph automorphism* $f$ of a graph $X$ is an edge-preserving bijective function $f : V_X \to V_X$, i.e., $f$ is a permutation of the vertices such that for any $a, b \in V_X$, $(a, b) \in E_X$ if and only if $(f(a), f(b)) \in E_X$.

**Definition 3.1 (Galois covering)** Let $Y/X$ be a $d$-sheeted covering with projection map $\pi : Y \to X$. We call $Y$ a *Galois covering* of $X$ if there are $d$ graph automorphisms $\sigma : Y \to Y$ such that $\pi \circ \sigma = \pi$. The *Galois group* $\mathrm{Gal}(Y/X)$ is the group of maps $\sigma$ under function composition.

For an example, consider the cube of Figure 2.4, which is a quadratic Galois covering of $K_4$. Its Galois group consists of the trivial automorphism and the automorphism that exchanges $v'$ with $v''$ for each vertex $v$ in $G$. However, the quadratic covering of Figure 2.5 is not Galois since a nontrivial automorphism would need to exchange $d'$ with $d''$, and $b'$ with $b''$, but $b''$ and $d''$ are adjacent while $b'$ and $d'$ are not.

Returning to a finite field extension $K/L$, we have hinted at what it means for $K/L$ to be Galois. However, we might wish for a more algebraic characterization.

First, it is not always the case that $|\mathrm{Aut}(K/L)| = [K : L]$. For an example, consider $K = \mathbb{Q}(\sqrt[3]{2})$ and $L = \mathbb{Q}$. For a $\sigma \in \mathrm{Aut}(\mathbb{Q}(\sqrt[3]{2})/\mathbb{Q})$, we require $\sigma(\sqrt[3]{2})^3 = \sigma(2) = 2$; so $\sigma(\sqrt[3]{2})$ is a cube root of 2 but $\mathbb{Q}(\sqrt[3]{2}) \subset \mathbb{R}$ and the only real cube root of 2 is $\sqrt[3]{2}$. Therefore, $\sigma(\sqrt[3]{2})$ must be $\sqrt[3]{2}$. It is not hard to show that $\{1, \sqrt[3]{2}, \sqrt[3]{2}^2\}$ is a $\mathbb{Q}$-basis for $\mathbb{Q}(\sqrt[3]{2})$, and so $\sigma$ fixes all of $\mathbb{Q}(\sqrt[3]{2})$. Thus, $\mathrm{Aut}(\mathbb{Q}(\sqrt[3]{2})/\mathbb{Q})$ consists of just the identity automorphism.

The *fixed field* $K_G$ of a group of automorphisms $G$ of a field $K$ is defined to be the subset of $K$ that is pointwise fixed by $G$. That is, $k \in K_G$ if and only if $\sigma(k) = k$ for all $\sigma \in G$.[1] For instance, we see that the fixed field of $\mathrm{Aut}(\mathbb{Q}(\sqrt{2})/\mathbb{Q})$ is $\mathbb{Q}$ while that of $\mathrm{Aut}(\mathbb{Q}(\sqrt[3]{2})/\mathbb{Q})$ is the whole field $\mathbb{Q}(\sqrt[3]{2})$. The observation that the fixed field of $\mathrm{Aut}(\mathbb{Q}(\sqrt{2})/\mathbb{Q})$ is exactly $\mathbb{Q}$ is an important one and constitutes what it means to be a Galois extension.

**Definition 3.2 (Galois field extension)** A finite field extension $K/L$ is *Galois* if and only if the

[1] We haven't actually proven that $\mathrm{Aut}(L/K)$ is a group or that $K_G$ is a field, but these facts follows rather quickly from the definitions.

fixed field of $\mathrm{Aut}(K/L)$ is $L$. When $K/L$ is Galois, we denote $\mathrm{Aut}(K/L)$ as $\mathrm{Gal}(K/L)$ instead and call it the *Galois group* of $K/L$.

The characterization we indicated earlier is also true.

**Theorem 3.3** *A finite field extension $K/L$ is Galois if and only if* $|\mathrm{Aut}(K/L)| = [K : L]$.

A proof can be found in [3, pp. 244-245].

The analogy between Galois extensions and Galois coverings is illustrated by the diagrams of Figure 3.1. Here $\iota$ denotes the embedding of the field $L$ into $K$ and $\pi$ as usual is the projection map. The condition $(\sigma \circ \iota)(l) = \iota(l)$ for all $l \in L$ is precisely the condition that $L$ is fixed pointwise by $\sigma$. When $K/L$ is Galois, there are exactly $[K : L]$ automorphisms $\sigma$ of $K$ which make the diagram commute. Similarly for a Galois covering.


(a) A Galois field extension

(b) A Galois covering

Figure 3.1

We now return to developing the Galois theory for graph coverings. This next proposition will be basic to proving the main theorem of this section. It tells us that if two vertices $\widetilde{v_1}$ and $\widetilde{v_2}$ of a Galois covering $Y/X$ lie above a vertex $v$ of $X$, then there exists an automorphism $g \in \mathrm{Gal}(Y/X)$ such that $g(\widetilde{v_1}) = \widetilde{v_2}$. Recall that for a mapping $f : Y \to X$, the *fiber* of $x \in X$ under $f$ is its preimage $f^{-1}(x)$.

**Proposition 3.4** *Suppose that $Y/X$ is a Galois covering and let $v$ be a vertex in $X$. Then* $\mathrm{Gal}(Y/X)$ *acts transitively on the fiber of $v$ under the projection map $\pi : Y \to X$.*

To prove this proposition, we need the next lemma, which we will repeatedly appeal to even later and is true for non-Galois coverings too. Given a path $P$ in $X$, a *lift* of $P$ to $Y$ is a path $\widetilde{P}$ in $Y$ such that $\pi(\widetilde{P}) = P$. For example, the path $\langle b, c, d\rangle$ in $K_4$ lifts to the paths $\langle b', c'', d'\rangle$ and $\langle b'', c', d''\rangle$ in the cube (Figure 2.4).

**Lemma 3.5 (Unique path-lifting property)** *Let $Y/X$ be a covering. Let $v$ be a vertex in $X$ and let $\widetilde{v}$ be a vertex in the fiber of $v$ under the projection $\pi$. If $P$ is a path in $X$ with initial vertex $v$, then there is a unique lift $\widetilde{P}$ of $P$ to $Y$ with initial vertex $\widetilde{v}$.*

*Proof.* Let $\widetilde{U}$ and $U$ be neighborhoods of $\widetilde{v}$ and $v$ respectively. Suppose the first edge of $P$ is $e$. Since we require that $\pi : \widetilde{U} \to U$ be a homeomorphism, there is precisely one edge $\widetilde{e}$ in the

neighborhood of $\widetilde{v}$ such that $\pi(\widetilde{e}) = e$. So the first edge of $\widetilde{P}$ has to be $\widetilde{e}$. Repeating the same argument for the remaining vertices of $P$, we conclude that there is a unique lift $\widetilde{P}$ of $P$ starting at $\widetilde{v}$. □

We now prove Proposition 3.4.

*Proof.* We have to show that the $d$ distinct automorphisms in $\mathrm{Gal}(Y/X)$ map a vertex to $d$ distinct vertices of $Y$. Now, two automorphisms $g_1$ and $g_2$ map a vertex $\widetilde{v}$ to distinct vertices if and only if $g_1^{-1}g_2(\widetilde{v}) \neq \widetilde{v}$. So, it is sufficient to show that, for some vertex $\widetilde{v}$ in $Y$ and an automorphism $g \in \mathrm{Gal}(Y/X)$, if $g(\widetilde{v}) = \widetilde{v}$ then $g$ is the trivial automorphism. Let $\widetilde{u}$ be any other vertex of $Y$ and let $\widetilde{P}$ be a path from $\widetilde{v}$ to $\widetilde{u}$. Let $P$ be the projection of $\widetilde{P}$ to $X$. Note that the path $g(\widetilde{P})$ in $Y$ begins at $g(\widetilde{v}) = \widetilde{v}$ and ends at $g(\widetilde{u})$. Further, since $\pi \circ g = g$, we have $\pi(g(\widetilde{P})) = \pi(\widetilde{P}) = P$ and so both $g(\widetilde{P})$ and $\widetilde{P}$ are lifts of $P$ starting at $\widetilde{v}$. By Lemma 3.5, we must then have $g(\widetilde{P}) = P$, and thus $g(\widetilde{u}) = u$. Therefore $g$ is the trivial automorphism. □

Proposition 3.4 gives us a useful way to structure how we think about the sheets of a Galois covering $Y/X$. Let $v$ be a vertex in $X$. Then, corresponding to the identity automorphism, we can arbitrarily label some vertex of $Y$ in the fiber of $v$ as $(v, 1)$ and label the vertex we obtain by applying an automorphism $g \in \mathrm{Gal}(Y/X)$ to $(v, 1)$ as vertex $(v, g)$. The transitivity of the action of $\mathrm{Gal}(Y/X)$ on each fiber ensures we can label *all* vertices of $Y$ by pairs of the form $(v, g)$ for some vertex $v$ in $X$ and $g \in \mathrm{Gal}(Y/X)$.

## 3.2 Fundamental Theorem of Galois Theory

We begin with a broad overview of the Fundamental Theorem of Galois Theory, so that the reader who has not seen Galois Theory before might be able to better appreciate Terras' Galois Theory for graph coverings. We refer the reader to [3] for a more complete exposition of finite Galois Theory.

Suppose we have a finite Galois extension $K/L$ and let $H$ be a subgroup of $\mathrm{Gal}(K/L)$. Now, what is the fixed field $K_H$? By definition, $K_H$ is the subfield of $K$ that is pointwise fixed by all elements of $H$. Since $H \leq \mathrm{Gal}(K/L)$, we certainly know that $L \subseteq K_H$. Thus $K_H$ is an intermediate extension of $K/L$, i.e., $L \subseteq K_H \subseteq K$. What about $\mathrm{Aut}(K/K_H)$? We can see that every $\sigma \in \mathrm{Aut}(K/K_H)$ must also be in $\mathrm{Gal}(K/L)$ since $L \subseteq K_H$, and so $\mathrm{Aut}(K/K_H)$ is a subgroup of $\mathrm{Gal}(K/L)$. The fascinating part is that in fact $\mathrm{Aut}(K/K_H) = H$, which by the definition means that $K/K_H$ is also Galois! Put differently, this means that the map sending an intermediate field $F$ of $K/L$ to $\mathrm{Aut}(K/F)$ is a surjective map $\varphi$ from the set of intermediate fields of $K/L$ to the set of subgroups of $\mathrm{Gal}(K/L)$.

Moreover, every subfield $F$ of $K$ containing $L$ arises as the fixed field of some subgroup $H \leq \mathrm{Gal}(K/L)$, i.e., $F = K_H$ and, as you would hope, it can be shown that $H = \mathrm{Aut}(K/F)$. So, $F = K_{\mathrm{Aut}(K/F)}$. This means that the map $\varphi$ (from above) is injective − if for two interme-

diate fields $F_1$ and $F_2$, $\mathrm{Aut}(K/F_1) = \mathrm{Aut}(K/F_2)$, then $F_1 = K_{\mathrm{Aut}(K/F_1)} = K_{\mathrm{Aut}(K/F_2)} = F_2$. Therefore, there is a bijective correspondence between the intermediate fields of a Galois extension and the subgroups of its Galois group. This fact is the central assertion of the Fundamental theorem for Galois field extensions.

