

Galois Theory & Questions of Feasibility in Graph Drawing

Carl Kwan

April 20, 2018

Abstract

We survey the applications of Galois theory to the computability of certain graph drawings. First, we review some abstract algebra and Galois theory. Then we discuss graphs which can or cannot be drawn in certain models of computation. Finally, we conclude with a novel corollary extending the results

1 Introduction

Galois theory concerns itself with the connections between the structure of fields and the structure of groups. In fact, the Fundamental Theorem of Galois Theory provides an explicit correspondence between fields and groups which makes certain problems involving fields reducible to problems in group theory and vice versa. Upon immediate gaze, it may appear that Galois theory has scarce relevance to graph drawing. This paper reverses the prior assertion by introducing applications of Galois theory to questions of feasibility in graph drawing. We explore the role of Galois theory in two approaches to graphs: their structure and their representation.

Graphs are essentially mathematical structures which is by nature exactly what algebra aims to study. Among the properties of graphs susceptible to algebraic inspection are the characteristic polynomials of matrices such as the Laplacian and the adjacency matrix. In particular, a significant result due to Abel and Ruffini of Galois theory is the (non)existence of algebraic solutions for polynomials in general which has implications for the feasibility of drawing a graph in certain models of computation - especially for models built upon radicals. This part of the project will look at the relationship between solvable groups and the drawing of graphs in certain algebraic models of computation.

Drawings, on the other hand, are ultimately geometric creatures. Drawings of graphs - doubly so. A classical application of Galois theory looks at compass and straightedge constructions and, by doing so, we can discern which graphs can be drawn in computation models equivalent to classical constructions. This part of the project considers the results in classical geometry from a Galois theoretic perspective and their implications for graph drawing.

We will begin by introducing some algebraic structures such as groups, fields, etc. Following will be an overview of Galois theory and some of its applications. The third section concerns itself with examples of graphs that cannot be drawn. Finally, we conclude with a discussion of future work and some classification results.

Proofs of most theorems and lemmas in algebra will be omitted since the results of interest are those pertaining to graph drawing and because the proofs can be found in most standard algebra texts [1, 3]. Most of the results involving graph drawing are from [2].

2 Groups and Fields

2.1 Groups

Groups are a fundamental structure in algebra upon which many other structures are constructed. They formalize and generalize some intuitive notions we obtain from arithmetic regarding how elements interact with each other under certain operations. We begin with some definitions.

Definition 2.1. A *group* is a couple $(G, +)$ where G is a set and $+ : G \times G \rightarrow G$ a binary operation such that

1. for any $a, b, c \in G$

$$(a + b) + c = a + (b + c),$$

2. there is a $0 \in G$ such that

$$0 + a = a$$

for any $a \in G$,

3. for any $a \in G$, there is a $-a \in G$ such that

$$a + (-a) = 0.$$

We may write G when $+$ is clear.

Some examples of groups are the integers under addition $(\mathbb{Z}, +)$ or modulo n , ie.

$$\mathbb{Z}/n\mathbb{Z} = \{0, 1, 2, \dots, n-1\}.$$

We also note that groups can contain other groups.

Definition 2.2. Given a group $(G, +)$, a subgroup of G is a subset $H \subset G$ such that H is also a group under $+$. Write $H \leq G$.

Note that any group has itself and the trivial group $\{0\}$ as subgroups.

2.1.1 The Symmetric Group

Of particular relevance to Galois theory are the permutation groups S_n .

Definition 2.3. A *permutation* on n items is a bijection $\{1, \dots, n\} \rightarrow \{1, \dots, n\}$. We write S_n for all the permutations on n items, ie.

$$S_n = \{\rho : \{1, \dots, n\} \leftrightarrow \{1, \dots, n\}\}.$$

It is a matter of checking to see that S_n forms a group under function composition. The identity of S_n is the identity function and inverses are inverse functions. We call S_n the *symmetric group*.

Regarding notation, permutations may sometimes be written in *Cauchy two-line* form, ie.

