Algebraic Properties of Chromatic Polynomials and Their Roots

A thesis

submitted in partial fulfilment

of the requirements for the Degree

of

Master of Science

at the

University of Waikato

by

Hamish Julian Gilmore

THE UNIVERSITY OF
WAIKATO
Te Whare Wānanga o Waikato

University of Waikato

2015

Abstract

In this thesis we examine chromatic polynomials from the viewpoint of algebraic number theory. We relate algebraic properties of chromatic polynomials of graphs to structural properties of those graphs for some simple families of graphs. We then compute the Galois groups of chromatic polynomials of some sub-families of an infinite family of graphs (denoted $\{G_{p,q}\}$) and prove a conjecture posed in [15] concerning the Galois groups of one specific sub-family. Finally we investigate a conjecture due to Peter Cameron [8] that says that for any algebraic integer α there is some $n \in \mathbb{N}$ such that $\alpha + n$ is the root of some chromatic polynomial. We prove the conjecture for quadratic and cubic integers and provide strong computational evidence that it is true for quartic and quintic integers.

Acknowledgements

I would like to thank my supervisor Dr. Daniel Delbourgo for his continual guidance in writing this thesis and for his suggestion of an interesting project. His encouragement and patience, particularly during final stages of writing, have been invaluable.

I also greatly appreciate Prof. Kevin Broughan for very generously reading a draft of my thesis, for his constructive comments, and for his warmth and encouragement.

I am grateful for the financial support of a University of Waikato Masters Research Scholarship and A Zulauf Trust Scholarship.

Contents

Notation

$(x)_n$	The falling factorial, $(x)_n = x(x-1)\dots(x-n+1)$

Graph theory

$V(G)$	The vertex set of a graph G
$E(G)$	The edge set of a graph G
$G[X]$	The graph induced by $X \subseteq V(G)$
$G + H$	The join of graphs G and H
$G - X$	The graph obtained by deleting vertices $X \subseteq V(G)$
$G \pm X$	The graph obtained by adding/deleting edges $X \subseteq E(G)$
$\overline{G}$	The complement of G
C_n	The cycle of order n
K_n	The complete graph of order n
$\overline{K}_n$	The null graph of order n
P_n	The path of order n
W_n	The wheel of order n
θ_{a_1,a_2,a_3}	Theta graph
χ	A graph colouring
$P(G;x)$	The chromatic polynomial of G

Algebraic number theory

$R[x]$	The ring of polynomials with coefficeints in R
$\deg(f(x))$	The degree of the polynomial $f(x)$
$\mu_{\alpha,F}(x)$	The minimal polynomial for α over F

E/F	E is a field extension of F
$[E : F]$	The degree of E/F
$F(\alpha_1, \ldots, \alpha_n)$	The field obtained by adjoining $\alpha_1, \ldots, \alpha_n$ to F
$K_{f(x)}/F$	The splitting field for $f(x)$ over F
$\langle x \rangle$	The ideal generated by x
$\{1\}$	The trivial group
A_n	The alternating group on n letters
S_n	The symmetric group on n letters
$D(n)$	The dihedral group of order $2n$
$C(n) \cong \mathbb{Z}/n\mathbb{Z}$	The cyclic group of order n
$E(n)$	The Euclidean group of order n ($E(4)$ is the Klein four-group)
S/R	S is a ring extension of R
$\mathcal{O}_F$	The ring of integers in F
$\Delta_{\mathcal{B}}$	Discriminant of a basis $\mathcal{B}$
Δ_F	Discriminant of a field F

Chapter 1

Introduction

Graphs have been studied for a number of centuries. Chronologically, Euler's solution to the 'Seven Bridges of Königsberg' problem, published in 1736, is regarded as being the first use of graph theory. Since then graph theory has had many applications in a variety of subjects: to model molecules in chemistry and physics, to model networks in computer science, to describe structures in natural language, and to study various aspects of social behaviour, to name but a few.

Perhaps the most famous graph-theoretic problem to be posed is the four colour theorem, which asserts that any map can be coloured with at most four colours such that adjacent regions do not share the same colour. By representing each region of a map with a vertex, and adding an edge between two vertices if the two regions share a border, one obtains a type of graph known as a planar graph (i.e. a graph that can be drawn with no crossing edges).

The chromatic polynomial itself was introduced by Birkhoff in 1912, and for planar graphs it was hoped that their study would lead to a proof of the four colour theorem (the chromatic polynomial counts the number of colourings of a graph, see section 2.2). While the chromatic polynomial played no role in the eventual proof of the four colour theorem, it has been since been generalised to include non-planar graphs.

The chromatic polynomial has been used mostly as a tool to answer combinatorial questions, that is as a means of relating the structure of certain families of graphs to their chromaticity. An overview of much of this work can be found in [10].

Less well developed is the study of chromatic polynomials as a subclass of polynomials in their own right. A notable exception to this is the work of Woodall and Jackson, who showed in [25] and [14] that there are no chromatic roots in the real intervals $(-\infty, 0)$, $(0, 1)$, and $(1, 32/27]$; Thomassen, who showed in [23] that chromatic roots are dense in the interval $(32/27, \infty)$; and Sokal, who showed that chromatic roots are dense in the complex plane [22]. These results have significance in statistical physics where the location of chromatic roots yield possible locations of phase transitions in the Potts model [21] (in fact the chromatic polynomial is a special case of the Potts model partition function).

Very little is currently known about the algebraic nature of chromatic polynomials and their roots, especially the relationship between the structure of a graph and the algebraic properties of its chromatic polynomial. It is this interplay that we shall consider in this thesis.

1.1 Overview

We begin the background discussion in **Chapter 2** by defining graphs and some graph operations, and introducing the appropriate notation and terminology. We then discuss graph colourings, define the chromatic polynomial, and establish various relations that will enable us to calculate the chromatic polynomials for a given graph.

Chapter 3 covers the basics of algebraic number theory, including field extensions and rings of integers. We also define algebraic invariants such as Galois groups and number field discriminants, that will be discussed in relation to chromatic polynomials later in this thesis.

As we mentioned before, the study of the algebraic nature of chromatic polynomials is not well developed, so in **Chapter 4** we briefly review some of what is currently known. First we discuss some results that follow immediately from already known properties of three families of graphs; namely chordal graphs, clique-separable graphs, and cycle graphs. We then give an overview of some computational investigations of chromatic polynomials; work that has been done towards proving Peter Cameron's '$\alpha + n$' and '$n\alpha$' conjectures, as well as a study of algebraic invariants of a family of graphs called theta graphs.

In [15] Morgan described a three-parameter family of graphs and found infinite sub-families of graphs with chromatic polynomials that have Galois groups A_3, $\mathbb{Z}/4\mathbb{Z}$, and $D(4)$. In **Chapter 5** we show that in order to determine the Galois groups of the chromatic polynomials of this family, it is actually only necessary to consider a two-parameter sub-family of graphs. This observation allows us to completely determine the Galois group of the chromatic polynomials for graphs with certain fixed values for one of the parameters (which includes those graphs considered in [15]), and in doing so we prove a conjecture posed in [15].

In **Chapter 6** we study a family of graphs called bicliques in order to address Peter Cameron '$\alpha + n$' conjecture. This conjecture has been proven to be true for quadratic and cubic integers. We improve these results by describing larger sets of bicliques that satisfy the conjecture; for a sub-family of bicliques we are able to fully describe the splitting fields of the chromatic polynomials in terms of the biclique's parameters.

Finally, in **Chapter 7** we present computational evidence for the $\alpha + n$ conjecture by demonstrating that every quartic field with discriminant $|\Delta| \leq 10^6$ arises as the splitting field of the chromatic polynomial a $(4, k)$-biclique. We also show that every quintic field with discriminant $|\Delta| \leq 10^6$ arises as the splitting field of a $(5, k)$-biclique. In doing this we find a $(5, k)$-biclique whose chromatic polynomial has Galois group $C(5)$, previously there were no known graphs with Galois group $C(n)$ where $n \geq 5$.

Chapter 2

Graphs and the chromatic polynomial

In this chapter some basic graph theory will be introduced, followed by a discussion of graph colourings and the chromatic polynomial.

2.1 Graph theory

Let us begin by defining a graph.

Definition 2.1 (Graph)

1. *A **finite simple graph** $G = (V, E)$ is a finite set V together with a set E of two-element*[1] *subsets of V. An element $\{u, v\}$ of E will often be represented using the shorter notation uv.*

2. *The elements of V are called **vertices** and the elements of E are called **edges**. To avoid ambiguity, the vertex set and edge set of a graph G will sometimes be denoted $V(G)$ and $E(G)$, respectively.*

Definition 2.2 (Order and size of a graph) *The **order** of a graph G is the number of vertices $|V(G)|$, and the **size** of G is the number of edges $|E(G)|$.*

[1] That is two distinct elements, we will not consider graphs with loops.

A few basic examples of graphs are the complete graphs, null graphs, and cycle graphs, as we now describe.

Example 2.3 (Complete graph) *The* ***complete graph of order*** n, K_n, *is the graph with* $|V| = n$ *and* $E = \{\{u, v\} \mid u, v \in V, u \neq v\}$.

Example 2.4 (Null graph) *The* ***null graph of order*** n *is the graph with* $|V| = n$ *and* $E = \emptyset$. *This graph will be denoted* $\bar{K}_n$ *(see Definition 2.10).*

Example 2.5 (Path graph) *For any positive integer* n *the* ***path of order*** n, *or path on* n *vertices, is the graph* $P_n = (V, E)$ *where* $V = \{v_1, \ldots, v_n\}$ *and* $E = \{\{v_i, v_j\} \mid i - j = 1\}$. *For example the path* P_5 *is shown in figure 2.1. The vertices* v_1 *and* v_n *are called the* ***end-vertices*** *of the path.*

Figure 2.1: The path of order 5, P_5.

Graph theory is concerned not with the underlying set of vertices but with the relationships between them, those relationships being expressed as edges. Therefore we will typically be concerned with properties of graphs that are invariant under isomorphisms.

Definition 2.6 (Graph isomorphism) *Two graphs* $G = (V, E)$ *and* $G' = (V', E')$ *are* ***isomorphic*** *if there is a bijection* $\phi : V \to V'$ *such that* $\{u, v\} \in E$ *if and only if* $\{\phi(u), \phi(v)\} \in E'$. *The function* ϕ *is called a graph isomorphism. If* G *and* G' *are isomorphic then we write* $G \cong G'$.

Embedded in any graph G is a number of smaller graphs, called subgraphs, with vertex sets that are subsets of $V(G)$.

Definition 2.7 (Subgraph) *Let* $G = (V, E)$ *be a graph. A* ***subgraph*** *of* G *is a graph* $G' = (V', E')$ *such that* $V' \subseteq V$ *and* $E' \subseteq E$. *Note that it is implicit in the assertion that* G' *is a graph that the elements of* E' *are two-element subsets of* V'.

An example of a subgraph of a graph G is the vertex induced subgraph. For any $V' \subseteq V(G)$ it is the subgraph of G with vertex set V' and the maximum number of edges.

Definition 2.8 (Vertex-induced subgraph) *Let $G = (V, E)$ be a graph and $V' \subseteq V$. The **subgraph induced by** V' (or spanned by V'), denoted $G[V']$, is the graph (V', E') with $E' = \{\{u, v\} \mid u, v \in V' \text{ and } \{u, v\} \in E\}$.*

Of particular interest to us will be subsets of vertices that induce complete graphs.

Definition 2.9 (Clique) *Let $G = (V, E)$ be a graph. A set $V' \subseteq V$ is called a **clique** if $G[V']$ is isomorphic to a complete graph. If $G[V'] \cong K_n$ then V' is called a n-clique or a clique of order n.*

We could have defined a clique to be a subgraph that is complete, and indeed many authors do, however it will be more useful for us to think of a clique as a set of vertices rather than the graph that it induces.

We can perform operations on graphs to create new ones. A simple example of this is taking a graph's complement which is done by replacing edges with 'non-edges' (two-element subsets of V that are not in E) and vice versa.

Definition 2.10 (Graph complement) *The **complement** a graph $G = (V, E)$ is the graph $\bar{G} = (V, E')$ where $E' = \{\{u, v\} \mid \{u, v\} \notin E\}$.*

A subgraph can be obtained by simply removing vertices along with any edges incident with those vertices. Edges may also be added or removed from a graph.

Definition 2.11 *Let $G = (V, E)$ be a graph.*

1. (Vertex deletion) *If $X \subseteq V$ then $G - X$ is the graph with vertex set $V(G - X) = V \setminus X$ and edge set $E(G - X) = \{uv \in E \mid u \notin X \text{ and } v \notin X\}$.*

2. (Edge deletion) *If $X \subseteq E$ then $G - X$ is the graph with vertex set $V(G - X) = V$ and edge set $E(G - X) = E \setminus X$.*

3. (Edge addition) *If X is a set of two-element subsets of V such that $E \cap X = \emptyset$ then $G + X$ is the graph with vertex set $V(G + X) = V$ and edge set $E(G + X) = E \cup X$.*

The graph obtained by deleting a single vertex v will be denoted by $G - v$. Graphs obtained by adding or removing a single edge uv will be denoted by $G - uv$ and $G + uv$ respectively.

Contracting a graph G on an edge uv is done by 'merging' vertices u and v; that is, replacing u and v with a single vertex that is adjacent to every vertex that was adjacent to either u or v.