Let us see a few examples. Consider $\mathbb{Q}(\sqrt{2})/\mathbb{Q}$, which has a Galois group of just two elements, and is thus isomorphic to $\mathbb{Z}/2\mathbb{Z}$. The group $\mathbb{Z}/2\mathbb{Z}$ has only two subgroups, namely the trivial subgroup and the whole group itself. The trivial subgroup corresponds to $\mathbb{Q}$ while $\mathbb{Z}/2\mathbb{Z}$ corresponds to $\mathbb{Q}(\sqrt{2})$; the Fundamental theorem then implies that there are is no field strictly between $\mathbb{Q}$ and $\mathbb{Q}(\sqrt{2})$. Next, consider the field extension $\mathbb{Q}(\zeta_5)/\mathbb{Q}$, where $\zeta_5$ is a primitive fifth root of unity (so $\zeta_5^5 = 1$, and $\zeta_5^k \neq 1$ for any $1 \leq k < 5$). The field $\mathbb{Q}(\zeta_5)$ consists of all elements of the form $a_0 + a_1\zeta_5 + a_2\zeta_5^2 + a_3\zeta_5^3$, for $a_i \in \mathbb{Q}$, and is therefore is a degree-4 extension of $\mathbb{Q}$. As earlier, for any $\sigma \in \mathrm{Aut}(\mathbb{Q}(\zeta_5)/\mathbb{Q})$ we need $\sigma(\zeta_5)^5 = 1$, and so $\sigma(\zeta_5) \in \{1, \zeta_5, \zeta_5^2, \zeta_5^3, \zeta_5^4\}$; however $\sigma(1) = 1$, and so $\sigma(\zeta_5)$ must be $\zeta_5^k$ for some $1 \leq k < 5$. Once $\sigma(\zeta_k)$ is fixed, the action of $\sigma$ on the rest of the field is determined since

$$\sigma(a_0 + a_1\zeta_5 + a_2\zeta_5^2 + a_3\zeta_5^3) = a_0 + a_1\sigma(\zeta_5) + a_2\sigma(\zeta_5)^2 + a_3\sigma(\zeta_5)^3.$$

Therefore, $\mathrm{Aut}(\mathbb{Q}(\zeta_5)/\mathbb{Q})$ consists of the four automorphisms $\sigma_k$ that send $\zeta_5$ to $\zeta_5^k$ for $1 \leq k < 5$, implying that $\mathbb{Q}(\zeta_5)/\mathbb{Q}$ is Galois. Further, notice that $\mathrm{Gal}(\mathbb{Q}(\zeta_5)/\mathbb{Q})$ is cyclic with generator $\sigma_2$, and is therefore isomorphic to $(\mathbb{Z}/5\mathbb{Z})^\times$. Now the subgroups of $(\mathbb{Z}/5\mathbb{Z})^\times$ are the trivial subgroup, the subgroup $\{\overline{1}, \overline{4}\}$, and the whole group itself. Therefore, the Fundamental theorem tells us that there is a field strictly between $\mathbb{Q}$ and $\mathbb{Q}(\zeta_5)$. It is easy to show that this intermediate field is $\mathbb{Q}(\zeta_5+\zeta_5^{-1}) = \mathbb{Q}(\zeta_5+\zeta_5^4)$, which corresponds to the fixed field of the subgroup of automorphisms $\{\sigma_1, \sigma_4\}$. A similar analysis applies more generally to field extensions of the form $\mathbb{Q}(\zeta_n)/\mathbb{Q}$, with $\zeta_n$ a primitive $n$-th root of unity; these are called *cyclotomic extensions* and are of great importance in algebraic number theory.

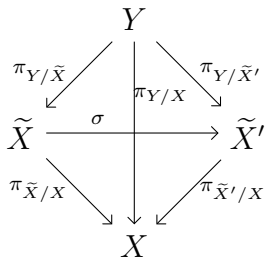
We now move to the analogue of the Fundamental Theorem for graph coverings, beginning with the notion of an intermediate covering. For a covering $Y/X$, let $\pi_{Y/X} : Y \to X$ denote its projection map.

**Definition 3.6 (Intermediate Covering)** Let $Y/X$ be a covering of graphs. Then a graph $\tilde{X}$ is an *intermediate covering* to $Y/X$ if $\widetilde{X}/X$ is a covering, $Y/\widetilde{X}$ is a covering, and the projection maps are transitive:

$$\pi_{Y/X} = \pi_{\widetilde{X}/X} \circ \pi_{Y/\widetilde{X}}.$$

**Definition 3.7 (Covering Isomorphism)** Let $\widetilde{X}$ and $\widetilde{X}'$ be intermediate coverings to $Y/X$. Then a graph isomorphism $\sigma : \widetilde{X} \to \widetilde{X}'$ is a *covering isomorphism* if $\pi_{\widetilde{X}/X} = \pi_{\widetilde{X}'/X} \circ \sigma$; if such a $\sigma$ exists, $\widetilde{X}$ and $\widetilde{X}'$ are *covering isomorphic*. Further, if $\sigma \circ \pi_{Y/\widetilde{X}} = \pi_{Y/\widetilde{X}'}$, then $\widetilde{X}$ and $\widetilde{X}'$ are said to be *equivalent*, denoted $\widetilde{X} \approx \widetilde{X}'$.

Summarising, when we have two equivalent intermediate coverings $\widetilde{X}$ and $\widetilde{X}'$ in a covering $Y/X$, the following diagram commutes:




For a simple example of a covering isomorphism, consider the cube as a covering of $K_4$ (Figure 2.4). We can trivially view the cube as an intermediate covering between the cube and $K_4$, and so here we take both $\widetilde{X}$ and $\widetilde{X}'$ to be the cube. Then the non-identity automorphism $\sigma$ exchanging $v'$ with $v''$ is a covering isomorphism from the cube to itself precisely because $\sigma$ belongs to the Galois group of the covering; this idea that an automorphism in the Galois group of a Galois covering gives us a covering isomorphism from the covering to itself will be exploited in the proof of Theorem 3.11.

Drawing analogies with field extensions, we might predict that there is a bijective correspondence between intermediate coverings of a Galois covering and subgroups of its Galois group. We would be mostly right in asserting this except that we cannot hope for a literal equality of graphs when their corresponding subgroups are equal since there is no canonical inclusion map; however we settle for the slightly weaker sense of equivalence defined above. Here we prove only the first two assertions because the rest follow quite directly from the definitions and utilize the same ideas as for the first ones.

**Theorem 3.8 (Fundamental Theorem of Galois Theory)** *Let $Y/X$ be a Galois covering with Galois group $G$.*

1. *Given a subgroup $H \leq G$, there exists a graph $\widetilde{X}$ intermediate to $Y/X$ such that $H = \mathrm{Gal}(Y/\widetilde{X})$. Denote $\widetilde{X}$ as $\widetilde{X}(H)$.*
2. *Suppose that $\widetilde{X}$ is intermediate to $Y/X$. Then there is a subgroup $H \leq G$ which equals $\mathrm{Gal}(Y/\widetilde{X})$. Denote $H$ as $H(\widetilde{X})$.*
3. *Two intermediate graphs $\widetilde{X}$ and $\widetilde{X}'$ are equivalent (in the sense of Definition 3.7) if and only if $H(\widetilde{X}) = H(\widetilde{X}')$.*
4. *$H(\widetilde{X}(H)) = H$ and $\widetilde{X}(H(\widetilde{X})) \approx \widetilde{X}$. So there is a one-to-one correspondence $\widetilde{X} \leftrightarrow H$ between coverings intermediate to $Y/X$ and subgroups of $G(Y/X)$.*
5. *If $\widetilde{X}_1 \leftrightarrow H_1$ and $\widetilde{X}_2 \leftrightarrow H_2$ then $\widetilde{X}_1$ is intermediate to $Y/\widetilde{X}_2$ if and only if $H_1 \leq H_2$.*

*Proof of [1 and 2].*

1. The intermediate covering $\widetilde{X}$ is constructed as follows. We let the vertices of $\widetilde{X}$ be $\{(v, Hg) \mid v \in V_X, g \in G\}$. Two vertices $(v, Hr)$ and $(w, Hs)$ are adjacent if and only if $(v, hr)$ and $(w, h's)$ are adjacent in $Y$ for some $h, h' \in H$.

First, $Y/\widetilde{X}$ is a covering via the map $\pi_{Y/\widetilde{X}} : (v, g) \mapsto (v, Hg)$ and $\tilde{X}/X$ is a covering via $\pi_{\widetilde{X}/X} : (v, Hg) \mapsto v$. Thus, $\widetilde{X}$ is intermediate to $Y/X$ because

$$\pi_{\widetilde{X}/X} \circ \pi_{Y/\widetilde{X}}(v, g) = v = \pi_{Y/X}(v, g).$$

To check that $H$ is the Galois group $\mathrm{Gal}(Y/\widetilde{X})$, let $h \in H$. Then note

$$\pi_{Y/\widetilde{X}} \circ h(v, g) = \pi_{Y/\widetilde{X}}(v, hg) = (v, Hg) = \pi_{Y/\widetilde{X}}(v, g).$$

2. Fix a vertex $v_0$ in $X$. Consider $(v_0, 1)$ in $Y$. Then

$$H = \{h \in G \mid \pi_{Y/\widetilde{X}}(v_0, h) = \pi_{Y/\widetilde{X}}(v_0, 1)\}.$$

Since $G$ is finite, to prove $H$ is a subgroup we need only check it is closed under the group operation. We denote $\pi_{Y/\widetilde{X}}(v_0, 1)$ as $(v_0, H)$. Let $h_1, h_2 \in H$. Consider a path $\widetilde{p}$ on $Y$ from $(v_0, 1)$ to $(v_0, h_2)$. Then, $h_1 \circ \widetilde{p}$ is a path from $(v_0, h_1)$ to $(v_0, h_1h_2)$. Now project $\widetilde{p}$ to $\tilde{X}$ to get a loop at $(v_0, H)$ and then lift this loop to $Y$ beginning at $(v_0, h_1)$ and call this path $\widetilde{p}'$. Since $h_1 \in G(Y/X)$, by Lemma 3.5 we must have $h_1 \circ \widetilde{p} = \widetilde{p}'$ and so $(v_0, h_1h_2)$ too lies above $(v_0, H)$.

To check that $H = \mathrm{Gal}(Y/\tilde{X})$, we need to show that

$$\pi_{Y/\widetilde{X}}(v, hg) = (v, Hg) := \pi_{Y/\widetilde{X}}(v, g),$$

for any vertex $v$ of $X$, $h \in H$, and $g \in G$. Let $\widetilde{p}$ be a path from $(v_0, 1)$ to $(v, g)$. Then $h \circ p$ is a path from $(v_0, h)$ to $(v, hg)$. Now project $\widetilde{p}$ to a path $p$ in $\widetilde{X}'$ from $(v_0, H)$ to $(v_0, Hg)$. Lift $p$ to $Y$ starting at $(v_0, h)$ and since $h \in \mathrm{Gal}(Y/X)$, it must be that (Lemma 3.5) this lift is the same as $h \circ p$, i.e., $(v_0, hg)$ also lies above $(v, Hg)$.

□

The Fundamental Theorem for Galois field extensions guarantees us even more. If $F$ is an intermediate field in a Galois extension $K/L$, then $F/L$ is a Galois extension if and only if $\mathrm{Aut}(K/F)$ is a normal subgroup of $\mathrm{Gal}(K/L)$; in fact, when $F/L$ is Galois, its Galois group $\mathrm{Gal}(F/L)$ is isomorphic to the quotient group $\mathrm{Gal}(K/L)/\mathrm{Gal}(K/F)$. Proving these facts properly requires field theory but here is the basic idea.