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & \dots & n \\ \sigma(1) & \sigma(2) & \sigma(3) & \dots & \sigma(n) \end{pmatrix}$$

Now, here is an interesting result regarding the subgroups of S_n :

Lemma 2.4. Suppose a subgroup $H \leq S_n$ contains:

1. a permutation σ such that $\sigma^k(x) = x$ for a unique $x \in H$ and fixes all elements not of the form $\sigma^i(x)$ (ie. a *cycle*)
2. a permutation that only swaps two elements (ie. a *transposition*).

Then $H = S_n$.

2.1.2 Abelian Groups

For sufficiently large n , there is a fundamental difference between the symmetric group S_n and the other examples such as $(\mathbb{Z}, +)$ and $(\mathbb{Z}/n\mathbb{Z}, +)$. The notion of addition in \mathbb{Z} comes not only with associativity, but also the property of *commutativity*. That is to say, for any $a, b \in \mathbb{Z}$, we have

$$a + b = b + a.$$

Definition 2.5. If all elements in a group G commutes, then we call G *abelian*.

Note that S_n is not abelian for sufficiently large $n \geq 3$. However, while S_3 and S_4 are not abelian themselves, they happen to be constructible from abelian groups.

2.1.3 Solvable Groups

Consider the cyclic group

$$\mathbb{Z}/n\mathbb{Z} = \{0, 1, \dots, n-1\}.$$

The notation invokes some pensivity. In particular, the notation $n\mathbb{Z}$ actually refers to a group

$$n\mathbb{Z} = \{n \cdot m \mid m \in \mathbb{Z}\}.$$

By removing all the elements of $n\mathbb{Z}$ from \mathbb{Z} , we obtain $\mathbb{Z}/n\mathbb{Z}$. We call $\mathbb{Z}/n\mathbb{Z}$ a *quotient group*.

Quotient groups are only introduced because we wish to consider *solvability*.

Definition 2.6. A group G is *solvable* if there is a chain of subgroups

$$\{1\} = G_0 \trianglelefteq G_1 \trianglelefteq \dots \trianglelefteq G_n = G$$

such that G_{i+1}/G_i is abelian.

Corollary 2.7. From the definition, we can see that the subgroup of a solvable group is itself solvable by simply taking a shorter chain.

Theorem 2.8. The symmetric group S_n is not solvable for $n \geq 5$.

The name *solvable* is used due to the connotation with polynomials solvable by radicals. In fact, we will see that Theorem 2.8 is the reason there are no general closed form solutions for polynomials of degree 5 or higher.

2.2 Fields

We begin with some basic definitions and examples.

Definition 2.9. A field is a triple $(F, +, \cdot)$ such that $(F, +)$, $(F - \{0\}, \cdot)$ are abelian groups that satisfy the distributive property, ie.

$$x(y + z) = xy + xz$$

Examples of fields include \mathbb{Q} , \mathbb{R} , and \mathbb{C} . Similar with groups, we can consider fields that contain other fields. In this instance, we have

$$\mathbb{Q} \subset \mathbb{R} \subset \mathbb{C}$$

so we may say \mathbb{Q} is a *subfield* of \mathbb{R} . However, in the context of Galois theory, instead of looking from the “outside-in” as we do with groups, we usually look at fields from the “inside-out”.

Definition 2.10. A field E is an *extension* of a field F if $E \supset F$. If there is a chain of extensions

$$F \subset E_1 \subset E_2 \subset \cdots,$$

then we call F the *base field*. One writes E/F .

Now given a base field, usually \mathbb{Q} in this article, we can construct more fields. For example, consider

$$\mathbb{Q}(\sqrt{2}) = \{a + b\sqrt{2} \mid a, b \in \mathbb{Q}\}.$$

Checking the axioms shows that $\mathbb{Q}(\sqrt{2})$ is indeed a field. Moreover, it contains \mathbb{Q} so $\mathbb{Q}(\sqrt{2})$ is an extension of \mathbb{Q} . By *adjoining* \mathbb{Q} with $\sqrt{2}$, a field extension has been constructed. One can continue to adjoin roots

$$\mathbb{Q}(\sqrt{2})(\sqrt{3}) \simeq \mathbb{Q}(\sqrt{2}, \sqrt{3}) = \{a + b\sqrt{2} + c\sqrt{3} + d\sqrt{6} \mid a, b, c, d \in \mathbb{Q}\}.$$

Note that the inclusion of $\sqrt{6}$ as an element since $\sqrt{2}\sqrt{3} = \sqrt{6} \notin \mathbb{Q}$ so in order to satisfy closure, we must include it explicitly.