Definition 2.12 (Vertex identification and edge contraction) *Given a graph $G = (V, E)$, G/uv is the graph with vertex set $V' = (V \setminus \{u, v\}) \cup \{w\}$ and edge set $E' = E_1 \cup E_2$ where $w \notin V$ is a new vertex, $E_1 = \{e \in E \mid u \notin E \text{ and } v \notin E\}$ is the set of edges not containing u or v, and $E_2 = \{\{x, w\} \mid xu \in E \text{ or } xv \in E\}$ is a new set of edges such that every vertex in V that was adjacent to either u or v is now adjacent to w. We call G/uv the graph obtained from G by identifying vertices u and v. If $uv \in E$ then we may call G/uv the graph obtained by contracting the edge uv, and denote it by G/e where $e = uv$.*

For example, cycle are constructed from paths by identifying the paths endpoints.

Example 2.13 (Cycle graph) *For any given integer $n \geq 3$, let P_{n+1} be the path of order $n + 1$ with endvertices v_1 and v_{n+1} as defined in Definition 2.5. The **cycle of order** n is the graph $C_n = P_{n+1}/v_1v_{n+1}$. The cycle C_7 is shown in figure 2.2.*

Lastly we define the operation of joining two graphs by adding edges from every vertex in the first graph to every vertex in the second graph.

Definition 2.14 (The join of two graphs) *If G and H are two graphs with disjoint vertex sets then the **join** of G and H is the graph $G + H$ that has vertex set $V(G+H) = V(G) \cup V(H)$ and edge set $E(G+H) = E(G) \cup E(H) \cup \{\{u, v\} \mid u \in V(G), v \in V(H)\}$.*

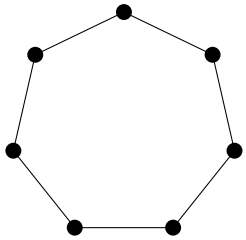

Figure 2.2: The cycle of order 7, C_7.

Example 2.15 (Wheel graph) *The* ***wheel of order*** $n \geq 4$ *is the graph* $W_n = C_{n-1} + K_1$. *The wheel of order* 8 *is shown in figure 2.3.*

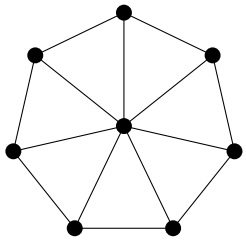

Figure 2.3: The wheel of order 8, W_8.

2.2 Graph colourings and the chromatic polynomial

The problem of 'colouring' a graph is that of assigning some set of attributes to the vertices, one to each vertex, in such a way that adjacent vertices are not assigned the same values. The terminology used reflects the historical origin of this problem, the four colour theorem.

Definition 2.16 (Graph colouring) *A (proper)* ***colouring*** *of a graph* $G = (V, E)$ *is a function* $\chi : V \to C$, *for some set* C *called the* ***palette****, such that if vertices* u *and* v *are adjacent then* $\chi(u) \neq \chi(v)$. [2] *If* $|C| = x$ *then* χ *is called an* x*-colouring. If* G *has an* x*-colouring then we say that* G *is* x*-colourable.*

A natural question to ask is; given some graph G and positive integer x, how many x-colourings will G have?

[2] The notation $\chi(G)$, where G is a graph, is often used to denote the chromatic number of a graph.

Definition 2.17 (Chromatic polynomial) *Given a graph G, the **chromatic polynomial** of G is the function $P(G;x)$ that given any positive integer x returns the number of x-colourings of G.*

Although it is not at all evident, we will show later that the function $P(G;x)$is indeed a polynomial in x (hence its name). The main object of our study will be the roots of this family of polynomials.

Definition 2.18 (Chromatic root) *If a number α is the root of some chromatic polynomial, then α is called a **chromatic root**.*

While calculation of chromatic polynomials is difficult in general, it is straightforward for complete and null graphs.

Example 2.19 (Chromatic polynomial of a complete graph) *A colouring of a complete graph must have each vertex coloured with a different colour since every pair of vertices is adjacent. Therefore the chromatic polynomial of the complete graph of order n is $P(K_n;x) = (x)_n = x(x-1)\dots(x-n+1)$.*

Example 2.20 (Chromatic polynomial of the null graph) *Since the null graph has no edges there are x choices of colour for every vertex, hence $P(\bar{K_n};x) = x^n$.*

We can write the chromatic polynomial of $G + K_n$ in terms of the chromatic polynomial of G as follows.

Example 2.21 (Chromatic polynomial of $G + K_n$) *For any graph G, we can colour $G + K_n$ by first colouring the n-clique and then colouring $V(G)$. There are $(x)_n$ ways of colouring the n-clique and since each vertex in $V(G)$ is adjacent to every vertex in the n-clique this leaves $x-n$ colours with which to colour $V(G)$. Therefore the chromatic polynomial of $G + K_n$ is $P(G;x-n)(x)_n$.*

Example 2.22 *Let H be a graph containing K_n as a subgraph. Construct a graph G from H by adding a new vertex v adjacent to very vertex in K_n (See Figure 2.4). This graph may be coloured by first colouring H and then*

colouring v, once H has been coloured using x colours, there will be $x - r$ colours available to colour v. Therefore the chromatic polynomial of G is

$$P(G; x) = (x - r)P(H; x).$$

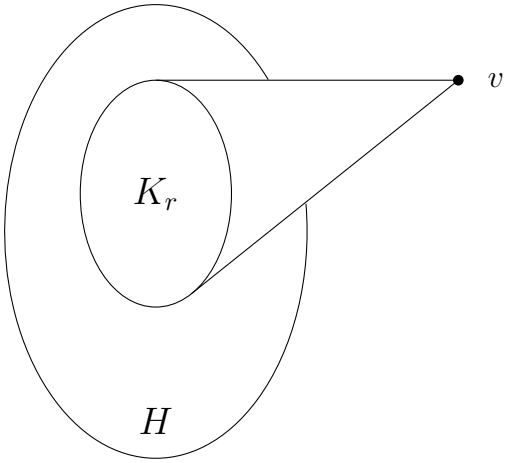

Figure 2.4

Our primary tool for calculating chromatic polynomials will be the following deletion-contraction recurrence relation.

Proposition 2.23 (Deletion-contraction relations) *Let G be a graph with vertices u and v. If $uv \in E(G)$ then*

$$P(G; x) = P(G - uv; x) - P(G/uv; x) \ . \tag{2.1}$$

This equation is called the deletion-contraction relation.

Proof. The number of colourings such that $\chi(u) = \chi(v)$ is $P(G/uv; x)$ and the number of colourings such that $\chi(u) \neq \chi(v)$ is $P(G; x)$, therefore $P(G - uv; x) = P(G; x) + P(G/uv; x)$. Rearranging gives the deletion-contraction relation. □

As an example of how we may use this result to compute chromatic polynomials, we present calculations of the chromatic polynomials of paths and cycles.

Example 2.24 (Chromatic polynomials of P_n and C_n) *First we will compute the chromatic polynomial of a path, and then we will use this result to compute the chromatic polynomial of a cycle.*

The chromatic polynomial of a path of order one is $P(P_1; x) = x$. *For any* $n > 1$, *applying the deletion-contraction relation to the graph* P_n *gives the following recursive formula*

$$\begin{aligned} P(P_n; x) &= xP(P_{n-1}; x) - P(P_{n-1}; x) \\ &= (x-1)P(P_{n-1}; x) \ . \end{aligned}$$

It follows immediately that $P(P_n; x) = x(x-1)^{n-1}$.

Now deleting an edge from a cycle yields and path of the same order, and contracting on an edge in a cycle yields another cycle with the order reduced by one. Therefore the chromatic polynomial of a cycle of order $n > 3$ *may be expressed recursively as follows*

$$\begin{aligned} P(C_n) &= P(P_n; x) - P(C_{n-1}; x) \\ &= x(x-1)^{n-1} - P(C_{n-1}; x). \end{aligned}$$

Using this recursive formula, it may be shown by induction that

$$P(C_n; x) = (x-1)^n + (-1)^n(x-1) \ .$$

Finally, we use the deletion-contraction relation to show that $P(G; x)$ is indeed a polynomial in x for every graph G.

Theorem 2.25 *For every graph* $G = (V, E)$, *the function* $P(G; x)$ *is a monic polynomial in* x *of degree* $n = |V|$ *with integer coefficients.*

Proof. Assume $E = \{e_1, e_2, \ldots, e_m\}$. Define $E_0 = \{\}$ and $E_i = E_{i-1} \cup \{e_i\}$ for $i = 1, \ldots, m$. Applying the deletion-contraction relation (2.1) to every edge in

E one derives;

$$P(G;x) = P(G-E;x) - \sum_{i=1}^{m} P\left((G-E_{i-1})/e_i;x\right)$$

Now $G - E \cong \bar{K}_n$ has chromatic polynomial x^n and each $(G - E_{i-1})/e_i$ is a graph of order at most $n-1$, so the result follows by induction on the order of G. □

From this proof we also deduce the well known result that the coefficient of x^{n-1} is $-|E|$, and that the constant term of the chromatic polynomial is zero.

Chapter 3

Algebraic number theory

In this section we introduce algebraic number theory. It is assumed that the reader is familiar with standard algebraic structures such as groups, rings, and modules, including fields, polynomial rings, and vector spaces. A more detailed overview of these can be found in [11].

We begin with the definition of a field extension, and examine some properties that a field extension exhibits. We then describe two algebraic invariants of number fields, namely the Galois group and discriminant, and their significance.

Proofs in this section will generally be brief or omitted. For more details see, for example, [20] and [1].

3.1 Field extensions

Definition 3.1 *Let F be field. An **extension** of F is a field E that contains F as a subfield; we say that E/F is a field extension.*

It is a routine exercise to check the axioms of a vector space, in order to verify the next proposition.

Proposition 3.2 *Let E/F be a field extension. The field E forms a vector space over F under multiplication by elements of F.*

This allows us to define the degree of a field extension.

Definition 3.3 *Let E/F be a field extension. The* ***degree*** *of E/F, denoted $[E : F]$, is the dimension of E viewed as a vector space over F. If the degree is finite then we say that E/F is a finite extension.*

Field extensions may have subextensions in which case we have the following useful formula for its degree.

Proposition 3.4 *If E/K and K/F are finite field extensions then E/F is a field extension with*

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

We call K an ***intermediate field****.*

Proof. If $\{\alpha_1, \ldots, \alpha_m\}$ is a basis for K over F and $\{\beta_1, \ldots, \beta_n\}$ is a basis for E over K then it is a straightforward exercise in linear algebra to show that the set $\{\alpha_i\beta_j : 1 \leq i \leq m, 1 \leq j \leq n\}$ is basis for E over F. □

The extensions E/F we will be interested in all have finite degree and consequently also have the property that every element of E is the root of a polynomial in $F[x]$.

Definition 3.5 *Let E/F be a field extension. An element $\alpha \in E$ is* ***algebraic over*** *F if it is the root of a polynomial $f(x) \in F[x]$, otherwise α is* ***transcendental*** *over F. If every element in E is algebraic over F then we say that E/F is an* ***algebraic extension****.*

Proposition 3.6 *Any finite extension E/F must be algebraic.*

Proof. Consider a finite extension E/F of degree n. For any $\alpha \in E$ the set $\{1, \alpha, \ldots, \alpha^n\}$ is linearly dependent (viewing E as a vector space over F). Therefore $c_n\alpha^n + \ldots + c_1\alpha + c_0 = 0$ for some $c_i \in F$. Dividing by c_m, where m is the largest number such that $c_m \neq 0$, shows that α is the root of a monic polynomial in $F[x]$. □

Definition 3.7 *Let E/F be a field extension.*

1. *For any $\alpha_1, \ldots, \alpha_n \in E$, the smallest extension of F that contains $\{\alpha_1, \ldots, \alpha_n\}$ is called the field obtained by adjoining $\alpha_1, \ldots, \alpha_n$ to F and is denoted by $F(\alpha_1, \ldots, \alpha_n)$. It is the intersection of all subfields of E containing $F \cup \{\alpha_1, \ldots, \alpha_n\}$.*

2. *An extension obtained by adjoining a single element is called a **simple extension**. If $E = F(\alpha)$ we call α a **primitive element**.*

A further property that a field extension may have is separability.

Definition 3.8 *A polynomial $f(x) \in F[x]$ is **separable** if it has no repeated roots. An extension E/F is separable if every element of E that is algebraic over F has a separable minimal polynomial.* [1]

At this point we state two well known facts about extensions of $\mathbb{Q}$. The first is that every finite extension of $\mathbb{Q}$ is separable , this is Corollary 39 of Section 13.5 in [11]. The second is that every finite extension of $\mathbb{Q}$ is primitive, which follows from the following theorem (Theorem 25 in Section 14.4 of [11]).

Theorem 3.9 *Every finite, separable extension is simple.*

The next proposition is fundamental to a number of subsequent results. It says that the root of an irreducible polynomial cannot be the root of any polynomial of lower degree.