It can be shown that $F/L$ is Galois if and only if $\sigma(F) \subseteq F$ for all $\sigma \in \mathrm{Gal}(K/L)$. So, $F/L$ is Galois if and only if for all $\tau \in \mathrm{Aut}(K/F)$, $\sigma \in \mathrm{Gal}(K/L)$, and $\alpha \in F$, $\tau(\sigma(\alpha)) = \sigma(\alpha)$, i.e., $\sigma^{-1}\tau\sigma(\alpha) = \alpha$. This means that $F/L$ is Galois if and only if $\sigma^{-1}\,\mathrm{Aut}(K/F)\sigma \subseteq \mathrm{Aut}(K/F)$ for all $\sigma \in \mathrm{Gal}(K/L)$, i.e., $\mathrm{Aut}(K/F)$ is normal in $\mathrm{Gal}(K/L)$.

Now, suppose $F/L$ is Galois, so that for each $\sigma \in \mathrm{Gal}(K/L)$, we have $\sigma(F) \subseteq F$. So, each $\sigma \in \mathrm{Gal}(K/L)$ restricts to an automorphism $\sigma_F$ of $F$ and since $L \subseteq F$, $\sigma_F \in \mathrm{Gal}(F/L)$. Thus we have a homomorphism $\phi : \mathrm{Gal}(K/L) \to \mathrm{Gal}(F/L)$, given by $\phi(\sigma) = \sigma_F$. The

kernel of $\phi$ is the set of all automorphisms $\tau \in \mathrm{Gal}(K/L)$ such that $\tau(\alpha) = \alpha$ for all $\alpha \in F$, which by definition means that $\mathrm{Ker}(\phi) = \mathrm{Gal}(K/F)$. Therefore, the image of $\mathrm{Gal}(K/L)$ in $\mathrm{Gal}(F/L)$ under $\phi$ is isomorphic to $\mathrm{Gal}(K/L)/\mathrm{Gal}(K/F)$. By Theorem 3.3, we know that $|\mathrm{Gal}(K/L)/\mathrm{Gal}(K/F)| = [K : L]/[K : F]$, which is equal to $[F : L]$ since $F$ is an intermediate field of $K/L$.[2] Therefore $\phi$ is surjective and so $\mathrm{Gal}(K/L)/\mathrm{Gal}(K/F) \cong \mathrm{Gal}(F/L)$.

In Theorem 3.11, we sketch proofs of the analogues of these facts for a Galois covering, but we prove an auxiliary result Theorem 3.10 first.

**Definition 3.9 (Conjugate coverings)** Let $Y/X$ be a Galois covering. If we have correspondences of intermediate coverings and subgroups of $\mathrm{Gal}(Y/X)$, $\widetilde{X} \leftrightarrow H$ and $\widetilde{X}' \leftrightarrow H'$, then $\widetilde{X}$ and $\widetilde{X}'$ are said to be *conjugate* if $H$ and $H'$ are conjugate, i.e., $H' = gHg^{-1}$ for some $g \in \mathrm{Gal}(Y/X)$.

**Theorem 3.10** *Let $Y/X$ be a Galois covering. Two intermediate coverings $Y/X$ are conjugate if and only if they are covering isomorphic.*

*Proof.* Suppose $\widetilde{X}$ and $\widetilde{X}'$ are conjugate. Let $H = \mathrm{Gal}(Y/\widetilde{X})$, then $\mathrm{Gal}(Y/\widetilde{X}') = g_0 H g_0^{-1}$ for some $g_0 \in G = \mathrm{Gal}(Y/X)$. The vertices of $\widetilde{X}$ are $\{(v, Hg) \mid v \in V_X, g \in G\}$ and the vertices of $\widetilde{X}'$ are $\{(v, H'g) \mid v \in V_X, g \in G\} = \{(v, H'g_0 g) \mid v \in V_X, g \in G\}$. We can let the covering isomorphism be $\sigma : (v, Hg) \mapsto (v, H'g_0 g)$ from $\widetilde{X}$ to $\widetilde{X}'$. To check this is well-defined, suppose $Hg_1 = Hg_2$; then $g_2 = hg_1$ for some $h \in H$ and so $H'g_0 g_2 = g_0 H h g_1 = g_0 H g_1 = H'g_0 g_1$. Further,

$$\pi_{\widetilde{X}'/X} \circ \sigma(v, Hg) = v = \pi_{\widetilde{X}/X}(v, Hg).$$

The other details also work out.

Conversely, suppose $\sigma : \widetilde{X} \to \widetilde{X}'$ is a covering isomorphism. Fix a vertex $v_0$ in $X$. Then consider $(v_0, 1)$ in $Y$ and its projection $(v_0, H)$ in $\widetilde{X}$. Then let $\widetilde{v}_0'$ be $\sigma(v_0, H)$. Since $\pi_{\widetilde{X}/X} = \pi_{\widetilde{X}'/X} \circ \sigma$, it follows that $\widetilde{v}_0'$ also lies above $v_0$ and so there exists $(v_0, g_0) \in Y$ such that $\pi_{Y/\widetilde{X}'}(v_0, g_0) = \widetilde{v}_0'$. We might suspect $\mathrm{Gal}(Y/\widetilde{X}') = g_0 H g_0^{-1}$, which works but we won't verify this here. □

**Theorem 3.11** *Suppose $\widetilde{X}$ is an intermediate covering of a Galois covering $Y/X$ with a corresponding subgroup $H \leq G = \mathrm{Gal}(Y/X)$. Then $\widetilde{X}/X$ is a Galois covering if and only if $H$ is normal in $G$. Further,* $\mathrm{Gal}(\widetilde{X}/X) \cong G/H$.

*Proof.* Let $H$ be normal in $G$. The vertices of $\widetilde{X}$ are $(v, Hr)$, $v \in V_x, r \in G$. The cosets $Hg$ act on $\widetilde{X}$ by sending $(v, Hr)$ to $(v, HgHr) = (v, Hgr)$. Clearly this action is a bijection on the vertices of $\widetilde{X}$. It also preserves edges: suppose there is an edge between $(v_1, Hr_1)$ and $(v_2, Hr_2)$;

[2] It is easily verified that if $\{l_i\}$ is a basis for $F$ over $L$ and $\{f_j\}$ is a basis for $K$ over $F$, then $\{l_i f_j\}$ is a basis for $K$ over $L$.

then by Theorem 3.8 there is an edge between $(v, h_1 r_1)$ and $(v, h_2 r_2)$ in $Y$ for some $h_1, h_2 \in H$. The action of a coset $Hg$ takes the vertices to $(v_1, Hgr_1)$ and $(v_2, Hgr_2)$. Now the action of $g$ takes $(v, h_1 r_1)$ and $(v, h_2 r_2)$ to $(v, gh_1 r_1)$ and $(v, gh_2 r_2)$ while preserving the edge between them; letting $h_i' = gh_i g^{-1} \in H \triangleleft G$, we see there is an edge between $(v, h_1' gr_1)$ and $(v, h_2' gr_2)$, implying there has to be an edge between $(v_1, Hgr_1)$ and $(v_2, Hgr_2)$.

For the converse, suppose $\widetilde{X}/X$ is Galois and let $\sigma$ be an automorphism in $\mathrm{Gal}(\widetilde{X}/X)$. Then since $\sigma$ can also be viewed as a covering isomorphism from $\widetilde{X}$ to $\widetilde{X}$, using Theorem 3.10 (and in particular its proof), we see that $g_0 H g_0^{-1} = H$ for some $g_0 \in G$, and as $\sigma$ runs through $\mathrm{Gal}(\widetilde{X}/X)$, $g_0$ runs through the right coset representatives of $H$. Thus $H$ is normal in $G$. $\square$

# 4 Artin $L$-Function

We are now approaching the analogue of the Artin $L$-function, which will lead to the graph-theoretic Riemann hypothesis. But, to begin with, we need to delve deeper into the connection between graph coverings and number fields. We first see how the Frobenius automorphism for a graph covering is defined, beginning with a short interlude on the basics of algebraic number theory. The interested reader might like to refer to [8] for an introduction to algebraic number theory requiring minimal algebraic background and [7, 6, 9] for more abstract approaches. On a related note, for simplicity here we will only consider finite field extensions $K/L$ with $L = \mathbb{Q}$, but all the theory generalizes to when even $L$ is a number field strictly above $\mathbb{Q}$.

## 4.1 Primes in Coverings

Recall that a number field is a finite field extension of $\mathbb{Q}$. Within a number field $K$, lives a subring $\mathcal{O}_K$ called the *ring of integers* of $K$ that plays the same role as the integers $\mathbb{Z}$ do for the rationals $\mathbb{Q}$. This is the reason for the name "number field": we can generalize much of the beautiful arithmetic of $\mathbb{Q}$ to number fields. The idea of generalization is key here, because, for instance, the usual Fundamental Theorem of Arithmetic (FTA) of $\mathbb{Z}$ usually fails miserably in number fields. The classic example is that in $\mathbb{Q}[\sqrt{-5}]$, 6 can be factored into irreducibles as both $2 \cdot 3$ and $(1 - \sqrt{-5})(1 + \sqrt{-5})$. This is fixed by instead considering the ideals of $\mathcal{O}_K$. Before going further, let us first define what is $\mathcal{O}_K$, for which we need a few definitions pertaining to integrality. *Rings for our purposes are commutative with unity.*

**Definition 4.1 (Integrality)** Let $A$ be a subring of a ring $B$. Then an element $b \in B$ is *integral* over $A$ if there exist $n \in \mathbb{Z}_{\geq 1}$ and $a_i \in A$ such that

$$b^n + a_{n-1} b^{n-1} + \cdots + a_0 = 0.$$

In other words there exists a monic $p(x) \in A[x]$ such that $p(b) = 0$. The *integral closure* of $A$

in $B$ is the set of elements in $B$ that are integral over $A$. Further, $A$ is *integrally closed* if the integral closure of $A$ in its field of fractions is again $A$.

It follows that $A$ is contained in its integral closure since an element $\alpha \in A$ is a root of the polynomial $x - \alpha$. Also, if you are familiar with the Rational Roots theorem, notice that it implies that $\mathbb{Z}$ is integrally closed. Lastly, while it is not obvious from the definition, using basic module theory it can be shown that the integral closure of a ring is yet another ring [1, pp. 21].

**Definition 4.2 (Ring of integers)** Let $K$ be a number field. The *ring of integers* $\mathcal{O}_K$ is the integral closure of $\mathbb{Z}$ in $K$.

Just like $\mathbb{Q}$ is the field of fractions of $\mathbb{Z}$, it is easy to show that $K$ is the field of fractions of $\mathcal{O}_K$. We also fully understand the structure of $\mathcal{O}_K$ when $K$ is a quadratic field $\mathbb{Q}(\sqrt{d})$ for some squarefree integer $d$. For instance, when $d = 2$, just as one would first guess, we have that $\mathcal{O}_K = \mathbb{Z}[\sqrt{2}]$, i.e., every element of the ring of integers of $\mathbb{Q}(\sqrt{2})$ is of the form $a + b\sqrt{2}$, for some $a, b \in \mathbb{Z}$. The situation is not as straightforward for all quadratic number fields; for instance, the ring of integers of $\mathbb{Q}[\sqrt{5}]$ is $\mathbb{Z}[\frac{1+\sqrt{5}}{2}]$ rather than $\mathbb{Z}[\sqrt{5}]$. In general, $\mathcal{O}_K$ is usually not generated by a single element over $\mathbb{Z}$ (other than 1) but we can always find a finite $\mathbb{Z}$-basis for $\mathcal{O}_K$, i.e., $\mathcal{O}_K$ is always a finitely generated $\mathbb{Z}$-module.