Observe that every element of $\mathbb{Q}(\sqrt{2}, \sqrt{3})$ is a linear combination of $1, \sqrt{2}, \sqrt{3}, \sqrt{6}$. Indeed, not only is $\mathbb{Q}(\sqrt{2}, \sqrt{3})$ an extension of \mathbb{Q} , it is also a vector space over \mathbb{Q} . And like with any vector space, we can consider its dimension.

Definition 2.11. Let E/F be a field extension. Call the dimension of E/F as a vector space the *degree* of E/F and write $[E : F]$.

Lemma 2.12. If $E \supset K \supset F$ as fields, then

$$[E : F] = [E : K][K : F].$$

2.2.1 Splitting Fields

Note that most examples of fields extensions up to this point consisted of adjoining roots of polynomials such as $\sqrt{2}, \sqrt{3}$, etc. Indeed, we can define fields by how polynomials act in them. For example, $\mathbb{Q}(\sqrt{2})$ contains the roots of $p(x) = x^2 - 2 = (x - \sqrt{2})(x + \sqrt{2})$ so we may factor $p(x)$ over $\mathbb{Q}(\sqrt{2})$. Moreover, $p(x)$ is the *minimal* polynomial of $\sqrt{2}$ since it is the polynomial of smallest degree with $\sqrt{2}$ as a root. On the other hand, $p(x)$ does not factor over \mathbb{Q} since $\sqrt{2} \notin \mathbb{Q}$. In this case, we say $p(x)$ is *irreducible* over \mathbb{Q} .

Definition 2.13. The splitting field of a polynomial p over a base field F is the field extension of smallest degree in which p splits into linear factors. Write $\text{split}(p)/F$

Conversely, a field extension E that happens to be the splitting field of a polynomial over F is called a *normal* extension of F . A field that happens to split the minimal polynomial of all its elements is called *separable*.

Note that a splitting field will contain all the roots of the polynomial of interest.

2.2.2 Cyclotomic Fields

From the definitions and examples of field extensions, we see that $\mathbb{R}(i) = \mathbb{C}$ where i is the root to $i^2 + 1 = 0$. (Incidentally, $\mathbb{R}^2 \simeq \mathbb{C}$ over \mathbb{R} due a dimensionality argument). However, the more algebraically interesting structure is $\mathbb{Q}(i)$. In fact, we may generalize the notion of i .

Definition 2.14. The n -th root of unity is the complex number ζ_n that satisfies $\zeta_n^n = 1$.

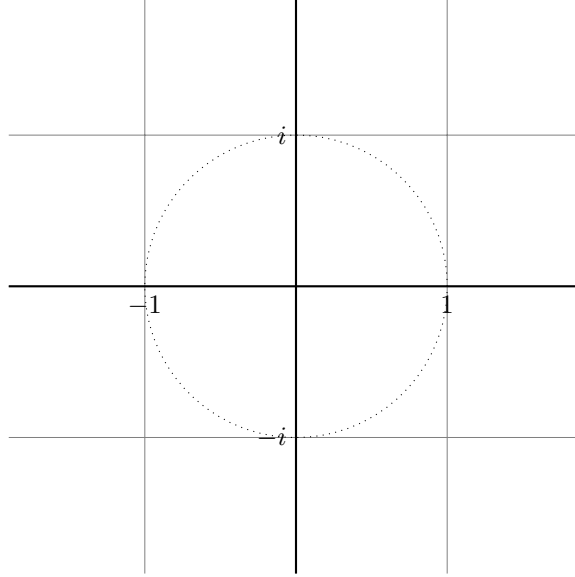


Figure 1: The powers of $\zeta_4 = i$

By this definition, $i = \zeta_4$ is the 4-th root of unity. As desirable as it may be, unfortunately $\mathbb{Q}(\zeta_n)$ does not have degree n over \mathbb{Q} . Looking at

$$\mathbb{Q}(i) = \{a + bi \mid a, b \in \mathbb{Q}\}$$

makes this clear. Instead, the result is even more astonishing.