Proposition 3.10 *Let F be a field and $p(x) \in F[x]$ be irreducible with a root α in some extension E of F. If $f(x) \in F[x]$ is another polynomial having α as a root then $p(x) \mid f(x)$.*

Proof. First let $m(x) \in F[x]$ be the polynomial of minimum degree having α as a root. By the Euclidean algorithm we can write $p(x) = q(x)m(x) + r(x)$ where $\deg(r(x)) < \deg(m(x))$ or $r(x) = 0$. Now $r(\alpha) = f(\alpha) - q(\alpha)m(\alpha) = 0$ so we must have $r(x) = 0$ or else the minimality of the degree of $m(x)$ is

[1] Some older texts define a polynomial to be separable if none of its irreducible factors has repeated roots. This does not affect the definition of a separable extension since a minimal polynomial has a single irreducible factor.

violated. Furthermore, since $p(x)$ is irreducible, we must have $q(x) = c \in F$. Thus $p(x)$ had minimal degree all along. Therefore if $f(x) \in F[x]$ has α as a root we use the same reasoning to show that $f(x) = q(x)p(x)$ for some $q(x) \in F[x]$. □

Corollary 3.11 *Let E/F be field extension and $\alpha \in E$ be algebraic over F. There is a unique irreducible monic polynomial in $F[x]$ that has α as a root; this polynomial is called 'the minimal polynomial of α over F' and is denoted by $\mu_{\alpha,F}(x)$ (or simply $\mu(x)$ if α and F are clear from context).*

Recall that a polynomial $p(x) \in R[x]$ is said to be irreducible over R if it has no roots in R. The following theorem demonstrates that given a polynomial $p(x)$ that is irreducible over some field F, there will always be some extension of F containing a root of $p(x)$. This is done by giving an explicit construction of the extension. This construction tells us a lot about the structure of finite extensions.

Theorem 3.12 *Let F be a field and $p(x) \in F[x]$ be irreducible and have degree n. The quotient ring $E = F[x]/\langle p(x)\rangle$ is a field. Furthermore:*

1. *There exists an embedding $\phi : F \hookrightarrow E$ and $\alpha \in E$ such that α is a root of $\phi(p(x))$.*

2. *If α is a root of $p(x)$ in any extension of F, then $E \cong F(\alpha)$.*

3. *The set $\{1, \alpha, \ldots, \alpha^{n-1}\}$ is a basis for $F(\alpha)$ as a vector space over F, therefore $[F(\alpha) : F] = n$.*

Proof. Standard results in field theory may be used to show that $\langle p(x)\rangle$ is a prime ideal and, since $F[x]$ is a principal ideal domain and $\langle p(x)\rangle$ is also a maximal ideal. Hence $E = F[x]/\langle p(x)\rangle$ is indeed a field.

It is routine to verify that the map $\phi : F \to E$ defined by setting $\phi(a) = a + \langle p(x)\rangle$ embeds F in E, and that $\alpha = x + \langle p(x)\rangle$ is a root of $\phi(p(x))$. This proves point 1.

Now suppose that α is a root of $p(x)$ in some extension of F and consider the map $\sigma : F[x] \to F(\alpha)$ defined by setting $\sigma(f(x)) = f(\alpha)$. It follows from Proposition 3.10 that $\ker(\sigma) = \langle p(x) \rangle$ and so by the First Isomorphism Theorem for rings, $\sigma(F[x])$ is a subfield of $F(\alpha)$. Clary $\sigma(F[x])$ contains F and α so $\sigma(F[x]) = F(\alpha)$ by definition. This proves point 2.

Finally, given any $f(x) \in F[x]$ we may use the Euclidean algorithm to write $f(x) = q(x)p(x)+r(x)$ where $\deg(r(x)) < \deg(p(x))$ or $r(x) = 0$. Therefore every $f(x)+\langle p(x) \rangle \in E$ can be written in the form $c_{n-1}x^{n-1}+\ldots+c_1x+c_0+\langle p(x) \rangle$ for some $c_0, \ldots, c_{n-1} \in F$. It follows from point 2 that $\{1, \alpha, \ldots, \alpha^{n-1}\}$ is a spanning set for $F(\alpha)$ over F. Moreover, this set must be linearly independent since if it was not we would have $c_{n-1}\alpha^{n-1} + \ldots + c_1\alpha + c_0 = 0$ for some $c_i \in F$ meaning that α was the root of a polynomial with degree less than $p(x)$, contradicting Proposition 3.10. □

By applying this result inductively to any factor of $p(x)$ that is still irreducible in $F(\alpha)[x]$ we conclude that there will be some extension of F containing every root of $p(x)$, that is an extension in which $p(x)$ is a product of n linear factors.

Definition 3.13

1. *Let F be a field and $f(x) \in F[x]$. We say that $f(x)$* ***splits*** *in an extension E/F if every root of $f(x)$ is contained in E.*

2. *Suppose that $f(x) \in F[x]$ splits in an extension E/F. The* ***splitting field*** *of $f(x)$ is the smallest subfield of E in which $f(x)$ splits and is denoted by $K_{f(x)}$. It follows from Definition 3.7 that if $f(x)$ has roots $\alpha_1, \ldots, \alpha_n$ then $K_{f(x)} = F(\alpha_1, \ldots, \alpha_n)$.*

The remaining results in this section concern the interplay between homomorphism and polynomials, and also the roots of those polynomials. Ring homomorphisms can be extended to polynomial ring homomorphisms in the following natural way.

Definition 3.14 *Let $\phi : R \to S$ be a ring homomorphism. The natural extension of ϕ to $R[x]$ is the homomorphism that maps $f(x) = \sum c_i x^i \in R[x]$ to $\sum \phi(c_i)x^i \in S[x]$ (it is routine to verify that this is indeed a homomorphism). For the sake of simplicity we will denote this extension using the same symbol as the original homomorphism, i.e. $\phi(f(x))$.*

Roots of polynomials are preserved by this natural extension as we would intuitively expect.

Proposition 3.15 *Let $\phi : F \to F'$ be a field homomorphism. Also let $p(x) \in F[x]$, and E be an extension of F containing a root α of $p(x)$. Define $p'(x) = \phi(p(x)) \in F'[x]$ (not to be confused with the derivative of $p(x)$) and let E' be the splitting field of $p'(x)$ over F'. If $\hat{\phi} : E \to E'$ is any homomorphism that extends ϕ, then $\hat{\phi}(\alpha)$ is a root of $p'(x)$.*

Proof. Let $p(x) = \sum c_i x^i$ where each c_i is in F. Since $\hat{\phi}$ extends ϕ, we have $\phi(c_i) = \hat{\phi}(c_i)$ for each c_i and therefore

$$\begin{aligned} p'(\hat{\phi}(\alpha)) &= \sum \hat{\phi}(c_i)\hat{\phi}(\alpha)^i \\ &= \hat{\phi}\left(\sum c_i \alpha^i\right) \\ &= \hat{\phi}(p(\alpha)) \\ &= 0 \end{aligned}$$

as required. □

Proposition 3.16 *Let F and F' be fields with an isomorphism $\phi : F \to F'$. Consider a polynomial $p(x) \in F[x]$ and define $p'(x) = \phi(p(x)) \in F'[x]$. If α is a root of $p(x)$ and α' is a root of $p'(x)$, then there exists a unique isomorphism $\hat{\phi} : F(\alpha) \to F'(\alpha')$ extending ϕ such that $\hat{\phi}(\alpha) = \alpha'$.*

Proof. We know from Theorem 3.12 that $\{1, \alpha, \ldots, \alpha^{n-1}\}$ and $\{1, \alpha', \ldots, \alpha'^{n-1}\}$ are bases for $F(\alpha)$ over F and $F'(\alpha')$ over F' respectively. Define a map $\hat{\phi}$ by

setting $\hat{\phi}(\sum c_i\alpha^i) = \sum \phi(c_i)\alpha'^i$. It is routine to verify that this is an isomorphism and also that it extends ϕ and has $\hat{\phi}(\alpha) = \alpha'$.

Now suppose that σ is another such isomorphism, then we have

$$\begin{aligned}\sigma(\sum c_i\alpha^i) &= \sum \sigma(c_i)\sigma(\alpha)^i \\ &= \sum \phi(c_i)\hat{\phi}(\alpha)^i \\ &= \hat{\phi}\left(\sum c_i\alpha^i\right).\end{aligned}$$

This demonstrates that $\hat{\phi}$ is unique. □

This last proposition is fundamental to the proof of the next result concerning the number of distinct ways in which a field isomorphism may be extended to an isomorphism of a splitting field.

Proposition 3.17 *Let F and F' be fields with an isomorphism $\phi : F \to F'$. Also let $p(x) \in F[x]$ be separable with splitting field E of degree $[E : F] = n$. If $p'(x) = \phi(p(x)) \in F'[x]$ has splitting field E' then there are exactly n isomorphisms $\sigma : E \to E'$ that extend ϕ.*

Proof. We will prove the result by induction on n. If $n = 1$ then the result is trivial. If $n > 1$ then let $\alpha \in E \setminus F$ be a root of $p(x)$. We know from Proposition 3.15 that any embedding of $F(\alpha)$ in E' must map α to a root of $p'(x)$. Let $\deg(p(x)) = \deg(p'(x)) = r$, since $p'(x)$ has distinct roots, it follows from Proposition 3.16 that there are exactly r such embeddings. Now Proposition 3.4 implies that $[E : F(\alpha)] = n/r < n$. So, by the inductive hypothesis, any embedding of $F(\alpha)$ in E' extends to n/r embeddings of E in E'. That is, each of the r embeddings of $F(\alpha)$ in E' extends to n/r embeddings of E in E' so in total there are n embeddings of E in E'. □

Corollary 3.18 *Let $F/\mathbb{Q}$ be a field extension with finite degree n. There are n distinct embeddings of F in $\mathbb{C}$ that fix $\mathbb{Q}$ pointwise.*

Definition 3.19 *Let $F/\mathbb{Q}$ and $\sigma_1, \ldots, \sigma_n$ be the n embeddings of F in $\mathbb{C}$ fixing $\mathbb{Q}$ pointwise.*

1. *An embedding such that $\sigma_i(F) \subseteq \mathbb{R}$ is called a* ***real embedding of*** *F, and an embedding such that $\sigma_i(F) \not\subseteq \mathbb{R}$ is called a* ***(proper) complex embedding of*** *F.*

2. *Let r_1 be the number of real embeddings of F and $2r_2$ the number of complex embeddings [2], (so that $r_1 + 2r_2 = n$) the ordered pair (r_1, r_2) is called the* ***signature*** *of F.*

If all the embeddings are real then F is a called a ***totally real field****, and if all the embeddings are complex then F is a called a* ***totally complex field****.*

Finally we show that a homomorphism of a field generated by a finite set is determined completely by its behaviour on the elements in that set,

Proposition 3.20 *Let F be a field, $F(\alpha_1, \ldots, \alpha_n)$ be a finitely generated extension of F, and E be any other extension of F. If $\phi_1, \phi_2 : F(\alpha_1, \ldots, \alpha_n) \to E$ are two homomorphisms that fix F pointwise and also satisfy $\phi_1(\alpha_i) = \phi_2(\alpha_i)$ for each α_i then $\phi_1 = \phi_2$.*

Proof. It is enough to prove the results for simple extensions and the result for finitely generated extensions will follow by induction on n. Suppose that $\phi_1, \phi_2 : F(\alpha) \to E$ where ϕ_1 and ϕ_2 fix F pointwise and satisfy $\phi_1(\alpha) = \phi_2(\alpha)$. Any element of $a =\in F(\alpha)$ can be written $a = c_0 + c_1\alpha + \ldots + c_k\alpha^k$ for some $c_i \in F$. Clearly then we have

$$\begin{aligned}\phi_i(a) &= \phi_i(c_0) + \phi_i(c_1)\phi_i(\alpha) + \ldots + \phi_i(c_k)\phi_i(\alpha)^k \\ &= c_0 + c_1\phi_i(\alpha) + \ldots + c_k\phi_i(\alpha)^k\end{aligned}$$

which gives the same result for both $i = 1$ and $i = 2$ since $\phi_1(\alpha) = \phi_2(\alpha)$. □

[2] The number of complex embeddings will always be even since complex conjugation is a field automorphism of $\mathbb{C}$.

3.2 The Galois group

Definition 3.21 *Let E/F be a field extension. The **Galois group** of E/F, denoted* $\mathrm{Gal}(E/F)$*, is the group of automorphisms of E that fix F pointwise. If E is the splitting field of some polynomial $f(x) \in F[x]$, then we will call* $\mathrm{Gal}(E/F)$ *the Galois group of $f(x)$.*

Proposition 3.22 *If $f(x) \in F[x]$ has n distinct roots in its splitting field $K_{f(x)}$, then* $\mathrm{Gal}(K_{f(x)}/F)$ *is isomorphic to a subgroup of S_n.*

Proof. Let $X = \{\alpha_1, \ldots, \alpha_n\}$ be the roots of $f(x)$ and $G = \mathrm{Gal}(K_{f(x)}/F)$. Taking $F' = F$ and ϕ to be the identity function in Proposition 3.15 shows that if $\tau \in G$ then $\tau(X) = X$. Now G can be embedded into S_X by the homomorphism that maps each $\tau \in G$ to $\tau|_X$, the restriction of τ to X (this map is clearly a homomorphism and by Proposition 3.20, it is also injective). Thus G is isomorphic to a subgroup of S_X which is itself isomorphic to S_n. □

3.2.1 Galois groups of polynomials over $\mathbb{Q}$

We now outline a method for determining the Galois group of a polynomial with rational coefficients, and whose degree is less than or equal to four.

Proposition 3.23 *Let $f(x) \in \mathbb{Q}[x]$ be a polynomial of degree two. The Galois group of $f(x)$ is*

$$\mathrm{Gal}(K_{f(x)}/\mathbb{Q}) \cong \begin{cases} \{1\} & \text{if } \sqrt{\Delta} \in \mathbb{Q} \\ \mathbb{Z}/2\mathbb{Z} & \text{otherwise,} \end{cases} \tag{3.1}$$

where Δ is the discriminant of $f(x)$.

If a cubic polynomial $f(x) \in \mathbb{Q}[x]$ is reducible with rational root α then it has the same Galois group as $f(x)/(x - \alpha)$. We are therefore left with irreducible cubic polynomials to consider.