Now it turns out that $\mathcal{O}_K$ is a very special kind of ring called a *Dedekind domain*. It will be too long a digression to formally introduce Dedekind domains here and so we will take some of their fundamental properties for granted here; the beautiful theory of Dedekind domains can be found in most algebraic number theory texts and we especially recommend [6] for a first reading. The property we are most interested in is the following:

**Theorem 4.3 (FTA for Dedekind domains)** *Let $A$ be a Dedekind domain. Then every proper nonzero ideal $\mathfrak{a}$ of $A$ can be written as*

$$\mathfrak{a} = \mathfrak{p}_1^{e_1} \dots \mathfrak{p}_k^{e_k},$$

*where the $\mathfrak{p}_i$ are distinct prime ideals and $e_i > 0$ are integers. Furthermore, this expression is unique.*

This unique factorization of nonzero ideals in $\mathcal{O}_K$ helps us to answer one of the fundamental questions of algebraic number theory. We know that the ideal generated by a prime $p$ in $\mathbb{Z}$ is a prime ideal of $\mathbb{Z}$ and so it cannot be factored into two proper ideals of $\mathbb{Z}$ different from $p\mathbb{Z}$; but what about $p\mathcal{O}_K$, the ideal generated by $p$ in $\mathcal{O}_K$? For better or worse, $p\mathcal{O}_K$ is usually not prime. The next theorem explains the basic structure of the factorization of $p\mathcal{O}_K$.

**Theorem 4.4 ($e$-$f$-$g$ Theorem)** *Let $K$ be a number field of degree $n$. Let $p \in \mathbb{Z}$ be prime having the factorization*

$$p\mathcal{O}_K = \mathfrak{p}_1^{e_1} \dots \mathfrak{p}_g^{e_g}, \tag{1}$$

*with the $\mathfrak{p}_i$ distinct prime ideals and $e_i > 0$. Then*

- *for each* $1 \leq i \leq g$, $\operatorname{Nm} \mathfrak{p}_i := [\mathcal{O}_K : \mathfrak{p}_i] = p^{f_i}$ *for some* $f_i \in \mathbb{Z}_{>0}$, *and*
- $n = \sum_{i=1}^{g} e_i f_i$.

The prime ideals $\mathfrak{p}_i$ in the factorization of $p$ are said to *lie above* $p$, denoted $\mathfrak{p}_i \mid p$. Here $\operatorname{Nm} \mathfrak{p}_i$ is the *norm* of $\mathfrak{p}_i$ and we will see that projection map $\pi$ in a covering is sort of analogous to it. We also have the *norm* of an element $\alpha \in K$ which, when $K/\mathbb{Q}$ is a Galois extension, is defined as follows (we won't require a more general definition):

$$\operatorname{Nm} \alpha = \prod_{\sigma \in \operatorname{Gal}(K/\mathbb{Q})} \sigma(x). \tag{2}$$

For instance, in a quadratic field $\mathbb{Q}(\sqrt{d})$, we saw the Galois group consists of the trivial automorphism and the automorphism that sends $\sqrt{d} \mapsto -\sqrt{d}$. So the norm of an element $\alpha = a + b\sqrt{d}$, $a, b \in \mathbb{Q}$, is

$$\operatorname{Nm} \alpha = (a + b\sqrt{d})(a - b\sqrt{d}) = a^2 - b^2 d.$$

If $\alpha \in \mathcal{O}_K$, we have the useful fact that $\operatorname{Nm} \alpha \in \mathbb{Z}$. This is easy to see when $K/\mathbb{Q}$ is Galois: observe that for any $\tau \in \operatorname{Gal}(K/\mathbb{Q})$, applying $\tau$ to the norm of $\alpha \in \mathcal{O}_K$ corresponds to simply permuting the $\sigma$'s in (2), so that $\tau \operatorname{Nm} \alpha$ is equal to $\operatorname{Nm} \alpha$, implying that $\operatorname{Nm} \alpha \in \mathbb{Q}$. Since $\alpha \in \mathcal{O}_K$, each of the conjugates $\sigma(\alpha)$ also belong to $\mathcal{O}_K$ and therefore $\operatorname{Nm} \alpha \in \mathbb{Q} \cap \mathcal{O}_K = \mathbb{Z}$ (Rational Roots theorem).

Let us consider some examples of Theorem 4.4. In $K = \mathbb{Q}(\sqrt{3})$, $5\mathcal{O}_K = (5)$.[3] On the other hand in $K = \mathbb{Q}(\sqrt{5})$, $5\mathcal{O}_K = (\sqrt{5})^2$. Lastly, in $K = \mathbb{Q}(\sqrt[3]{2})$, $5\mathcal{O}_K = (5, \sqrt[3]{2} + 2)(5, \sqrt[3]{2}^2 + 3\sqrt[3]{2} + 4)$. These prime factorizations are not obvious and follow from a standard result of algebraic number theory (see [6, pp. 61] or [11, pp. 102]). Observe that in the first example, $e = 1, f = 2, g = 1$, while in the second one $e = 2, f = 1, g = 1$, and in the third one $e_i = 1, f_i = 1, g = 2$. The first example will be most relevant for us since the number field $K$ involved is Galois over $\mathbb{Q}$ and the prime 5 is *unramified* in $K$: the exponent $e$ is not greater than 1 for any of the primes (just one here) in the factorization.

We now turn to defining primes in graph coverings.

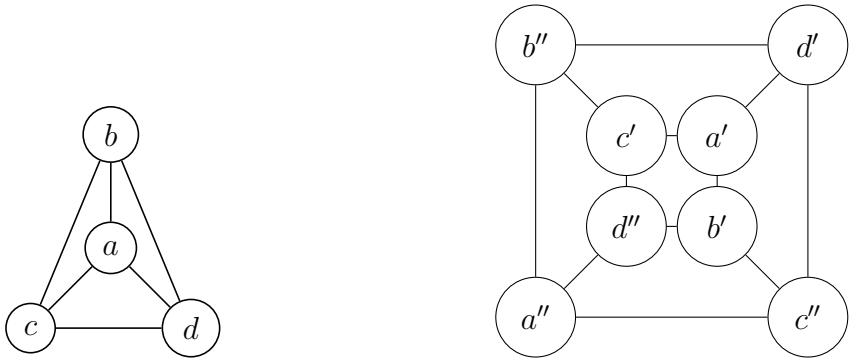
**Definition 4.5 (Primitive/Prime path)** Let $C = a_1 \dots a_s$ (the $a_i$ being edges) be a closed path with no backtrack ($a_{j+1} \neq a_j^{-1}$ for any $1 \leq j < s$) and no tail ($a_s \neq a_1^{-1}$). Then the closed path $C$ is called a *primitive or prime path* if $C \neq D^f$ for any path $D$ and integer $f > 1$, i.e., $C$ is not a repeated cycle. If the beginning and end vertex of a primitive path $C$ is $v$, then we say $C$ is *based at* $v$.

We will consider two paths with opposite directions to be distinct from each other. The condition that $C \neq D^f$ is our notion of "primeness". Now, if we have a primitive path $C = a_1 \dots a_s$, then we can obtain a new primitive path $C' = a_2 \dots a_s a_1$ by simply changing which vertex we

[3] By $(a_1, a_2, \dots, a_n)$ we mean the ideal generated by $a_1, a_2, \dots, a_n$ in the specified ring.

view as the initial vertex of the path. But morally we should not have to think $C'$ as being different from $C$, just like we don't distinguish between prime ideals that are generated by associates.[4] Therefore, we create an equivalence relation on the set of primitive paths that "forgets" the initial vertex of a primitive path.

**Definition 4.6 (Prime)** A *prime* in a graph $X$ is an equivalence class $[C]$, with $C = a_1 \dots a_s$ a primitive path, under the relation $C' \sim C$ if $C' = a_{\pi_s^k(1)} \dots a_{\pi_s^k(s)}$ where $k \in \mathbb{Z}$ and $\pi_s$ is the permutation $(1\,2 \cdots s)$. In other words, a prime is a set of primitive paths $\{a_1 \dots a_s, a_2 \dots a_s a_1, \dots, a_s a_1 \dots a_{s-1}\}$.




(a) The tetrahedron $K_4$ (b) The cube as a covering of $K_4$

Figure 4.1

For instance, in $K_4$ (Figure 4.1) some primes, specified by vertices, are $[\langle b, c, d, b\rangle]$, $[\langle b, a, c, d, b\rangle]$, and $[\langle b, a, d, b\rangle]$. However, $[\langle b, a, b, d, c, b\rangle]$ is not prime since it has backtrack and $[\langle b, a, d, b, a, d, b\rangle]$ is not prime since it is the same as $[\langle b, a, d, b\rangle]^2$. Generally, the number of primes in a graph is infinite. In $K_4$, one infinite family of primes is $[\langle a, b\rangle \langle b, c, d, b\rangle^n \langle b, a\rangle]$ for $n \in \mathbb{Z}_{\geq 1}$. One case where we do have a finite number of primes is the cycle graph $C_n$, $n \in \mathbb{Z}_{\geq 3}$; it has exactly two primes (because we consider the directions too).

Unfortunately, notice that there is no natural way to define a well-defined product of two primes, and so we have no hope for finding a unique prime factorization for coverings. However, let us not be disheartened just yet! We will see that an analog of the $e$-$f$-$g$ Theorem (or more accurately an $f$-$g$ Theorem) holds for coverings. An immediate problem we have with absence of a result like Theorem 4.3 for a covering $Y/X$ is how to define when a prime $[D]$ of $Y$ lies above a prime $[C]$ of $X$? We use the projection map $\pi_{Y/X}$. Indeed, if $[D]$ is a prime in $Y$, then the reader should convince themselves that $\pi_{Y/X}(D)$ will not have backtrack or tail. But there may exist a prime $C$ and positive integer $f$ such that $\pi_{Y/X}(D) = C^f$ (if $\pi_{Y/X}(D)$ is primitive, then $f = 1$). This situation is described by saying $[D]$ *lies above* $[C]$, or $[D] \mid [C]$, and $f$ is called the *residual degree* of $D$, denoted $f_{Y/X}(D)$. In a Galois covering $Y/X$, observe that if $[D]$ and $[D]'$ lie over $[C]$ with residual degrees $f$ and $f'$, then $f = f'$; informally, we can apply some

[4]Recall two elements $a$ and $b$ of a ring are called *associates* if $a = bu$ for some unit $u$.

$\sigma \in \mathrm{Gal}(Y/X)$ so that $\sigma \circ D$ is based at the same vertex as $D$ and so the first edge of $\sigma \circ D$ is the same as that of $D'$, and continuing in this way, they must have the same length and thus have the same residual degree; we will see that the corresponding statement holds for Galois number fields too.

Consider the cube and $K_4$ in Figure 4.1. The prime path $D = \langle c', d'', b', c'', d', b'', c' \rangle$ in $Y$ lies above the prime path $C = \langle c, d, b, c \rangle$ in $X$, with $f_{Y/X}(D) = 2$. Another example is that $D_1 = \langle c', a', d', b'', c' \rangle$ lies above $C = \langle c, a, d, b, c \rangle$; also, $D_2 = \langle c'', a'', d'', b', c'' \rangle$ is another prime path inequivalent to $D_1$ over $C$. In both these cases, the residual degree is 1 and we can see that there is no other prime lying over $[C]$, so that $2 \cdot 1 = 2$ is equal to the degree of the covering, an example of the $f$-$g$ Theorem in action! The proof of the $f$-$g$ Theorem will follow quite easily from the theory of the Frobenius automorphism, which we now develop.

## 4.2 Frobenius Automorphism

Suppose we a have a number field $K/\mathbb{Q}$. Let $\mathfrak{p}$ be a prime ideal of $\mathcal{O}_K$ lying above a rational prime $p \in \mathbb{Z}$. One of the defining axioms of a Dedekind domain is that every nonzero prime ideal is maximal. So the integral domain $F_\mathfrak{p} = \mathcal{O}_K/\mathfrak{p}$ is in fact a field and has $F_p = \mathbb{Z}/p\mathbb{Z}$ as a subfield. We now argue that $F_\mathfrak{p}$ is a Galois extension of $F_p$, i.e., $|\mathrm{Aut}(F_\mathfrak{p}/F_p)| = [F_\mathfrak{p} : F_p] = f_{K/\mathbb{Q}}(\mathfrak{p})$ by showing that $A := \mathrm{Aut}(F_\mathfrak{p}/F_p)$ has an element of order $f := f_{K/\mathbb{Q}}(\mathfrak{p})$. Here we are taking for granted the general fact that the number of $L$-automorphisms of a finite (separable) field extension $K/L$ cannot exceed the degree of the extension (see [3, pp. 240-241]).