Definition 2.15. The Euler- φ function counts the number of positive integers relatively prime up to a specified natural, ie.

$$\varphi(n) = \# \text{ of positive integers relatively prime to } n.$$

Theorem 2.16.

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

3 Galois Theory

Galois theory provides a correspondence between fields and groups. Interestingly, there is an application to compass and straightedge constructions despite the historical gap between the Ancient Greeks and Évariste Galois. We begin by introducing automorphisms.

3.1 Automorphism and Galois Groups

A common method of investigating algebraic structures is by looking at the maps between them. In our case, it is sufficient to look at maps from fields to themselves.

Definition 3.1. An *automorphism* of a field F is a bijection $\tau : F \rightarrow F$ that is linear in addition and multiplication, ie.

$$\tau(xy + z) = \tau(x)\tau(y) + \tau(z)$$

for all $x, y, z \in F$.

As with the permutations, the set of automorphisms also form a group.

Definition 3.2. Let $\text{Aut}(E/F)$ denote the set automorphisms over a field extension E/F . This forms a group under function composition. We call $\text{Aut}(E/F)$ the *automorphism group* of E/F .

If E/F is normal and separable, then we call E a *Galois extension* of E . The automorphism group of E/F is then called its *Galois group* and we write $\text{Gal}(E/F)$.

Recall again that one may view finite field extensions as vector spaces and linear maps on vector spaces are defined by how they act on the basis. If the field of interest is the splitting field of a polynomial irreducible over the base field, then the basis contains the roots of the polynomial. By necessity, the automorphism must send the roots to other roots. In this sense, the automorphisms are really permutations on the roots. For example, the automorphism group of $\mathbb{Q}(\sqrt{2}) = \text{split}(x^2 - 2)$ consists of

$$\text{id} = \begin{pmatrix} \sqrt{2} & -\sqrt{2} \\ \sqrt{2} & -\sqrt{2} \end{pmatrix}, \quad \sigma = \begin{pmatrix} \sqrt{2} & -\sqrt{2} \\ -\sqrt{2} & \sqrt{2} \end{pmatrix}$$

so $\text{Gal}(\mathbb{Q}(\sqrt{2})/\mathbb{Q}) = S_2$. Notice that $\text{Gal}(\mathbb{Q}(\sqrt{2}, \sqrt{3})) = \text{Gal}(\text{split}((x^2 - 2)(x^2 - 3)))$ must contain automorphisms that move the roots of $x^2 - 2$ but fix those of $x^2 - 3$. These automorphisms, then, are equivalent to id and σ - the automorphisms of $\text{Gal}(\mathbb{Q}(\sqrt{2})/\mathbb{Q}) \simeq S_2$. Hence, we must know S_2 is a subgroup of $\text{Gal}(\mathbb{Q}(\sqrt{2}, \sqrt{3})/\mathbb{Q})$. Yet, $\mathbb{Q}(\sqrt{2})$ is also a subfield of $\mathbb{Q}(\sqrt{2}, \sqrt{3})$. This is no coincidence. Indeed, the Fundamental Theorem of Galois Theory provides a correspondence between the subgroups of a Galois group and the subfields of the field in question. We forgo the statement of the theorem here and instead conclude the section with some results involving Galois groups.

Theorem 3.3. Suppose α can be written as an expression using radicals and is a root of an irreducible polynomial p with coefficients in \mathbb{Q} . Let $K = \text{split}(p)$. Then $\text{Gal}(K/\mathbb{Q})$ cannot contain S_n for $n \geq 5$ as a subgroup.

Proof. It is a known result $\text{Gal}(K/\mathbb{Q})$ must be solvable from the given hypotheses. From Corollary 2.7 we know that subgroups of solvable groups are solvable. Hence, S_n for $n \geq 5$ cannot be a subgroup by Theorem 2.8. \square

Theorem 3.4. Let $q(x)$ be an irreducible monic polynomial with integer coefficients. Let d be the discriminant of q . Let p be prime not dividing d . If $q(x)$ splits over $\mathbb{Z}/p\mathbb{Z}$ into irreducible polynomials of degrees d_1, d_2, \dots, d_n , then $\text{Gal}(\text{split}(q)/\mathbb{Q})$ contains a permutation that is the composition of disjoint cycles of lengths d_1, d_2, \dots, d_n .