Proposition 3.24 *Let $f(x) \in \mathbb{Q}[x]$ be an irreducible polynomial of degree three. Then the Galois group of $f(x)$ is*

$$\mathrm{Gal}(K_{f(x)}/\mathbb{Q}) \cong \begin{cases} A_3 & \text{if } \sqrt{\Delta} \in \mathbb{Q} \\ S_3 & \text{otherwise} \end{cases}$$

where Δ is the discriminant of $f(x)$.

To compute the Galois group of a quartic polynomial, it is helpful to first compute the Galois group of its resolvent cubic. First we note that if $f(x) = ax^n + bx^{n-1} + \ldots$ then the polynomial $f(x - b/n)$ has no x^{n-1} term (it is said to be **reduced**), furthermore it has the same Galois group as $f(x)$. Therefore it is sufficient to be a able to determine the Galois group of reduced monic polynomials in $\mathbb{Q}[x]$.

Definition 3.25 *Let $f(x) = x^4 + qx^2 + rx + s$ be a reduced, monic, quartic polynomial. The **resolvent cubic** of $f(x)$ is the polynomial*

$$g(x) = x^3 - 2qx^2 + (q^2 - 4s)x + r^2.$$

The reason this is useful is that the roots of the resolvent cubic are closely related to the roots of the original quartic. If α_1, α_2, α_3, and α_4 are the roots of $f(x)$ then the roots of $g(x)$ are u, v, and w where

$$\begin{aligned} u &= (\alpha_1 + \alpha_2)(\alpha_3 + \alpha_4) \\ v &= (\alpha_1 + \alpha_3)(\alpha_2 + \alpha_4) \\ w &= (\alpha_1 + \alpha_4)(\alpha_2 + \alpha_3)\ . \end{aligned}$$

The next proposition describes the relationship between the Galois group of a reduced quartic polynomial and its resolvent cubic.

Proposition 3.26 *Let $f(x) \in \mathbb{Q}[x]$ be a monic irreducible polynomial of degree four with resolvent cubic $g(x)$. If $G = \mathrm{Gal}(K_{g(x)}/\mathbb{Q})$ then the Galois group*

of $f(x)$ is

$$\mathrm{Gal}(K_{f(x)}/\mathbb{Q}) \cong \begin{cases} V_4 & \text{if } G \cong \{1\} \\ \mathbb{Z}/4\mathbb{Z} \text{ or } D(4) & \text{if } G \cong \mathbb{Z}/2\mathbb{Z} \\ A_4 & \text{if } G \cong A_3 \\ S_4 & \text{if } G \cong S_3. \end{cases}$$

3.3 Rings of integers

In this section we turn our attention to rings of integers. These are subrings of fields the have properties analogous to those of $\mathbb{Z}$ viewed as a subring of $\mathbb{Q}$ (for instance if a field F has ring of integers $\mathcal{O}_F$, then F is the field of fractions of $\mathcal{O}_F$). For many properties of field extensions, there are corresponding properties of rings of integers. For example, where an extension of $\mathbb{Q}$ is a vector space over $\mathbb{Q}$ (or equivalently, a $\mathbb{Q}$-module), the corresponding ring of integers is a $\mathbb{Z}$-module.

In order to be able to see these things, let's begin with some definitions.

Definition 3.27 *Let R be a commutative ring* [3]*. A **ring extension** of R is a ring S that contains R as a sub-ring; we say that S/R is a ring extension.*

Definition 3.28 *Let S/R be a ring extension.*

1. *An element $s \in S$ is **integral over** R if it is the root of a monic polynomial in $R[x]$.*

2. *An extension S/R in which every element is integral over R is called an **integral extension**.*

3. *The set of all $s \in S$ which are integral over R is called the **integral closure** of R in S.*

4. *If R is equal to its integral closure in S ,then we say that R is **integrally closed** in S.*

[3] We follow the convention that a ring is assumed to have a multiplicative identity unless stated otherwise.

Proposition 3.29 *Let S/R be a ring extension and $s \in S$. The following are equivalent:*

(1) the element s is integral over R,

(2) $R[s]$ is a finitely generated R-module, and

(3) there exists a ring R', with $s \in R'$ and $R \subseteq R' \subseteq S$, that is a finitely generated R-module.

Proof. Suppose that $s \in S$ is integral over R; then $s^n = r_{n-1}s^{n-1} + \dots r_0$ for some $n \in \mathbb{N}$ and $r_i \in R$ say. Therefore given any integer $m \geq 0$ we can show, by induction on m, that s^{n+m} can be written as an R-linear combination of elements of $\{1, \dots, s^{n-1}\}$ and so $R[s] = R\ 1 + \dots + Rs^{n-1}$ which is a finitely generated R-module. Thus (1) implies (2).

By taking $R' = R[s]$ we see that (2) implies (3).

Finally, suppose that $s \in R' = Ra_1 + \dots + Ra_n$ (where each $a_i \in R'$). Then $sa_i \in R'$ for each a_i, so there exist $r_{ij} \in R$ such that $sa_i = r_{i1}a_1 + \dots + r_{in}a_n$. Therefore s is a root of the monic polynomial $\det(x\delta_{ij} - r_{ij}) \in R[x]$ in which case (3) implies (1). □

Corollary 3.30 (Transitivity of integral extensions) *If T/S and S/R are integral extensions, then T/R is also an integral extension.*

Proof. Consider some $t \in T$. Since T is an integral extension of S there exists a positive integer n and $s_0, \dots s_{n-1} \in S$ such that $t^n + s_{n-1}t^{n-1} \dots + s_0 = 0$. Clearly t is also integral over $R[s_0, \dots, s_{n-1}]$ which is a finitely generated R-module (since each s_i is integral over R), therefore $R' = R[s_0, \dots, s_{n-1}, t]$ is a finitely generated R-module. Moreover, $R \subseteq R' \subseteq R$ and $t \in R'$ so t is integral over R by the previous result. □

Corollary 3.31 *The integral closure of R in S is an integrally closed sub-ring of S.*

Proof. Let $s, t \in S$ be integral over R; then $R[s]$ and $R[t]$ are finitely generated R modules. It follows that $R[s-t]$ and $R[st]$ are finitely generated hence $s-t$ and st are integral over R, which shows that the integral closure is a sub-ring. It follows from the previous corollary that the integral closure of R is integrally closed in S. □

We now consider integral closures of $\mathbb{Z}$ in algebraic extensions of $\mathbb{Q}$.

Definition 3.32 *Let $F/\mathbb{Q}$ be a field extension. An element $\alpha \in F$ is called an **algebraic integer** if it is integral over $\mathbb{Z}$. The integral closure of $\mathbb{Z}$ in F is called the **ring of integers** of F, and will be denoted by $\mathcal{O}_F$.*

We have a useful criterion for determining if an algebraic element of an extension of $\mathbb{Q}$ is integral in terms of that elements minimal polynomial.

Proposition 3.33 *Let $F/\mathbb{Q}$ be a field extension. An element $\alpha \in F$ is an algebraic integer if and only if α is algebraic over $\mathbb{Q}$ and its minimal polynomial belongs to $\mathbb{Z}[x]$.*

Proof. If $\alpha \in F$ is an algebraic integer then it is the root of some monic polynomial $p(x) \in \mathbb{Z}$, without loss of generality we may assume that $p(x)$ is irreducible. But $p(x)$ is also a monic irreducible polynomial in $\mathbb{Q}[x]$ so $p(x)$ must be the minimal polynomial for α. The converse is trivial. □

Recalling Corollary 3.18 regarding the number embeddings of extensions of $\mathbb{Q}$ in $\mathbb{C}$, we may define the discriminant of a $\mathbb{Q}$-basis for a finite extension of $\mathbb{Q}$.

Definition 3.34 *Let $F/\mathbb{Q}$ be a finite field extension extension of degree n. If $\mathcal{B} = \{b_1, \ldots, b_n\}$ is a basis for F over $\mathbb{Q}$ and $\sigma_1, \ldots, \sigma_n$ are the embeddings of F in $\mathbb{C}$, then the **discriminant** of $\mathcal{B}$ is $\Delta_{\mathcal{B}} = \det(\sigma_i(b_j))^2$.*

Proposition 3.35 *Let $F/\mathbb{Q}$ be a finite field extension. For every basis $\mathcal{B} = \{b_1, \ldots, b_n\}$ for F over $\mathbb{Q}$ there exists a non-zero $d \in \mathbb{Z}$ such that $\mathcal{B}' = \{db_1, \ldots, db_n\} \subseteq \mathcal{O}_F$ (and $\mathcal{B}'$ is also a basis for F over $\mathbb{Q}$).*

Proof. Since $F/\mathbb{Q}$ is finite (and therefore algebraic), every $b_i \in F$ is the root of some polynomial $p_i(x) \in \mathbb{Q}[x]$. There exists a number $d \in \mathbb{Z}$ such that for every i with $1 \leq i \leq n$, $dp_i(x)$ belongs to $\mathbb{Z}[x]$ and db_i is a root of $dp_i(x)$. Therefore each db_i is integral over $\mathbb{Z}$. □

By multiplying every element of a $\mathbb{Q}$-basis of a finite extension of $\mathbb{Q}$ by a suitable (rational) integer, we are able to show that every finite extension of $\mathbb{Q}$ has a $\mathbb{Q}$-basis contained entirely within its ring of integers.

Proposition 3.36 *Let $\mathcal{B}$ be a $\mathbb{Q}$-basis for a finite field extension $F/\mathbb{Q}$, then $\Delta_\mathcal{B} \in \mathbb{Q}$. If $\mathcal{B} \subseteq \mathcal{O}_F$ then $\Delta_\mathcal{B} \in \mathbb{Z}$.*

Proof. Let $[F : \mathbb{Q}] = n$ and $\sigma_1, \ldots, \sigma_n$ be the embeddings of F in $\mathbb{C}$. Since any embedding σ_k swaps rows of the matrix $[\sigma_i(b_j)]$ we have that

$$\begin{aligned}\sigma_k(\Delta_\mathcal{B}) &= \det(\sigma_k(\sigma_i(b_j)))^2 \\ &= (\pm \det(\sigma_i(b_j)))^2 \\ &= \Delta_\mathcal{B}.\end{aligned}$$

Since $\Delta_\mathcal{B}$ is fixed by every embedding of F in $\mathbb{C}$ it must be that $\mathbb{Q}(\Delta_\mathcal{B})$ has only one embedding in $\mathbb{C}$, therefore $\mathbb{Q}(\Delta_B) = \mathbb{Q}$. If $\mathcal{B} \subseteq \mathcal{O}_F$ then $\delta_\mathcal{B}$ $in \mathcal{O}_F$ so is the root of some polynomial in $\mathbb{Z}[x]$, however $\Delta_\mathcal{B}$ is also in $\mathbb{Q}$ so must in fact be in $\mathbb{Z}$. □

The discriminant of two bases for a finite extension of $\mathbb{Q}$ are related in the following way.

Proposition 3.37 *If $\mathcal{B}_1$ and $\mathcal{B}_2$ are $\mathbb{Q}$-bases for a finite extension $F/\mathbb{Q}$, then $\Delta_{\mathcal{B}_1} = D^2\Delta_{\mathcal{B}_2}$ for some $D \in \mathbb{Q}$.*

(The value of D is the determinant of the change of basis matrix from $\mathcal{B}_1$ to $\mathcal{B}_2$.)

As we mentioned earlier, rings of integers of extensions of $\mathbb{Q}$ will turn out to be $\mathbb{Z}$-modules. We therefore make the following definition for integral bases and then prove that these do indeed exist.

Definition 3.38 *Let $F/\mathbb{Q}$ be a field extension. A basis for $\mathcal{O}_F$ over $\mathbb{Z}$ is called an **integral basis** for F.*

Proposition 3.39 *Every finite extension of $\mathbb{Q}$ has an integral basis.*

Proof. Let $F/\mathbb{Q}$ be a finite extension of degree n. We know that F has a $\mathbb{Q}$-basis consisting only of elements of $\mathcal{O}_F$. Let $\mathcal{B} = \{b_1, \ldots, b_n\}$ be such a basis with minimal $|\Delta_{\mathcal{B}}|$. Suppose that $\mathcal{B}$ is not a $\mathbb{Z}$-basis for $\mathcal{O}_F$, so there is some $\omega \in \mathcal{O}_F$ such that if $\omega = \alpha_1 b_1 + \ldots + \alpha_n b_n$ then at least one α_i is not in $\mathbb{Z}$. We may assume without loss of generality that $\alpha_1 \notin \mathbb{Z}$. Let $r = \alpha_1 - \lfloor \alpha_1 \rfloor$ and $\mathcal{B}' = \{\omega - \lfloor \alpha_1 \rfloor b_1, b_2, \ldots, b_n\} \subseteq \mathcal{O}_F$. The matrix that maps $\mathcal{B}$ to $\mathcal{B}'$ is

$$\begin{pmatrix} r & \alpha_2 & \ldots & \alpha_n \\ 0 & 1 & \ldots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \ldots & 1 \end{pmatrix} \tag{3.2}$$

which has determinant $r \neq 0$ (so $\mathcal{B}'$ is also a basis for F). Since $0 < r < 1$ we have $|\Delta_{\mathcal{B}'}| = r^2 |\Delta_{\mathcal{B}}| < |\Delta_{\mathcal{B}}|$ contradicting the minimality of $|\Delta_{\mathcal{B}}|$. Therefore $\Delta_{\mathcal{B}}$ must have been a basis for $\mathcal{O}_F$ over $\mathbb{Z}$ all along. □

Corollary 3.40

1. *The ring of integers in $\mathcal{O}_F$ is a free $\mathbb{Z}$-module of rank n.*
2. *Any two integral bases of a finite extension $F/\mathbb{Q}$ have the same discriminant. We will call this the discriminant of the field F and denote it by Δ_F.*
3. *If $\mathcal{B} \subseteq \mathcal{O}_F$ is a $\mathbb{Q}$-basis for F and $\Delta_{\mathcal{B}} \in \mathbb{Z}$ is square-free, then $\mathcal{B}$ is a $\mathbb{Z}$-basis for $\mathcal{O}_F$.*

Proposition 3.41 *Let $f(x)$ be an irreducible polynomial in $\mathbb{Z}[x]$ with discriminant $\Delta_{f(x)}$, and let $K = K_{f(x)}$ be its splitting field with discriminant Δ_K. There exists $n \in \mathbb{Z}$ such that $\Delta_{f(x)} = n^2 \Delta_K$.*

We have the following useful formula for the sign of the discriminant of a number field.