First note that the mapping $\sigma : x \to x^p$ on $F_\mathfrak{p}$ is a member of $A$ since for any $a \in F_p$, we have $a^p = a$ (Fermat's Little theorem) and for any $x, y \in F_\mathfrak{p}$

$$(xy)^p = x^p y^p \text{ and } (x+y)^p = x^p + y^p,$$

where the second equality holds because $F_\mathfrak{p}$ has characteristic $p$. It is also easy to show that $\sigma$ must be injective and thus bijective. Let $n$ be the order of $\sigma$ in the group $A$, so that $\sigma^n(x) = x^{p^n} = x$ for all $x \in F_\mathfrak{p}$. Further, since $|F_\mathfrak{p}| = p^f$, and $F_\mathfrak{p}^\times$ is cyclic,[5] there exists $\alpha \in F_\mathfrak{p}$ having multiplicative order $p^f - 1$. So we have $\sigma^n(\alpha) = \alpha^{p^n} = \alpha$, implying that $p^f - 1 \mid p^n - 1$. But $p^f - 1 \mid p^n - 1$ is true only if $f \mid n$; therefore $n \geq f$. Lastly, simply because $F_\mathfrak{p}^\times$ is a group of order $p^f - 1$, $\sigma^f(x) = x^{p^f} = x$ for any $x \in F_\mathfrak{p}$; thus the order of $\sigma$ is $f$. Therefore, since $A$ has order at most $f$, it is cyclic of order $f$ with generator $\sigma$, and so $F_\mathfrak{p}/F_p$ is a Galois extension (Theorem 3.3). The generator $\sigma$ is called the *Frobenius element* $\mathrm{Frob}_\mathfrak{p}$ of $\mathrm{Gal}(F_\mathfrak{p}/F_p) = \mathrm{Aut}(F_\mathfrak{p}/F_p)$.

Now also assume $K/\mathbb{Q}$ is a Galois extension with Galois group $G$. For any $\sigma \in G$, it is a quick verification that $\sigma(\mathfrak{p})$ is also a prime ideal, and so $G$ acts on the set of prime ideals of $\mathcal{O}_K$. Let $Z_\mathfrak{p} = \{\sigma \in \mathrm{Gal}(K/\mathbb{Q}) \mid \sigma(\mathfrak{p}) = \mathfrak{p}\}$ denote the stabilizer of this action; $Z_\mathfrak{p}$ is called the *decomposition group of* $\mathfrak{p}$. Notice that we have a natural homomorphism $\varphi : Z_\mathfrak{p} \to \mathrm{Gal}(F_\mathfrak{p}/F_p)$

[5] Recall that the group of units of a finite field is cyclic.

$-$ for each $\sigma \in Z_{\mathfrak{p}}$, $\varphi(\sigma)$ sends $\alpha \bmod \mathfrak{p}$ to $\sigma(\alpha) \bmod \mathfrak{p}$. With a little work, it can be shown that when $\mathfrak{p}$ is unramified over $p$ then $\varphi$ is an isomorphism (see [11, pp. 104-106]). A consequence is that when $\mathfrak{p}$ is unramified over $p$, we can lift the Frobenius element $\mathrm{Frob}_{\mathfrak{p}}$ to $Z_{\mathfrak{p}}$, and so $Z_{\mathfrak{p}}$ is cyclic with generator $\mathrm{Frob}_{\mathfrak{p}}$.

We can also argue that the Galois group $G$ acts transitively on all prime ideals that lie above $p$. Suppose $\mathfrak{q}$ is a prime ideal different than $\mathfrak{p}$ lying above $p$ and $\tau(\mathfrak{p}) \neq \mathfrak{q}$ for any $\tau \in G$. Then by the Chinese Remainder theorem (since nonzero prime ideals in a Dedekind domain are maximal),[6] we can find an element $\alpha \in \mathfrak{q}$ not belonging to any of the prime ideals $\tau(\mathfrak{p})$, for any $\tau \in G$. So,

$$a := \mathrm{Nm}_{L/\mathbb{Q}}(\alpha) = \prod_{\tau \in G} \tau(\alpha) \in \mathfrak{q} \cap \mathbb{Z} = p\mathbb{Z},$$

and since $p\mathbb{Z} \subseteq \mathfrak{p}$, we infer that $a \in \mathfrak{p}$. Since $\mathfrak{p}$ is prime, it follows $\tau(\alpha) \in \mathfrak{p}$ for some $\tau \in G$, contradicting $\alpha \notin \tau^{-1}(\mathfrak{p})$. Therefore $G$ acts transitively on the prime ideals lying above $p$. An implication of transitivity is that, if $\mathfrak{q}$ and $\mathfrak{p}$ are two prime ideals above $p$ with $\mathfrak{q} = \tau(\mathfrak{p})$, then $\mathfrak{q}$ and $\mathfrak{p}$ will have conjugate decomposition groups $Z_{\mathfrak{q}} = \tau Z_{\mathfrak{p}} \tau^{-1}$; as a consequence $\mathrm{Frob}_{\mathfrak{q}} = \tau \,\mathrm{Frob}_{\mathfrak{p}}\, \tau^{-1}$.

We have yet another application of transitivity. Using Theorem 4.3, let

$$p\mathcal{O}_K = \mathfrak{p}_1^{e_1} \dots \mathfrak{p}_g^{e_g},$$

since $\mathfrak{p}_i = \tau_i(\mathfrak{p}_1)$ for some $\tau_i \in G$, by applying $\tau_i$ to the factorization, we see that $e_i = e_1$ and by a similar argument $f_i = f_1$. So by the $e$-$f$-$g$ theorem, $efg = [K : \mathbb{Q}]$. Therefore Galois extensions are quite special in this regard and the analogous phenomena happens for graph coverings, already visible in the example with the cube and tetrahedron above.

Back to coverings, the Frobenius automorphism is defined in a very constructive manner but helps us prove all of the analogs of the properties of number fields just discussed.

**Definition 4.7 (Frobenius automorphism)** Let $Y/X$ be a Galois covering. Let $C$ be a primitive path in $X$ based at the vertex $a$. Let $D$ be a primitive path in $Y$ over $C$, and let $D$ be based at vertex $(a, g)$. Suppose the unique lift of $C$ to $Y$ that starts at $(a, g)$ terminates at $(a, h)$. Then the *Frobenius automorphism* associated to $D$ is

$$\mathrm{Frob}_D = hg^{-1} \in \mathrm{Gal}(Y/X).$$

Notice that we have only defined a Frobenius automorphism associated with a primitive path rather than a prime, but in Theorem 4.8 we will see that this definition gives us a well-defined Frobenius automorphism for a prime as well.

Consider $K_4$ and the cube (Figure 4.1), and denote the nonidentity Galois automorphism of the cube by $\tau$. Let $D = \langle c', d'', b'', c'', d', b', c' \rangle$ in $Y$ which lies above the prime path $C = \langle c, d, b, c \rangle$.

[6] Recall that the CRT for a ring $R$ states that if $\mathfrak{i}_1, \mathfrak{i}_2, \dots, \mathfrak{i}_k$ are pairwise relatively prime ideals, then $\mathfrak{i}_1 \cap \mathfrak{i}_2 \cap \dots \cap \mathfrak{i}_k = \mathfrak{i}_1 \mathfrak{i}_2 \dots \mathfrak{i}_k$ and so by the Isomorphism theorem $R/(\mathfrak{i}_1 \mathfrak{i}_2 \dots \mathfrak{i}_k) \cong R/\mathfrak{i}_1 \times R/\mathfrak{i}_2 \times \dots \times R/\mathfrak{i}_k$.

Then, since $c' \equiv (c, 1)$ and $c'' \equiv (c, \tau)$, we see that $\mathrm{Frob}_D = \tau \cdot 1^{-1} = \tau$. If we instead consider $D' = \langle c'', d', b', c', d'', b'', c'' \rangle$ which also is in $[D]$, we get $\mathrm{Frob}_{D'} = 1 \cdot \tau^{-1} = \tau = \mathrm{Frob}_D$.

The *decomposition group* $Z_D$ of a prime $D$ in a Galois covering $Y/X$ is defined almost exactly as for number fields:

$$Z_D = \{\sigma \in \mathrm{Gal}(Y/X) \mid [\sigma \circ D] = [D]\}.$$

In this case, it is easily verified that this definition gives us a well-defined group $Z_D$ associated to a prime.

Continuing with the example above, we see that $Z_D = \mathrm{Gal}(Y/X)$ since applying $\tau$ (besides the identity automorphism) to $D$ gives us $D'$, which belongs to $[D]$; similarly $Z_{D'} = \mathrm{Gal}(Y/X)$. Clearly the decomposition group need not be the whole Galois group. For instance, if $E = \langle a', b', c', d'', a' \rangle$ , then $Z_E$ is just the trivial subgroup since $\tau(E) = \langle a'', b'', c'', d', a'' \rangle \notin [E]$. This last example also illustrates that just like for a Galois number field, the Galois group of a Galois covering acts transitively on the primes lying above the same prime; in fact, this follows directly from the fact that the Galois group acts transitively on each fiber (Proposition 3.4).

We now prove the properties of the Frobenius automorphism, giving us an $f$-$g$ theorem for coverings, which we can with some imagination interpret as an $e$-$f$-$g$ theorem because our coverings are unramified and so $e$ is always 1.

**Theorem 4.8** *Let $Y/X$ be a $d$-sheeted Galois graph covering with Galois group $G$ and let $[D]$ be a prime in $Y$. Then*

1. *If $D' = \sigma \circ D$ for some $\sigma \in G$, then*

$$\mathrm{Frob}_{D'} = \sigma \,\mathrm{Frob}_D\, \sigma^{-1}.$$

2. *For all $D' \in [D]$, $\mathrm{Frob}_{D'} = \mathrm{Frob}_D$. Thus $\mathrm{Frob}_{Y/X}([D])$ is well-defined.*
3. *The decomposition group $Z_D$ is cyclic of order $f = f_{Y/X}(D)$ and is generated by $\mathrm{Frob}_D$.*
4. *If $g$ is the number of primes in $X$ over a prime $[C]$, then $fg = d$, where $f$ is the common residual degree of primes over $f$.*

*Proof.*

1. Let $D$ be based at $(a, g_0)$, so that $D'$ is based at $(a, \sigma g_0)$, and let $C$ lie below $D$. Then suppose the lift $\widetilde{C}$ of $C$ starting at $(a, g_0)$ ends at $(a, g_1)$. So $\mathrm{Frob}_D = g_1 g_0^{-1}$. Since $Y/X$ is Galois, the lift $\widetilde{C}'$ of $C$ starting at $(a, \sigma g_0)$ is the same as $\sigma \circ \widetilde{C}$, so that $\widetilde{C}'$ ends at $(a, \sigma g_1)$. Thus, $\mathrm{Frob}_{D'} = (\sigma g_1)(\sigma g_0)^{-1} = \sigma(g_1 g_0^{-1})\sigma^{-1} = \sigma \,\mathrm{Frob}_D\, \sigma^{-1}$.
2. To prove this cleanly, it's useful to introduce a *normalized Frobenius automorphism* $\lambda$. For a path $p$ in $X$, suppose the lift of $p$ starting on sheet 1 ends on sheet $g$; let $\lambda(p) = g$. Note that $\lambda$ is multiplicative: $\lambda(p_1 p_2) = \lambda(p_1)\lambda(p_2)$.