3.2 Compass and Straightedge Constructions

The ancient Greeks did not have the benefits of modern algebra we do today. Instead of manipulating equations with numbers and polynomials, they instead considered constructions achievable by compass and straightedge, ie. circles and lines. In fact, Euclid's original proof of the infinitude of primes was achieved in this fashion. These are the rules of their constructions:

Definition 3.5. Start with two points p_0, p_1 . We may

1. draw lines intersecting any two previously constructible points,
2. draw circles centered at a previously constructible point through another constructible point,
3. take the points of intersection of any combination of constructible circles and lines as constructible points.

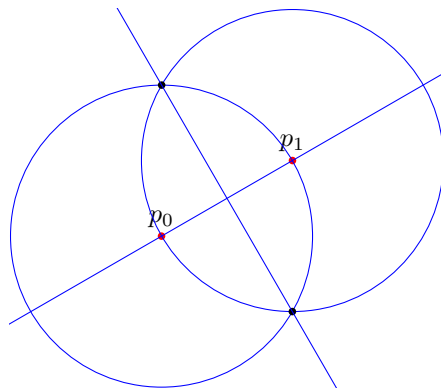


Figure 2: A compass and straightedge construction

If we take the distance between p_0, p_1 as the unit length, then addition, subtraction, multiplication, and division are straightforward along with the construction of \mathbb{N} , \mathbb{Z} , and \mathbb{Q} . Moreover, it is a matter checking that the constructible numbers form a field under the usual operations of \mathbb{R} . The following result provides a characterization of the constructible objects.

Theorem 3.6. Any constructible point must have coordinates in a field extension over a constructible base field as subsets of \mathbb{R} with a degree that is a power of 2.

Proof. Any constructible point is the root of intersections of circles

$$(x - a)^2 + (y - b)^2 - c = 0$$

or lines

$$ax + by + c = 0$$

or both. These are polynomial equations of degree two or lower. So our point must have coordinates in extensions of degree two or lower. The only possibilities are degrees 1 or 2 which are both powers of two. By Lemma 2.12, the multiplicity of degrees with respect to extensions means any constructible point must have coordinates in fields with degrees that are powers of 2. \square

This essentially says that we can find any constructible point using the usual operations of arithmetic and square roots.

4 Feasibility Results of Graph Drawing

First we describe the models of computation in which we compute the coordinates of graph. Then we provide examples of graphs that are impossible to draw using three different graph drawing techniques.

4.1 Models of Computation

Two similar models of computation are of interest. One of which is equivalent to the classical compass and straightedge constructions which the ancient Greeks originally levied.

Definition 4.1. Consider an algebraic computation tree where at each vertex one may perform square roots, complex conjugation, and the usual operations of arithmetic on previously computed values. We call this a *quadratic computation tree*.

Definition 4.2. Consider an algebraic computation tree where at each vertex one may perform k -th roots, complex conjugation, and the usual operations of arithmetic on previously computed values. We call this a *radical computation tree*.

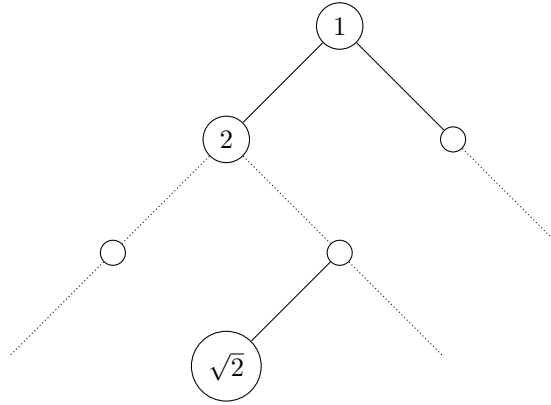


Figure 3: A possible quadratic (or radical) computation tree

By Theorem 3.6, quadratic computation trees can compute any point constructible by compass and straightedge. Moreover, despite the difference in strength between the two models, the only difference is that a quadratic computation tree is a radical computation tree but with the restriction $k = 2$.