Proposition 3.42 *Let F be a field extension of $\mathbb{Q}$ of degree n with signature (r_1, r_2). The sign of Δ_F is $(-1)^{r_2}$.*

Proof. Let $\phi_1, \ldots, \phi_n$ be the embeddings of F in $\mathbb{C}$ and $\mathcal{B} = \{b_1, \ldots, b_n\}$ be an integral basis for F. The discriminant of F is $\Delta_F = \det(\phi_i(b_j))^2$. Suppose that $\det[\phi_i(b_j)] = x + y\sqrt{-1}$ where $x, y \in \mathbb{R}$. We know that taking the complex conjugate of each embedding is the same as swapping r_2 rows in the matrix $[\phi_i(b_j)]$ so

$$x - y\sqrt{-1} = \det[\overline{\phi}_i(b_j)] = (-1)^{r_2}(x + y\sqrt{-1}) \ . \tag{3.3}$$

If r_2 is even then 3.3 becomes $x - y\sqrt{-1} = x + y\sqrt{-1}$, it follows that $y = 0$ and $\Delta_F = x^2 > 0$, If r_2 is odd then we get $x - y\sqrt{-1} = -x - y\sqrt{-1}$ which means that $x = 0$ and $\Delta_F = (y\sqrt{-1})^2 < 0$. □

Theorem 3.43 *The ring of integers $\mathcal{O}_F$, where F is a finite extension of $\mathbb{Q}$, is a Dedekind domain, i.e.*

1. *Every ideal in $\mathcal{O}_F$ is finitely generated,*
2. *Every non-trivial prime ideal in $\mathcal{O}_F$ is maximal, and*
3. *$\mathcal{O}_F$ is integrally closed in its field of fractions.*

We conclude this chapter by finding integral bases for quadratic fields and calculating their discriminants.

Example 3.44 *A quadratic number field is a degree two extension of $\mathbb{Q}$. These all have the form $\mathbb{Q}(\sqrt{D})$ where $D \neq 0, 1$ is a square-free integer. The ring of integers of $\mathbb{Q}(\sqrt{D})$ is $\mathcal{O}_{\mathbb{Q}(\sqrt{D})} = \mathbb{Z}[\omega] = \{a + b\omega : a, b \in \mathbb{Z}\}$ where*

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

The discriminant of $\mathbb{Q}(\sqrt{D})$ *is therefore*

$$\Delta_{\mathbb{Q}(\sqrt{D})} = \begin{cases} 4D & \text{if } D \equiv 2,3 \mod 4 \\ D & \text{if } D \equiv 1 \mod 4\ . \end{cases}$$

Proof. It is straightforward to show that $\mathbb{Z}[\omega]$ is a subring of $\mathcal{O}_{\mathbb{Q}(\sqrt{D})}$. Furthermore, ω is a root of $x^2 - D^2 \in \mathbb{Z}[x]$ if $D \equiv 2,3 \mod 4$ and a root of $x^2 - x + (1-D)/4 \in \mathbb{Z}[x]$ if $D \equiv 1 \mod 4$, so $\mathbb{Z}[\omega] \subseteq \mathcal{O}_{\mathbb{Q}(\sqrt{D})}$.

To show that $\mathcal{O}_{\mathbb{Q}(\sqrt{D})} \subseteq \mathbb{Z}[\omega]$, let $\alpha = a + b\sqrt{D} \in \mathcal{O}_{\mathbb{Q}(\sqrt{D})}$. If $b = 0$ then we have $\alpha \in \mathbb{Q} \cap \mathcal{O}_{\mathbb{Q}(\sqrt{D})}$, therefore $\alpha \in \mathbb{Z} \subseteq \mathbb{Z}[\omega]$. If $b \neq 0$ then α is a root of the polynomial $x^2 - 2ax + a^2 - b^2D$, so this must in fact be the minimal polynomial for α.

Proposition 3.33 implies that $2a$ and $a^2 - b^2D$ are both elements of $\mathbb{Z}$. Now we have $(2a)^2 - (2b)^2D = 4(a^2 - b^2D) \in \mathbb{Z}$ so $(2b)^2D \in \mathbb{Z}$. Suppose that $2b = n/m$ where $n, m \in Z$ and $gcd(n,m) = 1$. It follows that $n^2D/m^2 \in \mathbb{Z}$ which means that m^2 must divide D, but D is square free so it must be that $m = 1$ and therefore $2b = n \in \mathbb{Z}$. Let $a = A/2$ and $b = B/2$ where $A, B \in \mathbb{Z}$. Since $a^2 - b^2D \in \mathbb{Z}$ we must have

$$A^2 - B^2D \equiv 0 \mod 4. \tag{3.4}$$

If $D \equiv 2 \pmod 4$ then A must be even, since if A is odd then equation (3.4) becomes $1 - 2B^2 \equiv 0 \pmod 4$ which has no solutions. If A is even it follows immediately that (3.4) only holds when B is also even. If $D \equiv 3 \pmod 4$ then similar reasoning shows that both A and B must again be even. Therefore if $D \equiv 2,3 \pmod 4$ we have both a and b in $\mathbb{Z}$, so $\alpha = a + b\sqrt{D} = a + b\omega \in \mathbb{Z}[\omega]$.

If $D \equiv 1 \pmod 4$ then (3.4) becomes $A^2 - B^2 \equiv 0 \pmod 4$. This can easily be shown to have solutions only when A and B have the same parity, therefore $a - b \in \mathbb{Z}$. Hence $\alpha = a + b\sqrt{D} = (a-b) + 2b(\sqrt{D}+1)/2 = (a-b) + 2b\omega \in \mathbb{Z}[\omega]$. Thus we have shown that $\mathcal{O}_{\mathbb{Q}(\sqrt{D})} \subseteq \mathbb{Z}[\omega]$.

Now one of the two embeddings of $\mathbb{Q}(\sqrt{D})$ in $\mathbb{C}$ is the identity function,

the other is the function that maps $\sqrt{D}$ to $-\sqrt{D}$. Furthermore, we have just shown that $\{1, \omega\}$ is an integral basis for $\mathbb{Q}(\sqrt{D})$. Therefore if $D \equiv 2, 3 \pmod 4$ then

$$\Delta_{\mathbb{Q}(\sqrt{D})} = \left(\det \begin{pmatrix} 1 & \sqrt{D} \\ 1 & -\sqrt{D} \end{pmatrix} \right)^2 = 4D$$

and if $D \equiv 1 \pmod 4$ then

$$\Delta_{\mathbb{Q}(\sqrt{D})} = \left(\det \begin{pmatrix} 1 & \frac{1+\sqrt{D}}{2} \\ 1 & \frac{1-\sqrt{D}+1}{2} \end{pmatrix} \right)^2 = D \ .$$

□

Chapter 4

Background

In this chapter we will review what is currently known about some algebraic aspects of the chromatic polynomial and its roots.

First we will discuss two families of graphs which have already been studied for a long time (although not for the algebraic properties of their chromatic polynomials) for which some results are immediate.

4.1 Chordal graphs

Definition 4.1 *A cycle of length $k \geq 4$ in a graph G is said to be a* ***pure cycle*** *if it has no non-consecutive vertices that are adjacent. A graph G is called a* ***chordal graph*** *if it contains no pure cycles.*

It is known that any chordal graph can be constructed from a set of isolated vertices by recursively adding new vertices adjacent to every vertex in a clique. It follows from Example 2.22 that that the chromatic polynomial of a chordal graph must have the following form.

Proposition 4.2 *If G is a chordal graph of order n then*

$$P(G;x) = x^{r_0}(x-1)^{r_1}\dots(x-k)^{r_k}$$

where each $r_i \in \mathbb{N}$ and $k = r_0 + \ldots + r_k$.

This means that chromatic polynomials of chordal graphs only ever have integer roots. While this means that they are uninteresting from the point of view of algebraic number theory, they are noteworthy for that very reason. It was conjectured by Braun, Kretz, Walter, and Walter in 1974 that every chromatic polynomial with only integer roots belonged to a chordal graph [4], however this was disproved by Read in 1975 [19]. In fact the family of graphs discussed in Chapter 6 (bicliques) provides an infinite family of counter examples.

4.2 Cycles

We turn to an infinite family of graphs for which the calculation of the Galois group is straightforward, namely the family of cycles. Recall from Example 2.24 that the chromatic polynomial of C_n, the cycle of length n, is given by

$$\begin{aligned} P(C_n; x) &= (x-1)^n + (-1)^n(x-1) \\ &= (x-1)((x-1)^{n-1} + (-1)^n). \end{aligned}$$

Therefore $P(C_n; x)$ and $(x-1)^{n-1} + (-1)^n$ have the same splitting field which can easily be shown to be $\mathbb{Q}(e^{2\pi/(n-1)})$, the $(n-1)$-th cyclotomic field. This is well known to have Galois group over $\mathbb{Q}$ isomorphic to $(\mathbb{Z}/(n-1)\mathbb{Z})^*$ and discriminant

$$\Delta = (-1)^{\phi(n-1)/2} \frac{(n-1)^{\phi(n-1)}}{\prod_{p|n} p^{\phi(n-1)/(p-1)}},$$

where $\phi(n)$ is Euler's totient function [24].

In particular, if $n = p + 1$ where p is prime then the Galois group of $P(C_{p+1}; x)$ is the cyclic group $C(p-1)$. Hence every cyclic group of order $p-1$ where p is prime arises as the Galois group of a the splitting field of a chromatic polynomial. However there is currently no known graph with a chromatic polynomial that has a Galois group isomorphic to $C(n)$ for any odd $n \geq 5$ (Problem 2 in [15]).

4.3 Chromatic factorisation

If G is a graph with two components, H_1 and H_2, then $P(G;x) = P(H_1;x)P(H_2;x)$. Furthermore, such a factorisation is only possible if G is not connected (this follows from the fact the number of components in a graph is equal to the multiplicity of the root zero in its chromatic polynomial). Thus factorisation of chromatic polynomials in the usual sense is not particularly interesting.

Definition 4.3 *A graph G is said to be **clique-separable** if it can be constructed by identifying cliques of size r in graphs H_1 and H_2 (See Figure 4.1).*

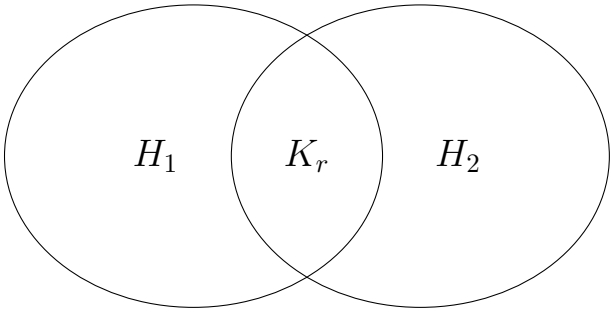

Figure 4.1

Proposition 4.4 *The chromatic polynomial of such a graph way is then given by*

$$P(G;x) = \frac{P(H_1;x)P(H_2;x)}{P(K_r;x)} \quad . \tag{4.1}$$

Proof. For $i = 1, 2$, let $n_i(x)$ be the number of x-colourings of the vertices in $V_i = V(H_i) \setminus V(K_r)$, given that the vertices in $V(K_r)$ have already been coloured. The chromatic polynomial of H_i can then be written $P(H + i; x) = n_i(x)P(K_r;x)$. Now the graph G may be coloured by first colouring the vertices in $V(K_r)$ and then colouring the vertices in each of the V_i. Since $V_1 \cap V_2 = \emptyset$ we have

$$P(G;x) = P(K_r;x)n_1(x)n_2(x) = \frac{P(H_1;x)P(H_2;x)}{P(K_r;x)} \ .$$

□

In [16], Morgan and Farr survey all chromatic polynomials of graphs with 10 or fewer edges and make the following observations. There exist graphs that are not clique-separable but are chromatically equivalent to clique-separable graphs, these are called *quasi-clique-separable*, (graphs that are neither clique-separable or quasi-clique-separable are called *strongly non-clique-separable*). Furthermore, there exist strongly non-clique-separable graphs with chromatic polynomials of the form (4.1). This latter observation in particular suggests that the following, slightly more general, notion of factorisability is worthy of further study.

Definition 4.5 *The chromatic polynomial of a graph G is said to have a chromatic factorisation of order r if it is of the form (4.1) for some graphs H_1 and H_2, both non-isomorphic to K_r. Likewise, a graph G is said to have chromatic a factorisation of order r if its chromatic polynomial has a factorisation of order r.*

Any clique-separable graph clearly has a chromatic factorisation and this can be easily explained from its structure, i.e. the existence of a clique that is a vertex cut-set. The relationship between structure and chromatic factorisation for non-clique-separable graphs is far from clear however. Morgan and Farr [16] introduce the concept of a *certificate of factorisation* in order explain the factorisation of strongly non-clique-separable graphs..