With same notation as the previous part, suppose $D' \in [D]$ and is based at $(b, h_0)$. Then $b$ is a vertex of $C$, and splits $C$ into paths: $C = p_1 p_2$, where $p_1$ ends at $b$ and $p_2$ begins at $b$. So $D'$ is a prime above $C' = p_1 p_2$. Suppose the lift $\widetilde{C'}$ of $C'$ starting at $(b, h_0)$ ends at $(b, h_1)$. We have to show $h_1 h_0^{-1} = g_1 g_0^{-1}$. Since $D$ lies above $C^f$, it can be decomposed into $f$ paths, each lying above $C$; let $(b, h_0)$ occur in the $r$-th component of $D$. Let $\widetilde{U}$ be a path from $(a, 1)$ to $(a, g_0)$ and $U$ its projection to $X$. Then, we have

$$g_0 = \lambda(U), g_1 = \lambda(UC), h_0 = \lambda(UC^{r-1}p_1), \text{ and } h_1 = \lambda(UC^r p_1).$$

Thus

$$g_1 g_0^{-1} = \lambda(UC)\lambda(U)^{-1} = \lambda(U)\lambda(C)\lambda(U)^{-1},$$

and

$$h_1 h_0^{-1} = \lambda(UC^r p_1)\lambda(UC^{r-1}p_1)^{-1} = \lambda(U)\lambda(C)\lambda(U)^{-1}.$$

Therefore $g_1 g_0^{-1} = h_1 h_0^{-1}$.

3. Continuing with the same notation, we have

$$\mathrm{Frob}_D^j = (g_1 g_0^{-1})^j = \lambda(U)\lambda(C)^j\lambda(U)^{-1}.$$

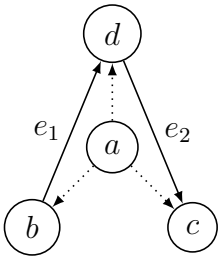
Now, $\lambda(C)^j = 1$ implies that $C^j$ lifts to a closed path in $Y$, and since the residual degrees of primes over $C$ are the same, it must be that $f \mid j$, and so $f$ is the order of $\mathrm{Frob}_D$. Since $\sigma \circ D \in [D]$ if and only if $\sigma \circ D$ is a cyclic permutation of $D$, and since $G$ acts transitively on fibers, $|Z_D| = f_{Y/X}(D)$. Since $Z_D$ has order $f$ and $\mathrm{Frob}_D \in Z_D$ also has order $f$, it follows $Z_D$ is cyclic with generator $\mathrm{Frob}_D$. This fact combined with part 1, implies that primes in $Y$ lying above the same prime in $X$ have conjugate decomposition groups.

4. Since $G$ acts transitively on the $g$ primes lying above the same prime and the size of the decomposition group (otherwise known as the stabilizer) has size $f$, by the orbit-stabilizer theorem we have $g = |G|/f = d/f$.

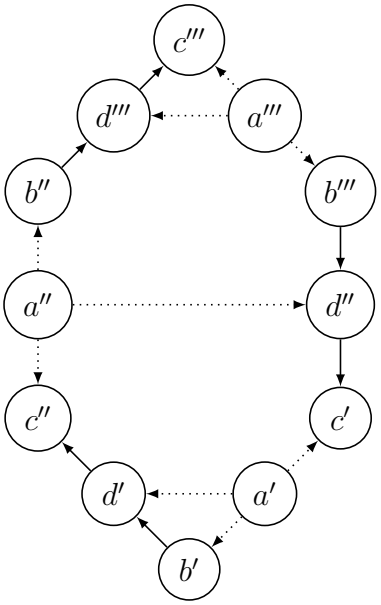
□

The Frobenius automorphism, besides being instrumental in helping us define the Artin-Ihara $L$-function (as we will soon see), also helps us construct special kinds of Galois coverings. Here we illustrate the construction with an example, but it readily generalizes.

We start with $X = K_4 - e$ (i.e., $K_4$ with one edge deleted) and a cubic covering $Y_3$ in Figure 4.2. The dotted edges in $X$ together represent a spanning tree. Observe that $Y_3$ is not Galois over $X$ (for instance, consider the fibers of $a$ and $d$). We will now minimally "extend" $Y_3$ so that it becomes Galois over $X$. More precisely, we will find a covering $Y_n$ of $X$ such that $Y_3$ is an intermediate covering of $Y_n/X$ and there is no Galois covering of $X$ strictly intermediate to $Y_n/Y_3$. Since $Y_3$ is cubic and $Y_n/Y_3$ is at least quadratic, $Y_n$ will be at least 6-sheeted over $X$, i.e., $n \geq 6$. We will see that $n = 6$ suffices. The reader familiar with Galois theory will recognize that our characterization of $Y_n$ is exactly analogous to the notion of a Galois closure.




(a) $X = K_4 - e$




(b) $Y_3$, a cubic non-Galois covering of $X$

Figure 4.2

First let us label our sheets of $Y_3$ so that $a'$ belongs to sheet 1, $a'''$ belongs to sheet 3, and so on. We consider how edges of $X$ not included in its spanning tree lift to $Y_3$. The edge $e_1 = \langle b, d\rangle$ lifts to $\langle b', d'\rangle, \langle b'', d'''\rangle$, and $\langle b''', d''\rangle$. So, we see that, in cycle form, $(1)(2\,3)$ represents how $e_1$ lifts to $Y_3$. Similarly, $(1\,2)(3)$ represents how $e_2$ lifts to $Y_3$. The elements $\{(2\,3), (1\,2)\}$ viewed as elements of $S_3$, generate $S_3$. It can be show that this implies $S_3$ is the Galois group of $Y_n/X$. Since $|S_3| = 6$, we have that $n = 6$.

We can recover $Y_6$ using the information that its Galois group is $S_3$ and that $Y_3$ is an intermediate covering. We begin by making six copies of the spanning tree of $X$, so that it remains to only lift $e_1$ and $e_2$. It can be shown that the permutations $(2\,3)$ and $(1\,2)$ are in fact $\lambda(e_1)$ and $\lambda(e_2)$ respectively, where $\lambda$ is the normalized Frobenius automorphism for $Y_6/X$ (from the proof of Theorem 4.8). So the lift of $e_1$ to $Y_6$ starting at on sheet $(1)$ ends on sheet $(2\,3)$, i.e., there is an edge between $(b, (1))$ and $(d, (2\,3))$. What about the lift of $e_1$ starting at some other sheet labelled by $\sigma \in S_6$? Since $Y_6$ is to be Galois over $X$, the lift of $e_1$ starting at $(b, \sigma) = \sigma((b, (1)))$ must terminate at $\sigma((d, (2\,3))) = (d, \sigma \circ (2\,3))$. Thus to lift $e_1$ to $Y_6$, we add the following edges to the six copies of the spanning tree of $X$:

$$(b, (1)) \to (d, (2\,3)), (b, (2\,3)) \to (d, (1)), (b, (1\,3)) \to (d, (1\,3\,2)),$$
$$(b, (1\,3\,2)) \to (d, (1\,3)), (b, (1\,2)) \to (d, (1\,2\,3)), (b, (1\,2\,3)) \to (d, (1\,2)).$$

Similarly, to lift $e_2$ we add the following edges:

$$(d, (1)) \to (c, (1\,2)), (d, (1\,2)) \to (c, (1)), (d, (1\,3)) \to (c, (1\,2\,3)),$$

$$(d, (1\,2\,3)) \to (c, (1\,3)), (d, (2\,3)) \to (c, (1\,3\,2)), (d, (1\,3\,2)) \to (c, (2\,3)).$$

All in all, if we make the following identifications:

$$v^1 = (v, (1)), v^2 = (v, (1\,3)), v^3 = (v, (1\,3\,2)),$$

$$v^4 = (v, (2\,3)), v^5 = (v, (1\,2\,3)), v^6 = (v, (1\,2)),$$

then we get $Y_6$ in Figure 4.3.

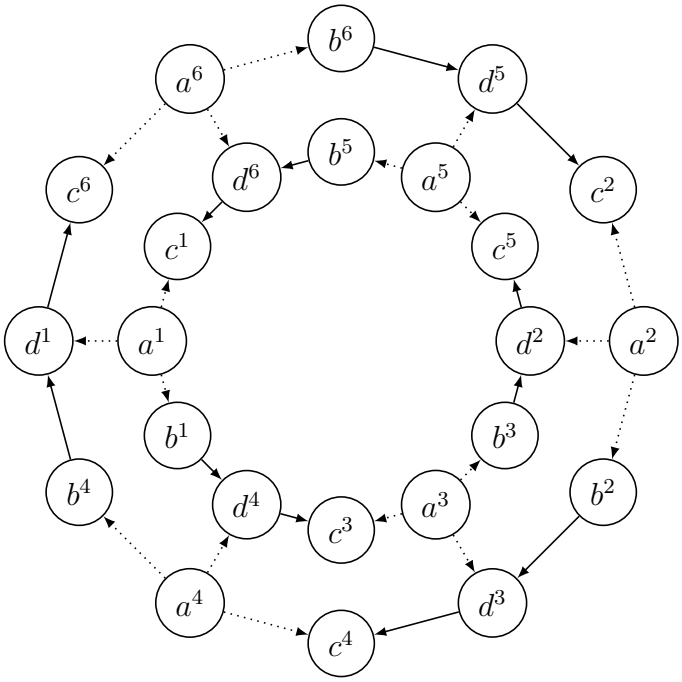



Figure 4.3: $Y_6$, a 6-sheeted Galois covering of $K_4 - e$.

Before moving on, let us take this opportunity to apply some of our Galois theory for coverings. For instance, what is the subgroup $H_3$ of $S_3$ that corresponds to the intermediate covering $Y_3$ in $Y_6/X$? From the proof of part 2 in Theorem 3.8, we see that $h \in H_3$ if and only if $\pi_{Y_6/Y_3}(a, h) = \pi_{Y_6/Y_3}(a, (1))$. Since we have not specified a projection map from $Y_6$ to $Y_3$, we will not have a well-defined subgroup $H_3$ corresponding to $Y_3$. However, for the time being suppose that $a^1$ projects to $a'$, so that $d^1$ projects to $d'$. Then since $b^4$ is adjacent to $d^1$, and $b'$ is the only vertex in the fiber of $b$ adjacent to $d'$, we conclude that $a^4$ must also project to $a'$, so that $H_3 = \{(1), (2\,3)\}$ in this case. Reasoning similarly, we find that if instead $a^1$ projects to $a''$ then $H_3' = \{(1), (1\,2)\}$ and if it projects to $a'''$ then $H_3'' = \{(1), (1\,3)\}$. Indeed, each of three projection maps give us three coverings $Y_6/Y_3$ which are conjugate to each other (Definition 3.9), since $H_3' = (1\,3\,2)H_3(1\,3\,2)^{-1}$ and $H_3'' = (1\,2\,3)H_3(1\,2\,3)^{-1}$. The fact that $Y_3/X$ is non-Galois is reflected in the fact that $H_3$ is not normal in $S_3$ (Theorem 3.11). Next, let us produce an intermediate covering of $Y_6/X$ that is also Galois over $X$. We use the subgroup

$H_2 = \{(1), (1\,2\,3), (1\,3\,2)\}$ which, being a union of two conjugacy classes, is normal in $S_3$. Since $[S_3 : H_2] = 2$, we make 2 copies of the spanning tree of $X$; also, let us denote the desired covering by $Y_2$. Then we add edges according to the proof of part 1 in Theorem 3.8. So, for instance since there is an edge between $b^1 = (b, (1))$ and $d^4 = (d, (2\,3))$, there has to be an edge between $(b, H_2)$ and $(d, H_2(2\,3))$ in $Y_2$. Repeating this process, we add four edges to the spanning trees to get the covering in Figure 4.4, which should not be surprising!