4.2 Impossible Force Directed Drawings

We consider force-directed drawings by Fruchterman and Reingold although similar results hold for other force-directed techniques. Fruchterman and Reingold defined for each vertex v an attractive force

$$f_a(d) = \frac{d^2}{k}$$

towards its neighbours and a repulsive force

$$f_r(d) = \frac{k^2}{d}$$

away from all vertices. Here, d is the distance between vertices and k a constant. The vertices are placed such that the total force on each vertex is zero, ie. at an equilibrium. For a cyclic graph C_n , this amounts to vertices spaced evenly apart on a circle. However, consider C_7 .

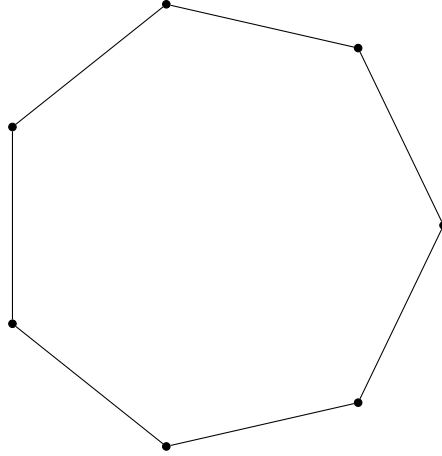


Figure 4: A Fruchterman and Reingoldman force-directed drawing C_7

The vertices are positioned exactly at the powers of ζ_7 in the complex plane.

Theorem 4.3. The Fruchterman and Reingoldman force-directed drawing of C_7 cannot be drawn using coordinates computed by a quadratic computation tree.

Proof. The vertices of C_7 in a Fruchterman and Reingoldman force-directed drawing are positioned exactly at the powers of ζ_7 in the complex plane. However,

$$[\mathbb{Q}(\zeta_7) : \mathbb{Q}] = \varphi(7) = 6$$

is not a power of 2. So they are not contained in a tower of square roots (nor computable using the usual operations of arithmetic) and cannot be computed by a quadratic computation tree. \square

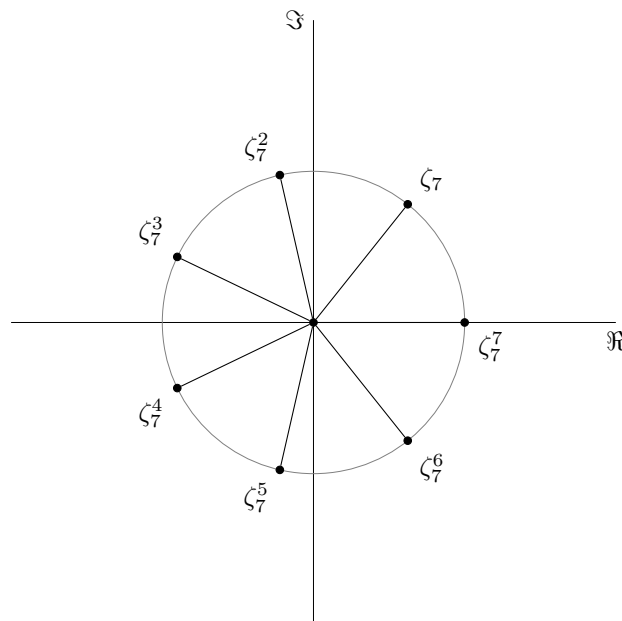


Figure 5: The powers of ζ_7

4.3 Impossible Spectral Drawings

Spectral graph drawing positions vertices according to the eigenpairs of the Laplacian of a graph. Recall, the Laplacian of a graph $G = (V, E)$ is a matrix defined to be

$$\mathcal{L} = D - A$$

where D is the degree matrix and A is the adjacency matrix of the graph, ie.

$$D_{ij} = \begin{cases} \deg(v_i) & \text{if } i = j \\ 0 & \text{otherwise} \end{cases}, \quad A_{ij} = \begin{cases} 1 & \text{if } (v_i, v_j) \in E \\ 0 & \text{otherwise} \end{cases}.$$

Finding the eigenvalues of \mathcal{L} reduces to finding the roots of the characteristic polynomial $\text{char}(\mathcal{L})$. If we can find a graph whose eigenvalues cannot be computed with roots, then we have found a graph whose spectral drawing cannot be computed with a radical computation tree.