A certificate of factorisation for a graph G is a finite sequence of rational functions of indeterminates, where the indeterminates represent chromatic polynomials, starting with $P(G;x)$ and ending with $P(H_1;x)P(H_2;x)/P(K_r;x)$. Each pair of consecutive elements in the sequence is accompanied by a *certification step*, a rule that explains why the two rational functions are equivalent. The different certification steps are all applications of one of the following:

- The deletion-contraction and addition-identification relations.
- The formula (4.1) for the chromatic polynomial of a clique separable graph.

- An application of the axioms of the field of rational functions.
- Definition of chromatically equivalent graphs.

A certificate that does not include steps of this last type, i.e. one that does not rely on two graphs being chromatically equivalent to explain the factorisation, is called an "extended certificate of factorisation".

It is then shown that every strongly non-clique-separable that has chromatic factorisation has an extended certificate of factorisation with a finite number of steps, and that the number of steps has an upper bound of $n^2 2^{n/2}$ where n is the order of the graph. That is, the factorisation can be explained by a finite number of r-gluings, applications of the addition-identification relations, and applications of the axioms of the field of rational functions. Extended certificates for all factorisable, strongly non-clique separable graphs of order 9 or less are then computed and all are found to have fewer than 57 steps.

4.4 Theta graphs

The graph θ_{a_1,a_2,a_3} is constructed by taking three paths of length a_1, a_2, and a_3 (i.e. of order a_1+1, a_2+1, and a_3+1) and identifying the start vertices of each path and also the end vertices of each path. In [9] Delbourgo and Morgan calculate the Galois groups of θ_{a_1,a_2,a_3} in two cases.

1. **All paths have equal length.** For every integer $a \geq 2$, the Galois group of $P(\theta_{a,a,a}; x)$ is the symmetric group $S_{3(a-1)}$.
2. **Path lengths are three consecutive integers.** For every integer $a \geq 2$ the Galois group of $P(\theta_{a,a+1,a+2}; x)$ is $(\mathbb{Z}/(a^2+a)\mathbb{Z})^* \times C(2) \times S_{a-1}$ if $a \equiv 1 \pmod 3$, and is $(\mathbb{Z}/(a^2+a)\mathbb{Z})^* \times S_{a+1}$ otherwise.

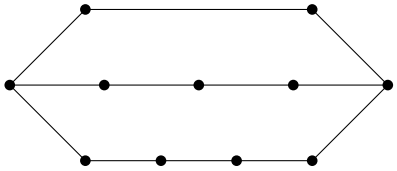

Figure 4.2: The graph $\theta_{3,4,5}$.

4.5 The algebraic nature of chromatic roots

Since chromatic polynomials are always monic and have integer coefficients, it is clear that chromatic roots are always algebraic integers. However it is also clear from the existence of root free intervals that not all algebraic integers are chromatic roots. In [8], Peter Cameron made two conjectures concerning the algebraic nature of chromatic roots.

The first, known as the "$n\alpha$ conjecture", says that if α is a chromatic root then so is $n\alpha$ for every natural number n. This has been shown to be true for an infinite family of graphs called clique-theta graphs [2].

The second, the "$\alpha + n$ conjecture", says that for every algebraic integer α, there is a natural number n such that $\alpha + n$ is a chromatic root. This has been proven to be true for quadratic and cubic integers [2], and will be the focus of Chapters 6 and 7.

Chapter 5

The family $\{G_{p,r}\}$

In [15] Morgan found infinite families of graphs with Galois groups A_3, $\mathbb{Z}/4\mathbb{Z}$, and $D(4)$, each arising from the family of graphs $\{G_{p,q,r}\}$ (see Definition 5.2).

In this chapter we will compute the Galois group of the chromatic polynomial for all graphs in this family for $p \leq 5$ and in doing so confirm that Conjecture 1 in [15] is true. It is helpful to recognise that it is actually only necessary to compute the Galois groups for the chromatic polynomials of a two-parameter sub-family of graphs. To see this let's define the graphs in question.

Definition 5.1 *For integers $p \geq 1$ and $r \geq 1$, let K_r be the complete graph of order r and $v_0, v_1, \ldots, v_p$ be vertices not in $V(K_r)$. The graph $G_{p,r}$ is constructed from K_r and $v_0, v_1, \ldots, v_p$ by adding edges $\{v_0, v_i\}$ and $\{v_i, u\}$ for every $u \in V(K_r)$ and i with $1 \leq i \leq p$.*

Each graph $G_{p,q,r}$ can now be defined in terms of a graph $G_{p',r'}$ for some p' and r'.

Definition 5.2 *For any $p \geq 1$, $q \geq 0$, and $r \geq q+2$*

$$G_{p,q,r} = G_{p,r-q-1} + K_q \ .$$

We see from this definition that $P(G_{p,q,r}; x)$ has the same splitting field as $P(G_{p,r-q-1}; x)$. For the remainder of this chapter we will be concerned with

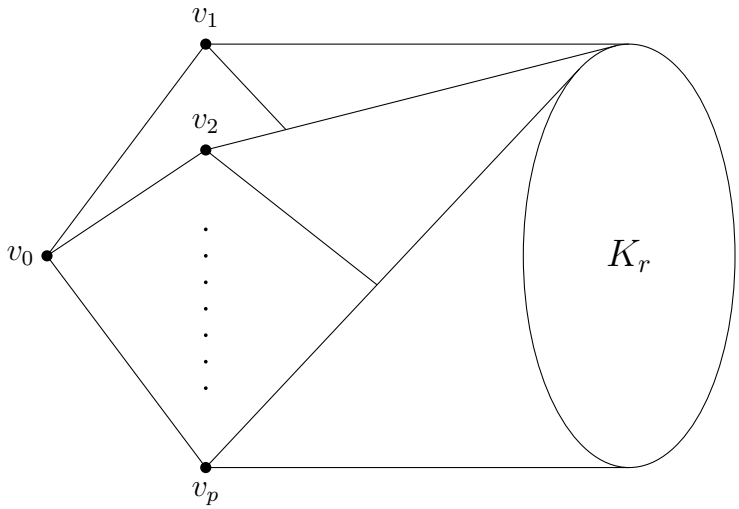

Figure 5.1: The graph $G_{p,r}$

computing the Galois group of every $P(G_{p,r};x)$ for $p \leq 5$. Once this has been done we will also have determined the Galois group of every $P(G_{p,q,r};x)$ for $p \leq 5$. The following conjecture about the Galois groups of chromatic polynomials of graphs in the family $\{G_{4,q,r}\}$ was made in [15]

Conjecture 5.3 *The family of graphs* $\{G_{4,q,r}\}$ *where* $q \geq 0$, $r \neq c^3+4c^2+q+1$ *for any* $c \in \mathbb{N}$, *and* $r \notin \{4,9,10\}$, *is a family of Galois equivalent graphs with each graph having a chromatic polynomial with Galois group* S_4.

First we need to find an expression for the chromatic polynomial of $G_{p,r}$. A detailed derivation of $P(G_{p,r};x)$ can be found in [15], here we provide an informal argument.

Proposition 5.4 *The chromatic polynomial of* $G_{p,r}$ *is*

$$P(G_{p,r};x) = (x)_{r+1}\ g_{p,r}(x)$$

where

$$g_{p,r}(x) = (x-r-1)^p + r(x-r)^{p-1}\ .$$

Proof. There are $(x)_r$ ways of colouring $V(K_r)$. For each of these colourings there are $(x-r)(x-r-1)^p$ ways of colouring $v_0,\ldots,v_p$ such that

$\chi(v_0) \notin \chi(V(K_r))$ and $r(x-r)^p$ ways of colouring $v_0, \ldots, v_p$ such that $\chi(v_0) \in \chi(V(K_r))$. Therefore

$$\begin{aligned} P(G_{p,r}; x) &= (x)_r \left((x-r)(x-r-1)^p + r(x-r)^p\right) \\ &= (x)_{r+1} \left((x-r-1)^p + r(x-r)^{p-1}\right). \end{aligned}$$

□

5.1 The Galois group of $P(G_{p,r}; x)$

Instead of computing the Galois group of $P(G_{p,r}; x)$ directly, we associate with each $G_{p,r}$ a polynomial with a simpler form than $P(G_{p,r}; x)$ which has the same splitting field.

Proposition 5.5 *For each $p \in \mathbb{Z}$ and $r \in \mathbb{Z}$ define the polynomial*

$$R_{p,r}(x) = x^p + (-1)^p rx + (-1)^p r \ . \tag{5.1}$$

If $p \geq 1$ and $r \geq 1$ then $R_{p,r}(x)$ has the same splitting field as $P(G_{p,r}; x)$.

Proof. For $p \geq 1$ and $r \geq 1$ we can define $R_{p,r}(x)$ in terms of $g_{p,r}(x)$ as follows:

$$R_{p,r}(x-1) = (-1)^p x^p g_{p,r}\left(\frac{1}{x} + r\right) \ . \tag{5.2}$$

The following calculation shows that this definition is equivalent to (5.1):

$$\begin{aligned} R_{p,r}(x-1) &= (-1)^p x^p \left(\left(\frac{1}{x} - 1\right)^p + r\left(\frac{1}{x}\right)^{p-1}\right) \\ &= (-1)^p x^p \left(\sum_{i=0}^{p} \binom{p}{i} (-1)^{i-p} \left(\frac{1}{x}\right)^i + r\left(\frac{1}{x}\right)^{p-1}\right) \\ &= \sum_{i=0}^{p} \binom{p}{i} (-1)^i x^{p-i} + (-1)^p rx \\ &= (x-1)^p + (-1)^p r(x-1) + (-1)^p r \ . \end{aligned}$$

It is clear from (5.2) that $R_{p,r}(x)$ has the same splitting field as $g_{p,r}(x)$ and therefore has the same splitting field as $P(G_{p,r};x)$ also. □

Proposition 5.6 *For all graphs $G_{p,r}$, the polynomial $R_{p,r}(x)$ has a rational root if and only if $r = 2^p$.*

Proof. Let n be a rational root of $R_{p,r}(x)$ for some p and r, then we must have

$$(-1)^{p+1}r = \frac{n^p}{n+1} = n^{p-1} - n^{p-2} + \ldots + (-1)^{p+1} + \frac{(-1)^p}{n+1} .$$

This is an integer if and only if $n = 0$ or $n = -2$. If $n = 0$ then $r = 0$ (which does not correspond to a graph) and if $n = -2$ then $r = 2^p$. □

The Galois group of $P(G_{2,r};x)$ can be determined immediately.

Corollary 5.7 (Galois group of $P(G_{2,r};x)$) *The Galois group of $P(G_{2,r};x)$ is trivial if $r = 4$ and is $\mathbb{Z}/2\mathbb{Z}$ otherwise.*

5.1.1 The Galois group of $P(G_{3,r};x)$

Theorem 5.8 *For any graph $G_{3,r}$ the Galois group of $P(G_{3,r};x)$ over $\mathbb{Q}$ is $\mathbb{Z}/2\mathbb{Z}$ if $r = 8$, A_3 if $r = c^2 + c + q + 7$ for some $c \in \mathbb{Z}$, and S_3 otherwise.*

Proof. If $r = 8$ then $R_{3,r}(x) = x^3 - 8x - 8 = (x+2)(x^2 - 2x - 4)$, which has an irreducible quadratic factor, so the Galois group is $\mathbb{Z}/2\mathbb{Z}$.

If $r \neq 8$ then $R_{3,r}(x)$ is irreducible (Proposition 5.6). The discriminant of $R_{3,r}(x)$ is $\Delta = r^2(4r - 27)$. The discriminant is a square if and only if $4r - 27 = n^2$ for some $n \in \mathbb{Z}$, analysis of this modulo 2 reveals that we must have $n = (2c+1)^2$ and therefore $r = c^2 + c + 7$ for some $c \in \mathbb{Z}$ (we note that that $\Delta > 0$ for every r of this form). Hence if $r = c^2 + c + 7$ for some $c \in \mathbb{Z}$ then Δ is a positive square number and the Galois group is A_3, otherwise the Galois group is S_3. □

5.1.2 The Galois group of $P(G_{4,r}; x)$

Lemma 5.9 *For all graphs $G_{4,r}$ with $r \neq 16$, the polynomial $R_{4,r}(x)$ is irreducible over $\mathbb{Q}$.*

Proof. Proposition 5.6 shows that for $r \neq 16$, if $R_{4,r}(x)$ is to be reducible over $\mathbb{Q}$ then it must have a quadratic factor. Suppose that $x^2 + Ax + B$ is a factor of $R_{4,r}(x)$ for some $r \in \mathbb{Z}$ and $A, B \in \mathbb{Q}$. The remainder of $R_{4,r}(x)$ on division by $x^2 + Ax + B$ is

$$(2AB - A^3 + r)x + B^2 - A^2B + r.$$

Setting the remainder to zero leads to a quadratic equation in B,

$$B^2 - (A^2 + 2A)B + A^3 = 0.$$

This will have rational solutions only if the discriminant $\Delta = A^2(A^2 + 4)$ is square. The discriminant is only square when $A = 0$ in which case we have $r = 0$ which does not correspond to a graph. Therefore $R_{4,r}(x)$ is irreducible for all graphs $G_{4,r}$ with $r \neq 16$. □

Lemma 5.10 *The resolvent cubic of $R_{4,r}(x)$, $f(x) = x^3 - 4rx + r^2$, has a rational root if and only if $r = c^3 + 4c^2$ for some $c \in \mathbb{Z}$. Moreover, $f(x)$ has only one rational root in this case.*

Proof. Suppose that n is a rational root of the resolvent cubic. Solving the equation $n^3 - 4rn + n^2 = 0$ for r yields

$$r = 2n \pm n\sqrt{4 - n}\ . \tag{5.3}$$

Since r is an integer we must have $n = 4 - m^2$ for some $m \in \mathbb{Z}$, substituting

this into (5.3) we see that

$$\begin{aligned} r &= 2n + n\sqrt{4-n} \\ &= m^2 - 2m^2 - 4m + 8 \\ &= c^3 + 4c^2 \end{aligned}$$

where $c = m - 2$ (taking $r = 2n - n\sqrt{4-n}$ leads to the same set of solutions). Now if we take $r = c^3 + 4c^2$ then

$$f(x) = \left(x - (c^2 + 4c)\right)\left(x^2 - (c^2 + 4c)x + (c^4 + 4c^3)\right) \ .$$

The discriminant of the quadratic term is $\Delta = c^2(c+4)(4-3c)$. Now $\Delta \geq 0$ if and only if $-f \leq c \leq 4/3$, the only integers in this interval for which Δ is square are $c = -4$ and $c = 0$ and in both cases $r = 0$. Therefore, if $r \geq 1$ then $f(x)$ can have at most one rational root and this occurs when r has the form $r = c^3 + 4c^2$. □

Corollary 5.11 *The Galois group of the resolvent cubic of $R_{4,r}(x)$ is $\mathbb{Z}/2\mathbb{Z}$ if $r = c^3 + 4c^2$ for some $c \in \mathbb{Z}$ and is S_3 otherwise.*

Proof. From lemma 5.10 we can conclude that the Galois group is $\mathbb{Z}/2\mathbb{Z}$ if $r = c^3 + 4c^2$. We just need to determine the Galois group if $r \neq c^3 + 4c^2$, that is if $f(x)$ is irreducible.