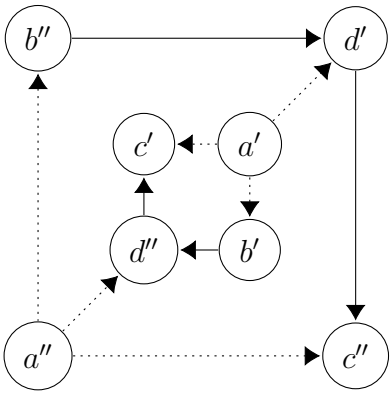



Figure 4.4: The cube without 2 edges as a Galois covering of $K_4 - e$.

## 4.3 Artin-Ihara $L$-function

The Artin $L$-function immensely generalizes the Riemann zeta function and helps us better understand the properties of the Dedekind zeta function. But there are deeper reasons for why the Artin $L$-function is important. For example, the Artin $L$-function plays an important role in the proof of the Chebotarev Density Theorem (see [13]), which in its simplest form roughly tells us about the density of primes that split in a finite Galois extension of number fields; this also has a graph covering analogue (see [12, Ch. 22]). Here, however, we will content ourselves with the definition of the Artin $L$-function and its graph theoretic analogue, along with some of its basic properties. The reader might like to refer to [10] for more information about the Artin $L$-function.

To define the Artin $L$-function, we need the definition of a representation. Later, we will also be appealing to basic theorems of representation theory, proofs of which can be found in any good reference on representation theory such as [4].

Let $V$ be a finite dimensional vector space over $\mathbb{C}$. A *representation* $(V, \rho)$ of a finite group $G$ is a group homomorphism $\rho : G \to \mathrm{GL}(V)$.[7] The *degree* $d_\rho$ of a representation $\rho$ is the dimension of $V$. A *subrepresentation* of a representation $(\rho, V)$ is a representation $(W, \rho\mid_W)$, where $W \subseteq V$ is a subspace which is $\rho$-invariant.

[7]Recall that $\mathrm{GL}(V)$ is the group of bijective linear maps from $V$ to $V$.

**Definition 4.9 (Artin $L$-function)** Let $K/\mathbb{Q}$ be a Galois number field and let $(V, \rho)$ be a representation of $\mathrm{Gal}(K/\mathbb{Q})$. The *Artin L-function* $L(s, \rho, K/\mathbb{Q})$ is then

$$L(s, \rho, K/\mathbb{Q}) = \prod_p \det[I - \rho(\mathrm{Frob}_{\mathfrak{p}})p^{-s}]^{-1}, \tag{3}$$

where the product runs over all primes $p \in \mathbb{Z}$ which are unramified in $K$ (i.e., $e = 1$) and $\mathfrak{p}$ is any prime ideal lying above $p$.

The product in (3) is well-defined since if $\mathfrak{q}$ is another prime lying above $p$, we know that $\mathrm{Frob}_{\mathfrak{q}}$ and $\mathrm{Frob}_{\mathfrak{p}}$ are conjugates, so that the characteristic polynomial $f_p(x) = \det[Ix - \rho(\mathrm{Frob}_{\mathfrak{p}})p^{-s}]$ remains unchanged (the characteristic polynomial is basis-invariant), and therefore so do the terms $f_p(1)$ in the product.

If we take $\rho = 1$ in $L(s, \rho, K/\mathbb{Q})$, the $\rho(\mathrm{Frob}_{\mathfrak{p}})$ term effectively has no contribution and thus the definition becomes independent of the field $K$, giving us the familiar Euler product for the Riemann zeta function. More generally, if we take $\rho = 1$ in $L(s, \rho, K/L)$, where $K/L$ is a Galois extension of number fields, we get the *Dedekind zeta function*, a generalization of the Riemann zeta function for number fields.

The analogue for coverings is defined almost the same way. Let $Y/X$ be a Galois covering with a representation $(V, \rho)$ of $\mathrm{Gal}(V, \rho)$. Let $\nu(C)$ denote the length of a path $C$. The *Artin-Ihara L-function* $L(s, \rho, Y/X)$ is defined as

$$L(s, \rho, Y/X) = \prod_{[C]} \det[I - \rho(\mathrm{Frob}_D)s^{\nu(C)}]^{-1}, \tag{4}$$

where the product runs over all primes $[C]$ of $X$ and $D$ is any prime path lying above $C$. Comparing (3) and (4), the difference between the terms $p^{-s}$ and $s^{\nu(C)}$ is conspicuous. Well, to get a function that is not a mere formal sum and has analytic properties, we have $\nu(C)$ rather than just $C$. So why not have $\nu(C)^{-s}$? A complete answer to this requires looking at the details proofs of properties we desire $L(s, \rho, Y/X)$ to have (e.g., see [12, Theorem 18.8, Ch. 18]), but here is the underlying idea. Every $n \in \mathbb{Z}$ is of the form $\prod_p p^{e_p}$, for primes $p \in \mathbb{Z}$ and some $e_p \in \mathbb{Z}_{\geq 0}$. On the other hand, the length of a closed path $T$ (with no backtrack and tail) is not necessarily of the form $\nu(T) = \nu(C)^j$ for some prime $[C]$, $j \in \mathbb{Z}_{\geq 0}$, but is instead of the form $\nu(T) = j \cdot \nu(C)$. In other words, the difference is a result of the fact that the norm map $\mathrm{Nm}_{K/\mathbb{Q}}$ is multiplicative while the length function $\nu$ is additive.

Before we consider some basic properties of $L(s, \rho, Y/X)$, we need a couple of ways to create new representations.

Given two representations $(V, \rho)$ and $(W, \sigma)$, we can get a new representation by defining their *direct sum* $(V \oplus W, \rho \oplus \sigma)$ – the vector space $V \oplus W$ is the usual direct sum and $\rho \oplus \sigma \in \mathrm{GL}(V \oplus W)$ is such that $\rho \oplus \sigma((v, w)) = (\rho(v), \sigma(w))$.

Next, given a representation $(W, \rho)$ of a subgroup $H$ in a group $G$, we can *induce* a represen-

tation $(V, \operatorname{Ind}_H^G \rho)$ of $G$, by letting

$$V = \{\phi : G \to W \mid \phi(hg) = \rho(h)\phi(g), \text{ for all } h \in H, g \in G\},$$

and

$$\operatorname{Ind}_H^G(g)(f) : x \mapsto f(xg),$$

for all $x, g \in G$.

In the following, we only outline the proofs of the first two parts since proving the third part is substantially harder (see [12, Ch. 19]). The corresponding properties and proofs hold for the Artin $L$-function $L(s, \rho, K/\mathbb{Q})$ too.

**Theorem 4.10** *Let $Y/X$ be a Galois covering with group $G$.*

1. *If $\rho_1$ and $\rho_2$ are representations of $G$, then*

$$L(s, \rho_1 \oplus \rho_2, Y/X) = L(s, \rho_1, Y/X)L(s, \rho_2, Y/X).$$

2. *Let $\widetilde{X}$ be an intermediate covering of $Y/X$, such that $\widetilde{X}/X$ is Galois. Suppose $\rho$ is a representation of $H = \operatorname{Gal}(\widetilde{X}/X)$; we can consider the representation $\widetilde{\rho}$ of $G$ defined by $\widetilde{\rho}(g) = \rho(Hg)$. Then*

$$L(s, \widetilde{\rho}, Y/X) = L(s, \rho, \widetilde{X}/X).$$

3. *If $\widetilde{X}$ is intermediate to $Y/X$ and $\rho$ is a representation of $H = \operatorname{Gal}(Y/\widetilde{X}) \leq \operatorname{Gal}(Y/X)$, then*

$$L(s, \operatorname{Ind}_H^G \rho, Y/X) = L(s, \rho, Y/\widetilde{X}).$$

*Proof of [1,2].*

1. In block-matrix form,

$$\rho_1 \oplus \rho_2 = \begin{bmatrix} \rho_1 & 0 \\ 0 & \rho_2 \end{bmatrix}.$$

So,

$$I - (\rho_1 \oplus \rho_2)(\operatorname{Frob}_D)s^{\nu(C)} = \begin{bmatrix} I_{d(\rho_1)} - \rho_1(\operatorname{Frob}_D)s^{\nu(C)} & 0 \\ 0 & I_{d(\rho_2)} - \rho_2(\operatorname{Frob}_D)s^{\nu(C)} \end{bmatrix}.$$

So, since the last matrix is the same as

$$\begin{bmatrix} I_{d(\rho_1)} - \rho_1(\operatorname{Frob}_D)s^{\nu(C)} & 0 \\ 0 & I_{d(\rho_2)} \end{bmatrix} \begin{bmatrix} I_{d(\rho_1)} & 0 \\ 0 & I_{d(\rho_2)} - \rho_2(\operatorname{Frob}_D)s^{\nu(C)} \end{bmatrix},$$

and because the determinant is multiplicative, the result follows.

2. This one follows directly, if we use that $\operatorname{Frob}_{\widetilde{C}}(\widetilde{X}/X) = H \operatorname{Frob}_D(Y/X)$, where $\widetilde{C}$ is a prime of $\widetilde{X}$ lying above $C$. Showing that $\operatorname{Frob}_{\widetilde{C}}(\widetilde{X}/X) = H \operatorname{Frob}_D(Y/X)$ is straightforward and we omit the verification here.

□

Now, consider what happens to $L(s, \rho, Y/X)$ for the trivial representation $\rho = 1$. We see that $\zeta_X(s) = L(s, 1, Y/X)$ is a well-defined function associated to a graph $X$ and is called the *Ihara zeta function* of $X$. Explicitly,

$$\zeta_X(s) = \prod_{[P]} (1 - s^{\nu(P)})^{-1},$$

with the product running over the primes of $X$.

We can use the Artin-Ihara $L$-function $L(s, \rho, Y/X)$ to get a factorization of the Ihara zeta function $\zeta_Y$ using a theorem of representation theory. An *irreducible representation* is a representation which has no nontrivial subrepresentations. A representation $(V, \rho)$ is a *unitary representation* if $\rho(g)$ is unitary for all $g \in G$, i.e., in matrix notation, $\rho(g)\overline{\rho(g)}^T = I_{d_\rho}$. For a finite group $G$, let $\hat{G}$ represent the set of irreducible unitary representations of $G$.

Then, we have the regular representation for the representation induced by the trivial representation of the trivial subgroup (see [4, Ch. 5]):

$$\mathrm{Ind}_{\{e\}}^G 1 \cong \bigoplus_{\rho \in \hat{G}} d_\rho \rho, \tag{5}$$

where, as before, $d_\rho$ denotes the degree of $\rho$.

So, taking $\widetilde{X} = Y$ and $\rho = 1$ in part 3 of Theorem 4.10 , we get

$$\begin{aligned} \zeta_Y(s) &= L(s, 1, Y/Y) \\ &= L(s, \mathrm{Ind}_{\{e\}}^G 1, Y/X) \\ &= \prod_{\rho \in \hat{G}} L(s, \rho, Y/X)^{d_\rho}, \end{aligned} \tag{6}$$

where we have used (5) along with part 1 of Theorem 4.10 in the last step. Here $G$ is $\mathrm{Gal}(Y/X)$. We can similarly factor the Dedekind zeta function using the Artin $L$-function. Notice that since $1 \in \hat{G}$ and $\zeta_X(s) = L(s, 1, Y/X)$, we see that for a Galois covering $Y/X$, $\zeta_X(s) \mid \zeta_Y(s)$ as polynomials. This divisibility relation in fact holds for non-Galois coverings $Y/X$ too (see [12, Ch. 2]).