Indeed:

Theorem 4.4. The spectral drawing of the graph in Figure 6 cannot be computed with a radical computation tree.

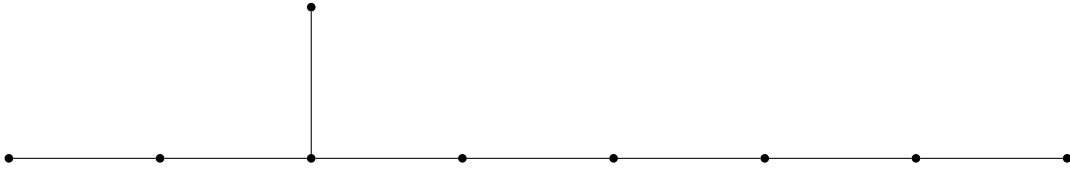


Figure 6: A graph whose spectral drawing cannot be computed with a radical computation tree.

Proof. Computing the characteristic polynomial of the graph gives

$$p(x) = x^9 - 16x^8 + 104x^7 - 354x^6 + 678x^5 - 730x^4 + 417x^3 - 110x^2 + 9x.$$

Since the zero eigenvalue is not very interesting we may factor out x and obtain

$$q(x) = x^8 - 16x^7 + 104x^6 - 354x^5 + 678x^4 - 730x^3 + 417x^2 - 110x + 9.$$

By a computer algebra system or otherwise, we see that q is irreducible. We claim there is a 7-cycle and a transposition in subgroup of $\text{Gal}(\text{split}(q)/\mathbb{Q})$. Observe that q factors into irreducibles

$$q(x) \equiv (x + 27)(x^7 + 19x^6 + 25x^5 + 25x^4 + 3x^3 + 26x^2 + 25x + 21) \pmod{31}$$

and

$$q(x) \equiv (x + 1)(x^2 + 15x + 39)(x^5 + 9x^4 + 29x^3 + 10x^2 + 36x + 16) \pmod{41}.$$

Now 31 and 41 are both primes not dividing the discriminant $9931583 \cdot 2^8$ of q . By Theorem 3.4, the first factorization admits the existence of a 7-cycle and the second admits the existence of a permutation σ that is the composition of a 5-cycle and a transposition. Then σ^5 is a transposition. By Lemma 2.4, we have $\text{Gal}(\text{split}(q)/\mathbb{Q}) \simeq S_8$. By Theorem 3.3, we cannot compute the roots of q with a radical computation tree. Hence, the only computable eigenvalue is zero. \square

4.4 Impossible Circle Packings

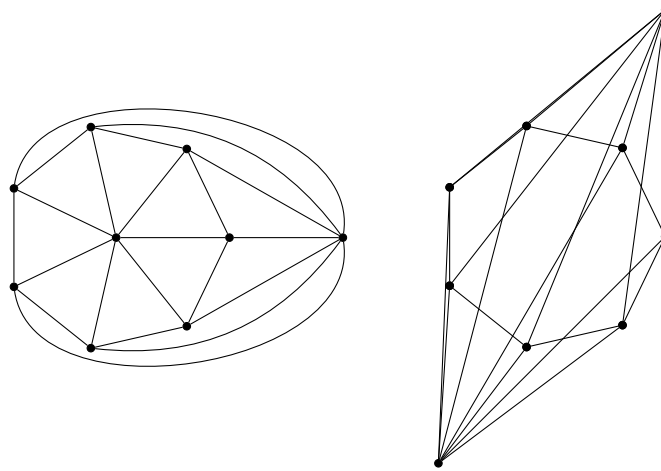


Figure 7: Bipyrmaid(7)

Circle packings are representations of graphs where nodes are represented with circles of arbitrary size and contact between perimeters denote edges. For example, the Bypyrmaid(7) graph (see Figure 7) has the circle packing seen in Figure 8.