The resolvent cubic has discriminant $\Delta = r^2(256r - 27r^2)$. If $r \geq 10$ then $\Delta < 0$ and the Galois group of $f(x)$ is S_3. It remains to determine the Galois group for those values of r with $0 < r < 10$ and $r \neq c^3 + 4c^2$, that is $r \in \{1, 2, 4, 6, 7\}$. For each of these values of r, Δ is positive and non-square so again the Galois group is S_3. □

Lemma 5.12 *The polynomial $R_{4,r}(x)$ has exactly two roots if and only if $r \geq 10$.*

Proof. The polynomial $R_{4,r}(x)$, viewed as a real valued function, has a local

minimum at $x = -\sqrt[3]{r/4}$ and no other extrema. It can easily be verified that $R_{4,r}(-\sqrt[3]{r/4}) < 0$ if and only if $r \geq 10$ (for integer values of r). □

Theorem 5.13 *The Galois group of $P(G_{4,r}; x)$ is $\mathbb{Z}/4\mathbb{Z}$ if $r = 5$, S_3 if $r = 16$, $D(4)$ if $r = c^3 + 4c^2$ and $r \neq 5$, and S_4 otherwise.*

Proof. If $r = 16$ then $R_{4,r}(x) = (x + 2)(x^3 - 2x^2 + 4x + 8)$, the cubic term has a negative discriminant so the Galois group is S_3.

If $r \neq 16$ and $r \neq c^3 + 4c^2$ then $R_{4,r}(x)$ is irreducible and the Galois group of its resolvent cubic is S_3, therefore the Galois group of $R_{4,r}(x)$ is S_4.

If $r = c^3 + 4c^2$ then $R_{4,r}(x)$ is irreducible (since $r \neq 16$) and the Galois group of its resolvent cubic is $\mathbb{Z}/2\mathbb{Z}$, so the Galois group of $R_{4,r}(x)$ is either $\mathbb{Z}/4\mathbb{Z}$ or $D(4)$. Now a quartic polynomial with rational coefficients and exactly two real roots has Galois group $D(4)$ or S_4 so for $r \geq 10$ the Galois group of $R_{4,r}(x)$ is $D(4)$. It remains to check the cases where $r < 10$ and $r = c^3 + 4c^2$, that is $r \in \{3, 5, 8, 9\}$. Computing the Galois group for the remaining values of r using the function `polgalois(F)` in PARI/GP [17] reveals that the Galois group is $D(4)$ in each case except $R_{4,5}$ which has Galois group $\mathbb{Z}/4\mathbb{Z}$. □

We note that this result, along with Definition 5.2, proves Conjecture 5.3.

5.1.3 The Galois group of $P(G_{5,r}; x)$

It is not known if there exists a graph with a chromatic polynomial that has Galois group $\mathbb{Z}_5$. In this section we show that the family of graphs $\{G_{5,r}\}$ do not answer this question (therefore neither does the family $\{G_{5,q,r}\}$) by showing that the Galois group of $P(G_{5,r}; x)$ is always isomorphic to S_5 (with one exception).

Lemma 5.14 *For all graphs $G_{5,r}$ with $r \neq 32$, the polynomial $R_{5,r}(x)$ is irreducible over $\mathbb{Q}$.*

Proof. If $r \neq 32$ then $R_{5,r}(x)$ does not have a rational root, therefore if it reducible it must have a quadratic factor. Suppose that $x^2 + Ax + B$ is a factor

for some $A, B \in \mathbb{Q}$. The remainder of $R_{5,r}(x)$ when divided by $x^2 + Ax + B$ is

$$(A^4 - 3BA^2 + B^2 - r)x + A^3B - 2AB^2 - r.$$

The remainder is zero if and only if

$$(2A + 1)B^2 - (A^3 + 3A^2)B + A^4 = 0.$$

Viewing this as a quadratic equation in B, we will have rational solutions if and only if the discriminant $\Delta_B = A^4(A^2 - 2A + 5)$ is square. Now Δ_B is square if and only if $A^2 + 2A + 5 - m^2 = 0$ for some $m \in \mathbb{Q}$. This quadratic equation in A has discriminant $\Delta_A = 4(m^2 - 4)$ which is square only when $m = 2$. Setting $m = 2$ leads to the conclusion that $R_{5,r}(x)$ has a quadratic factor only when $r = -1$ which does not correspond to a graph. □

Lemma 5.15 *If $r \geq 13$ then $R_{5,r}(x)$ has exactly three real roots.*

Proof. If we view $R_{5,r}(x) = x^5 - rx - r$ as a real valued function then it can be shown to have a local maximum at $x = -\sqrt[4]{r/5}$ and a local minimum at $x = \sqrt[4]{r/5}$ (and no other extrema). Therefore $R_{5,r}(x)$ has exactly three real roots when

$$R_{5,r}\left(-\sqrt[4]{\frac{r}{5}}\right) > 0 \quad \text{and} \quad R_{5,r}\left(\sqrt[4]{\frac{r}{5}}\right) < 0. \tag{5.4}$$

Now

$$R_{5,r}\left(-\sqrt[4]{\frac{r}{5}}\right) = r\left(4 \times 5^{5/4} r^{1/4} - 1\right)$$

and

$$R_{5,r}\left(\sqrt[4]{\frac{r}{5}}\right) = -r\left(4 \times 5^{5/4} r^{1/4} + 1\right)$$

so, assuming $r \geq 1$, the inequalities in (5.4) are satisfied if and only if $r > \frac{5^5}{4^4} = 12\frac{53}{526}$. □

Theorem 5.16 *The Galois group of $R_{5,r}(x)$ is S_4 if $r = 32$ and is S_5 otherwise.*

Proof. If $r = 32$ then $R_{5,r}(x) = (x+2)(x^4 - 2x^3 + 4x^2 - 8x - 16)$, the quartic factor can be shown to have Galois group S_4 (using PARI/GP for example).

If $r \geq 13$ then $R_{5,r}(x)$ has three real roots and a pair of complex roots, therefore its Galois group has a 2-cycle that fixes the real roots and transposes the complex roots. Furthermore, since $R_{5,r}(x)$ has degree five, its Galois group must be isomorphic to a subgroup of S_5 and must also contain a 5-cycle. It is a well known fact in Group theory that a 2-cycle and a 5-cycle generate a group isomorphic to S_5.

It can be checked using PARI/GP that the polynomials $R_{5,r}(x)$ for $r \in \{1, \ldots, 12\}$ also have Galois group S_5. □

Chapter 6

Bicliques and the $\alpha + n$ conjecture

In this chapter we will define a family of graphs called bicliques and discuss some of their properties in relation to their use for proving the $\alpha+n$ conjecture. We will then prove that the $\alpha+n$ is true for quadratic and cubic integers using this family of graphs.

6.1 Bicliques

Definition 6.1 (Biclique) *A graph $G = (V, E)$ is called a* biclique *if V can be written as the set union of two disjoint cliques*[1]*. If G is a biclique such that $G[V_1] \cong K_j$ and $G[V_2] \cong K_k$, where $V = V_1 \cup V_2$ and $V_1 \cap V_2 = \emptyset$, then G is said to be a biclique of degree (j, k) or a (j, k)-biclique. (Note that a biclique may have more than one degree.)*

For any biclique with cliques V_1 and V_2 let $N_{G,V_1} : \mathcal{P}^+(V_1) \to \mathbb{Z}$ be the function such that for every non-empty $X \subseteq V_1$, $N_{G,V_1}(X)$ is the number of vertices in V_2 that are adjacent to at least one vertex in X. (We use the notation $\mathcal{P}^+(S)$ to denote the non-empty subsets of S.)

[1]The term 'biclique' is more commonly used to refer to a complete bipartite graph.

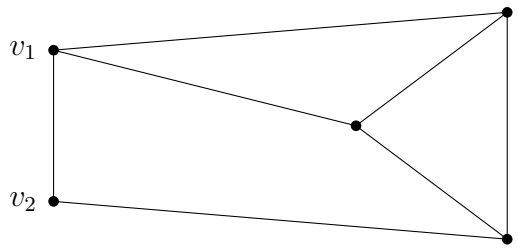

Figure 6.1: A $(2,3)$-biclique with 2-clique $\{v_1, v_2\}$ and parameters $N(\emptyset) = 0$, $N(v_1) = 1$, $N(v_2) = 2$, and $N(v_1, v_2) = 3$.

The chromatic polynomial of a biclique is calculated in [3] using a generalisation of the Möbius function to locally finite posets. Here it is proven inductively using the deletion-contraction relation.

Theorem 6.2 (Chromatic polynomial of a biclique) *Let $G = (V, E)$ be a biclique with degree (j, k) and j-clique V. The chromatic polynomial of G is*

$$P(G; x) = (x)_k(-1)^j \sum_{\rho \leq \{V\}} (-1)^{|\rho|} \prod_{\sigma \in \rho} (|\sigma| - 1)! \, (x - N_{G,V}(\sigma)) \,. \tag{6.1}$$

Here the notation $\rho' \leq \rho$ means that ρ' is a refinement of the partition ρ, so the sum is over partitions ρ of V.

Proof. For any positive integer n let $V_n = \{v_1, v_2, \ldots, v_n\}$. We will assume that the vertices in the j-clique are labelled $v_1, \ldots, v_j$, i.e. $V = V_j$, and that $N = N_{G,V}$.

First $P(G; x)$ will be expressed in terms of chromatic polynomials of $(j - 1, k)$-bicliques. Let $E_0 = \{\}$ and $E_i = E_{i-1} \cup \{v_i v_j\}$ for $i = 1, \ldots, j - 1$. Applying deletion-contraction to every edge in E_{j-1} yields

$$P(G; x) = P(G - E_{j-1}; x) - \sum_{i=1}^{j-1} P((G - E_{i-1})/v_i v_j; x)$$

Consider the graph $(G - E_{i-1})/v_i v_j$ for some fixed i. Let u be the new vertex that replaces v_i and v_j. In the graph $G - E_{i-1}$ every pair of vertices in V_j that does not include either v_i or v_j is adjacent; also v_i is adjacent to every other vertex in V_j. Therefore, in the graph $(G - E_{i-1})/v_i v_j$, every pair of vertices

in $(V \cup \{u\}) \setminus \{v_i, v_j\}$ is adjacent. Furthermore $N(u)$ has the same value as $N(v_i, v_j)$ in G, and $N(v_\ell)$ remains the same for every $v_\ell \notin \{v_i, v_j\}$. Thus $(G - E_{i-1})/v_iv_j$ is the same graph as the $(j-1,k)$-biclique G/v_iv_j. The graph $G - E_{j-1}$ clearly has chromatic polynomial $(x - N(v_j))P(G - v_j)$. Moreover $G - v_j$ is also a $(j-1,k)$-biclique, so we have

$$P(G;x) = (x - N(v_j))P(G - v_j;x) - \sum_{i=1}^{j-1} P(G/v_iv_j;\, x) \tag{6.2}$$

and we may now proceed by induction on j.

The formula (6.1) evaluated when $j = 1$ gives $(x - N(v_1))(x)_k$ which is the chromatic polynomial of a $(1,k)$-biclique.

Let $j > 1$. Assuming that (6.1) holds for $j-1$, the first term of (6.2) is

$$\begin{aligned}
&(x - N(v_j))P(G - v_j;x) \\
&\quad = (x - N(v_j))(x)_k(-1)^{j-1} \sum_{\rho \le \{V_{j-1}\}} (-1)^{|\rho|} \prod_{\sigma\in\rho} (|\sigma| - 1)!\,(x - N(\sigma)) \\
&\quad = (x)_k(-1)^{j-1} \sum_{\rho \le \{V_{j-1}, \{v_j\}\}} (-1)^{|\rho|-1} \prod_{\sigma\in\rho} (|\sigma| - 1)!\,(x - N(\sigma))\,. \qquad (6.3)
\end{aligned}$$

This is a sum over every partition ρ of V_j such that the part of ρ that contains v_j contains no other vertices.