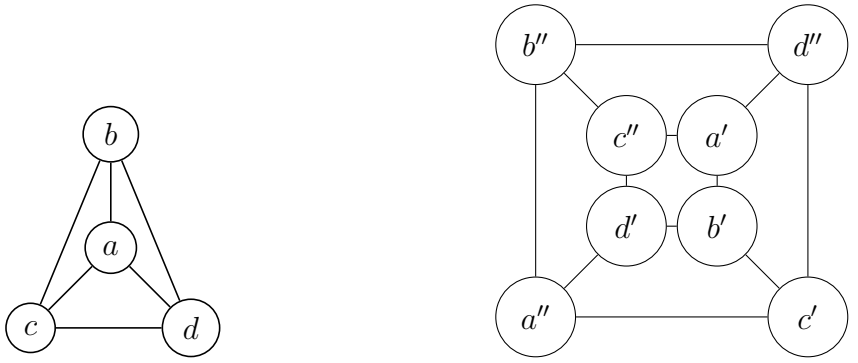
Before we consider an example, notice that the definition of $L(s, \rho, Y/X)$ is not particularly useful for explicit computation since it is generally an infinite product. A much simpler formula for $L(s, \rho, Y/X)$ can be proved, which we now state. For a representation $\rho$ of Galois covering $Y/X$, let the *Artinized adjacency matrix* $A_\rho$ be

$$A_\rho = \sum_{\sigma \in \mathrm{Gal}(Y/X)} A(\sigma) \otimes \rho(\sigma),$$

where $A(\sigma)$ is the matrix with entries $A(\sigma)_{u,v}$ which counts the number of undirected edges between $(u, 1)$ and $(v, \sigma)$ in $Y$, for vertices $u$ and $v$ in $X$. Here $\otimes$ is as usual the tensor product.[8] Also, let $Q_\rho$ be $Q \otimes I_{d_\rho}$, where $Q$ is the diagonal matrix with entries $Q_v = \deg(v) - 1$ for vertices $v$ in $X$. Then,

$$L(s, \rho, Y/X)^{-1} = (1 - s^2)^{(r-1)d_\rho} \det(I - A_\rho s + Q_\rho s^2), \tag{7}$$

where $r = |E_X| - |V_X| + 1$. A proof can be found in [12, Ch. 11].




(a) The tetrahedron $K_4$ (b) The cube as a covering of $K_4$

Figure 4.5

Let us compute the Artin-Ihara $L$-function of the cube as a covering of $K_4$ (Figure 4.5) using the determinant formula. Here $\mathrm{Gal}(Y/X) = \{1, \tau\}$, where $\tau$ exchanges $v'$ with $v''$ for each vertex $v$ of $X = K_4$, and is isomorphic to $\mathbb{Z}/2\mathbb{Z}$. The group $\mathbb{Z}/2\mathbb{Z}$ has two irreducible representations, the trivial representation 1 and the representation $\rho : 1 \mapsto 1, \tau \mapsto -1$. Ordering the vertices of $K_4$ in the natural way, we see that

$$A(1) = \begin{bmatrix} 0 & 1 & 0 & 0 \\ 1 & 0 & 1 & 1 \\ 0 & 1 & 0 & 0 \\ 0 & 1 & 0 & 0 \end{bmatrix}, A(\tau) = \begin{bmatrix} 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 1 \\ 1 & 0 & 1 & 0 \end{bmatrix}.$$

So, $A_1 = A(1) \cdot 1 + A(\tau) \cdot 1$ is the adjacency matrix of $X$, as we would expect, and $A_\rho = A(1) \cdot 1 + A(\tau) \cdot (-1)$. Also since both the representations are degree-1, $Q_1 = Q_\rho = Q \otimes I_1 = Q$, where $Q$ is the diagonal matrix with all entries 2, and so is the same as $2I_4$.

[8] If the reader is not familiar with the tensor product, a gentle introduction is in [2] and a terser presentation is in [1, Ch. 2].

Therefore using the determinant formula (7), since $r = 6 - 4 + 1 = 3$, we see that

$$\begin{aligned} L(s, 1, Y/X)^{-1} &= (1-s^2)^2 \det(I_4 - A_1 s + 2I_4 s^2) \\ &= (1-s^2)^2 \begin{vmatrix} 2s^2+1 & -s & -s & -s \\ -s & 2s^2+1 & -s & -s \\ -s & -s & 2s^2+1 & -s \\ -s & -s & -s & 2s^2+1 \end{vmatrix} \\ &= (s^2-1)^2(s-1)(2s-1)(2s^2+s+1)^3. \end{aligned}$$

Similarly,

$$\begin{aligned} L(s, \rho, Y/X)^{-1} &= (1-s^2)^2 \det(I_4 - A_\rho s + 2I_4 s^2) \\ &= (1-s^2)^2 \begin{vmatrix} 2s^2+1 & -s & s & s \\ -s & 2s^2+1 & -s & -s \\ s & -s & 2s^2+1 & s \\ s & -s & s & 2s^2+1 \end{vmatrix} \\ &= (s^2-1)^2(s+1)(2s+1)(2s^2-s+1)^3. \end{aligned}$$

Therefore, using (6), we must have

$$\begin{aligned} \zeta_Y(s)^{-1} &= L(s, 1, Y/X)^{-1} L(s, \rho, Y/X)^{-1} \\ &= (s^2-1)^5(4s^2-1)(2s^2+s+1)^3(2s^2-s+1)^3. \end{aligned}$$

We also know the Ihara zeta function of $K_4$, since it is simply $L(s, 1, Y/X)$.

We conclude this section with the Riemann hypothesis for the Ihara zeta function.

**Definition 4.11 (Riemann hypothesis)** Let $X$ be a connected $(q+1)$-regular graph with no degree-1 vertices. Then the Ihara zeta function $\zeta_X(q^{-s})$ satisfies the *Riemann hypothesis* if and only if when $0 < \Re(s) < 1$, then $\zeta_X(q^{-s})^{-1} = 0$ implies $\Re(s) = 1/2$.

It is a striking difference with number theory that the graph-theoretic Riemann hypothesis is very easily settled: it holds precisely for the family of Ramanujan graphs. A connected $(q+1)$-regular graph $X$ is said to be *Ramanujan* if

$$\mu = \max\{|\lambda| : \lambda \in \mathrm{Spec}(X), |\lambda| \neq q+1\}$$

is such that $\mu \leq 2\sqrt{q}$.

**Theorem 4.12** *Let $X$ be a connected $(q+1)$-regular graph with no degree-1 vertices. Then $\zeta_X$ satisfies the Riemann hypothesis if and only if $X$ is Ramanujan.*

For better or worse, the determinant formula (7) reduces the proof of this to a straightforward analysis of the quadratic formula, and we omit it here (see [12, Ch. 7]).

# 5 Conclusion

We hope the reader who has followed along thus far is convinced there is truly a wonderful genuine analogy between graphs and number theory. As we have seen, this connection is at the confluence of graph theory, algebra, number theory, topology, and analysis, which makes it all the more exciting. We conclude with a few questions that might be worth investigating in the future.

- An open problem asks whether every finite group occurs as the Galois group of a Galois number field $K/\mathbb{Q}$. This is the Inverse Galois problem. Can this problem be solved for graph coverings?
- One natural way to extend the analogy between graph coverings and number fields would be to introduce a suitable notion of ramification for graph coverings, perhaps by introducing a notion of multiplicity that leads to the concept of a branched covering. Then, we could examine if the $f$-$g$ theorem can be extended to an $e$-$f$-$g$ theorem for coverings. With an $e$-$f$-$g$ theorem, we could look to refine our understanding of the "factorization" of primes in coverings; we saw that in a Galois extension $K/\mathbb{Q}$, there is a surjective homomorphism $\varphi : Z_{\mathfrak{p}} \to \mathrm{Gal}(F_{\mathfrak{p}}/F_p)$, which is an isomorphism when $p$ is unramified. When $p$ is ramified, the kernel of $\varphi$ is called the *inertia subgroup* $I_{\mathfrak{p}}$ *of* $Z_{\mathfrak{p}}$. The group $Z_{\mathfrak{p}}$ and its subgroup $I_{\mathfrak{p}}$ help us understand how a prime behaves in going from $\mathbb{Z}$ to $\mathcal{O}_K$. For instance, it can be shown that the fixed field $K_{I_{\mathfrak{p}}}$ is the largest intermediate field in $K/\mathbb{Q}$ such that $p$ remains unramified in it and that $p$ only splits in going from $\mathbb{Q}$ to the fixed field $K_{D_{\mathfrak{p}}}$ (i.e., $e = f = 1$ and $g = [K_{D_{\mathfrak{p}}} : \mathbb{Q}]$). Do such "refining" towers of intermediate fields exist for graph coverings once we have a notion of ramification?
- Another way to extend the analogy would be to find an analogue to cyclotomic number fields $\mathbb{Q}(\zeta_n)$. It is not at all clear how one would do this, but suppose we succeeded in this! We could then investigate if the Kronecker-Weber theorem held for our cyclotomic graph coverings. The Kronecker-Weber theorem is a fascinating result: it shows that the number fields which are Galois over $\mathbb{Q}$ and have abelian Galois groups (such extensions are called *abelian extensions*) are in bijective correspondence with the intermediate fields of cyclotomic extensions $\mathbb{Q}(\zeta_n)/\mathbb{Q}$ as $n$ runs through $\mathbb{Z}$. Thus, by Galois theory, every finite abelian extension of $\mathbb{Q}$ corresponds to a subgroup of $\mathrm{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{Q}) \cong (\mathbb{Z}/n\mathbb{Z})^\times$ for some $n \in \mathbb{Z}$. A Kronecker-Weber theorem for graph coverings would essentially be the start of a class field theory, the construction of which is listed as a research problem by Terras in her book [12].

# 6 Acknowledgements

I am grateful to Professor Christopher French for copious and very insightful feedback on this report, and for giving me the opportunity to learn about this wonderful topic. Thanks also to

August Peterson for suggestions about making this exposition more clear and accessible. Finally, thank you to Professors Jennifer Paulhus and Joseph Mileti for guiding me in learning algebraic number theory.

# References

[1] M.F. Atiyah and I.G. Macdonald. *Introduction to Commutative Algebra*. Addison-Wesley Series in Mathematics. Addison-Wesley Publishing Company, 1969.

[2] K. Conrad. *Tensor Products*. Available at `https://kconrad.math.uconn.edu/blurbs/`.

[3] I.N. Herstein. *Topics in Algebra*. Second Edition. John Wiley and Sons, 2006.

[4] I.M. Isaacs. *Character Theory of Finite Groups*. Pure and Applied Mathematics. Academic Press, 1976.

[5] S. Lang. *Algebraic Number Theory*. Second Edition. Springer-Verlag, 1994.

[6] J.S. Milne. *Algebraic Number Theory (v3.07)*. Available at `https://www.jmilne.org/math/`. 2017.

[7] J. Neukirch. *Algebraic Number Theory*. Vol. 322. Springer-Verlag, 1999.

[8] P. Pollack. *A Conversational Introduction to Algebraic Number Theory: Arithmetic beyond $\mathbb{Z}$*. Second Edition. Vol. 84. Student mathematical library. American Mathematical Society, 2017.

[9] J.P. Serre. *Local Fields*. Springer-Verlag, 1979.

[10] N. Snyder. *Artin's L-functions: A Historical Approach*. Available at `http://pages.iu.edu/~nsnyder1/`. 2002.

[11] W. Stein. *Algebraic Number Theory, A Computational Approach*. Available at `https://www.williamstein.org/books/ant/`. 2007.

[12] A. Terras. *Zeta Functions of Graphs*. Cambridge Studies in Advanced Mathematics. Available at `https://www.cambridge.org/core`. Cambridge University Press, 2011.

[13] N.G. Triantafillou. *The Chebotarev Density Theorem*. Available at `http://www-math.mit.edu/~ngtriant/notes/`.