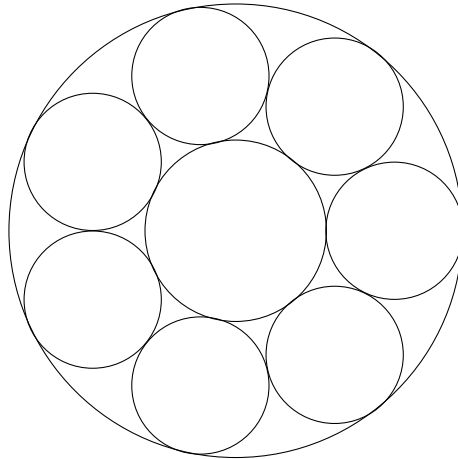


Figure 8: The circle packing of Bipyrmaid(7)

However, this example is a poor one for quadratic computation trees.

Theorem 4.5. The circle packing of Bipyrmaid(7) cannot be drawn by a quadratic computation tree.

Proof. Each of the circles in the middle ring of the circle packing of Bipyrmaid(7) are centred at a power of ζ_7 . Since

$$[\mathbb{Q}(\zeta_7) : \mathbb{Q}] = \varphi(7) = 6$$

is not a power of 2, it cannot be computed with a quadratic computation tree. \square

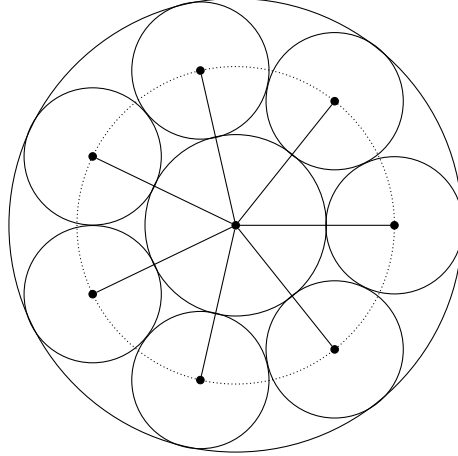


Figure 9: The centres of the middle ring of circles are located at the powers of ζ_7

5 Conclusion

We have seen that the tools of Galois theory leveraged correctly provide simple examples of graphs that have drawings that cannot be computed under certain models. These simple examples can be generalized easily to provide feasibility results (both positive and negative) for classes of graphs. For example:

Theorem 5.1. The Fruchterman and Reingold force-directed drawings of every cyclic graph C_p where p is a Fermat prime can be computed with a quadratic computation tree.

Proof. Equally spacing p vertices on a circle is equivalent to placing them on the powers of ζ_p . Since p is a Fermat prime, it is of the form $p = 2^k + 1$. Then

$$[\mathbb{Q}(\zeta_p) : \mathbb{Q}] = \varphi(p) = p - 1 = 2^k$$

is a power of two. Hence, the coordinates may be computed by a quadratic computation tree. \square

From here, there are two potential directions to take - not mutually exclusive to each other. One is to consider what tools from other areas of algebra (eg. algebraic geometry/topology, sheaf theory, etc.) can be applied to questions of feasibility. Topology is particularly promising as embeddings between spaces is an area of research that is well explored. The other is to look at other models of computation and investigate the classes of graphs that can be drawn using them. One model of note is the *root computation tree*, ie. the model that can compute all algebraic numbers. The obvious impossible results would stem from the graphs with transcendental coordinates. Circle packings have an immediate connection here in the form of π .

References

- [1] Serge Lang (auth.). *Algebra*. Graduate Texts in Mathematics 211. Springer-Verlag New York, 3 edition, 2002.
- [2] Michael J. Bannister, William E. Devanny, David Eppstein, and Michael T. Goodrich. The galois complexity of graph drawing: Why numerical solutions are ubiquitous for force-directed, spectral, and circle packing drawings. *Journal of Graph Algorithms and Applications*, 19(2):619–656, 2015.
- [3] Nathan Jacobson. *Basic algebra 1*. Bk. 1. 2 sub edition, 1985.