Assuming (6.1) holds for $j-1$, the chromatic polynomial of G/v_jv_j is

$$(-1)^{j-1} \sum_{\rho \le \{V_{j-1}\}} (-1)^{|\rho|} \prod_{\substack{\sigma\in\rho \\ v_i\notin\sigma}} (|\sigma| - 1)!\,(x - N(\sigma)) \prod_{\substack{\sigma\in\rho \\ v_i\in\sigma}} (|\sigma| - 1)!\,(x - N(\sigma \cup \{v_j\}))\,.$$

For each partition ρ of V_{j-1} let $f_i(\rho)$ be the partition of V_j obtained by adding v_j to the part of ρ that contains v_i. The chromatic polynomial of G/v_jv_j can now be written as

$$(-1)^{j-1} \sum_{\rho \le \{V_{j-1}\}} (-1)^{|\rho|} \prod_{\substack{\sigma\in f(\rho) \\ v_j\notin\sigma}} (|\sigma| - 1)!\,(x - N(\sigma)) \prod_{\substack{\sigma\in f(\rho) \\ v_j\in\sigma}} (|\sigma| - 2)!\,(x - N(\sigma))$$

hence the term $-\sum_{i=1}^{j-1} P(G/v_iv_j;\, x)$ in (6.2) becomes

$$(-1)^j \sum_{\rho \leq \{V_{j-1}\}} \sum_{i=1}^{j-1} (-1)^{|\rho|} \prod_{\substack{\sigma \in f(\rho) \\ v_j \notin \sigma}} (|\sigma|-1)!\,(x - N(\sigma)) \prod_{\substack{\sigma \in f(\rho) \\ v_j \in \sigma}} (|\sigma|-2)!\,(x - N(\sigma))\,.$$

Let ρ be a partition of V_j such that the part containing v_j contains at least one other vertex. We can write $\rho = f_i(\rho')$ for exactly one choice of ρ' and $|\sigma|-1$ choices of i, where σ is the part of ρ that contains v_j. Thus $-\sum_{i=1}^{j-1} P(G/v_iv_j;\, x)$ can be written in terms of partitions of V_j:

$$\begin{aligned}
&(-1)^j \sum_{\substack{\rho \leq \{V_j\} \\ \rho \not\leq \{V_{j-1}, \{v_j\}\}}} (-1)^{|\rho|} \prod_{\substack{\sigma \in \rho \\ v_j \notin \sigma}} (|\sigma|-1)!\,(x - N(\sigma)) \prod_{\substack{\sigma \in \rho \\ v_j \in \sigma}} (|\sigma|-1)\,(|\sigma|-2)!\,(x - N(\sigma)) \\
&= (-1)^j \sum_{\substack{\rho \leq \{V_j\} \\ \rho \not\leq \{V_{j-1}, \{v_j\}\}}} (-1)^{|\rho|} \prod_{\sigma \in \rho} (|\sigma|-1)!\,(x - N(\sigma))\,. \qquad (6.4)
\end{aligned}$$

This is a sum over every partition ρ of V_j such that the part of ρ that contains v_j contains at least one other vertex. Adding together (6.3) and (6.4) gives the desired result.

□

We will present proofs of the $\alpha + n$ conjecture (for quadratic and cubic integers) by proving the following conjecture for polynomials of degree less than or equal to three.

Conjecture 6.3 *For every monic polynomial $p(x) \in \mathbb{Z}[x]$ there exists a biclique G and non-negative integer n such that $p(x-n)$ is a factor of $P(G;x)$.*

We shall give a more complete description than in [3] of those bicliques for which $p(x-n)$ is a factor for any given $p(x)$, and also include an upper bound on the minimum value of n necessary.

First let us take a closer look at the chromatic polynomial of a biclique.

6.2 Chromatic polynomials of bicliques

Recall, by Theorem 6.2, that the chromatic polynomial of a (j,k)-biclique with j-clique V is

$$P(G;x) = (x)_k(-1)^j \sum_{\rho \leq \{V\}} (-1)^{|\rho|} \prod_{\sigma \in \rho} (|\sigma| - 1)! \, (x - N_{G,V}(\sigma)) \, .$$

We want $p(x-n)$ to be a factor of $P(G;x)$ for every monic $p(x) \in \mathbb{Z}[x]$. For polynomials that are irreducible over $\mathbb{Z}$ the term $(x)_k$, being composed only of linear factors, will play no role. Therefore we designate the remaining factor of $P(G;x)$ to be the 'interesting factor'.

Definition 6.4 *Let G be a (j,k)-biclique with j-clique V. The interesting factor of G with respect to V is the degree j polynomial*

$$g(G;V;x) = (-1)^j \sum_{\rho \leq \{V\}} (-1)^{|\rho|} \prod_{\sigma \in \rho} (|\sigma| - 1)! \, (x - N_{G,V}(\sigma)) \, . \tag{6.5}$$

The interesting factor of a biclique depends only on $N_{G,V}(X)$ for each subset X of V. We use this observation as a basis for the following generalisation of a biclique.

Definition 6.5 (Semi-biclique)

1. *A semi-biclique of degree n is an ordered pair $B = (V,N)$ where V is a set of size n and N is a function $N : \mathcal{P}^+(V) \to \mathbb{Z}$.*

2. *The interesting factor of a semi-biclique $B = (V,N)$ is the polynomial*

$$g(B;x) = (-1)^{|V|} \sum_{\rho \leq \{V\}} (-1)^{|\rho|} \prod_{\sigma \in \rho} (|\sigma| - 1)! (x - N(\sigma)). \tag{6.6}$$

The question arises: from which semi-bicliques are we able to construct a biclique with the same interesting factor?

Proposition 6.6 *Let $B = (V, N_B)$ be a semi-biclique of degree j. Define a function $M_B : \mathcal{P}^+(V) \to \mathbb{Z}$ by setting*

$$M_B(X) = \sum_{\substack{\bar{X} \subseteq Y \subseteq V \\ Y \neq \bar{\emptyset}}} (-1)^{|\bar{X}|+|Y|+1} N_B(Y) \tag{6.7}$$

for each non-empty subset X of V (and define $M_{G,V}$ for bicliques in the same way).

There exists a (j,k)-biclique G with j-clique V such that $N_{G,V} = N_B$ if and only if

$$M_B(X) \geq 0 \text{ for every non-empty } X \subseteq V. \tag{6.8}$$

Proof. It is a routine exercise to show that if $\mathcal{F} = \{S_i \mid i \in I\}$ is a family of sets indexed by a finite set I, then

$$\left| \bigcap_{i \in I} S_i \right| = \sum_{\emptyset \subsetneq J \subseteq I} (-1)^{|J|+1} \left| \bigcup_{j \in J} S_j \right|.$$

Using this result, along with the identity $|A \cap \bar{B}| = |A \cup B| - |B|$, it can be shown that for any non-empty $J \subseteq I$

$$\left| \left(\bigcap_{j \in J} S_j \right) \cap \left(\bigcap_{j \in \bar{J}} \bar{S}_j \right) \right| = \sum_{\bar{J} \subseteq K \subseteq I} (-1)^{|\bar{J}|+|K|+1} \left| \bigcup_{k \in K} S_k \right|.$$

Consider a (j,k)-biclique G with j-clique V. Let us construct a family of subsets of the k-clique indexed by V; one defines S_v to be the set of vertices in the k-clique that are adjacent to v (so $N_{G,V}(X) = |\bigcup_{v \in X} S_v|$). We see that for any non-empty $X \subseteq V$,

$$M_{G,V}(X) = \left| \left(\bigcap_{v \in X} S_v \right) \cap \left(\bigcap_{v \in \bar{X}} \bar{S}_v \right) \right|.$$

In other words, $M_{G,V}(X)$ counts the number of vertices in the k-clique that are adjacent to every vertex in X but not adjacent to any other vertex in V. Therefore (6.8) is both a necessary and sufficient condition for a semi-

biclique B to exhibit in order to be able to construct a biclique G such that $N_{G,V}(X) = N_B(X)$. □

If condition (6.8) is satisfied for a semi-biclique B then we can legitimately say that B is a biclique.

Recall that in Definition 2.14 we defined the graph $G + K_n$. We can generalise this operation to semi-bicliques in the following way:

Definition 6.7 (Integer shifted semi-biclique)

1. *For any function $N : \mathcal{P}^+(V) \to \mathbb{Z}$ and integer n, let "$N + n$" be the function defined by setting $(N + n)(X) = N(X) + n$ for each non-empty $X \subseteq V$.*

2. *If $B = (V, N_B)$ is a semi-biclique then define $B + n = (V, N_B + n)$.*

It is easy to see that if G is a (j, k)-biclique with j-clique V and we view $G+n$ as a $(j, k + n)$-biclique (also with j-clique V), then $N_{G+n,v} = N_{G,v} + n$. This shows that the operation $B + n$ corresponds to $G + n$ for those semi-bicliques with interesting factors arising as interesting factors of bicliques. We can use this operation to state Conjecture 6.3 in terms of semi-bicliques.

Proposition 6.8 *Conjecture 6.3 is equivalent to the prediction that for every monic polynomial $p(x) \in \mathbb{Z}[x]$ there exists a semi-biclique $B = (V, N)$ such that $g(B; x) = p(x)$ and $M_B(X) \geq 0$ for every X such that $\emptyset \subsetneqq X \subsetneqq V$.*

Proof. It can be shown that the equalities

$$g(B + n; x) = g(B; x - n) \tag{6.9}$$

and

$$M_{B+n}(X) = \begin{cases} M_B(X) & \text{if } \emptyset \subsetneqq X \subsetneqq V \\ M_B(X) + n & \text{if } X = V \end{cases} \tag{6.10}$$

both hold for every semi-biclique B and integer n. Let $p(x) \in \mathbb{Z}[x]$ be an arbitrary monic polynomial and B be a semi-biclique with $g(B;x) = p(x)$. Suppose that $M_B(X) \geq 0$ for every X such that $\emptyset \subsetneqq X \subsetneqq V$; equation (6.10) implies that there will exist a non-negative integer n such that $B + n$ is a biclique, and equation (6.9) implies that the interesting factor of $B + n$ is $p(x - n)$. Following similar reasoning, we discover that every biclique with interesting factor $p(x - n)$ arises in this way. □

6.3 Quadratic integers

We will now fully describe the bicliques G and non-negative integers n such that $g(G;x) = p(x - n)$, in the case where $p(x)$ is a quadratic polynomial. Let $p(x) = x^2 + C_1x + C_0$ for some arbitrary $C_1, C_0 \in \mathbb{Z}$, and denote the discriminant and roots of $p(x)$ by Δ, ω_-, and ω_+. Also let n be a non-negative integer, $\Omega = 4n + \Delta - 2C_1 - 3$, and define $\Gamma \subseteq \mathbb{R}$ as follows:

$$\Gamma = \begin{cases} \emptyset & \text{if } \Omega < 0 \\ \left[\frac{-C_1-1-\sqrt{\Omega}}{2}, \frac{-C_1-1+\sqrt{\Omega}}{2}\right] & \text{if } \Omega \geq 0, \Delta \leq 0 \\ \left[\frac{-C_1-1-\sqrt{\Omega}}{2}, \frac{-C_1-1+\sqrt{\Omega}}{2}\right] \setminus (\omega_-, \omega_+) \setminus (\omega_- - 1, \omega_+ - 1) & \text{if } \Omega \geq 0, \Delta > 0. \end{cases}$$

Theorem 6.9 *If G is a $(2,k)$-biclique with 2-clique $V_2 = \{v_1, v_2\}$ then $g(G;x) = p(x - n)$ if and only if*

$$\begin{aligned} N(v_1) &= n - i - (C_1 + 1) \\ N(v_2) &= i + n \\ N(v_1, v_2) &= i^2 + (C_1 + 1)i + C_0 + n. \end{aligned} \tag{6.11}$$

for some integer $i \in \Gamma$.

Moreover, such an i is guaranteed to exist if $n \geq n_0$ where the number

$$n_0 = \begin{cases} \frac{1}{4}(2C_1 + 3 - \Delta) & \text{if } \Delta \leq 0 \\ \frac{1}{2}(C_1 + 3\sqrt{\Delta} + 6) & \text{if } \Delta > 0 \end{cases}$$

Proof. In light of Proposition 6.8, we begin by finding a semi-biclique B such that $g(B;x) = p(x)$. The interesting factor of a semi-biclique $B = (V_2, N)$ with $N(v_1) = a_1$, $N(v_2) = a_2$, and $N(v_1, v_2) = a_{12}$ is

$$g(B;x) = x^2 - (a_1 + a_2 + 1)x + a_1 a_2 + a_{12}$$

Equating coefficients of $g(B;x)$ and $p(x)$ then rearranging, we find that if $g(B;x) = p(x)$ one must have

$$\begin{aligned} a_1 &= -a_2 - (C_1 + 1) \\ a_{12} &= a_2^2 + (C_1 + 1)a_2 + C_0. \end{aligned}$$

Setting $a_2 = i$ and applying the result of Proposition 6.8 shows that N must have the form given in (6.11) for some integer i.

By Proposition 6.6, for $g(B;x)$ to be the interesting factor of a biclique we require that

$$\begin{aligned} M(v_1) = \quad & a_{12} - a_2 && = i^2 + C_1 i + C_0 \geq 0 \\ M(v_2) = \quad & a_{12} - a_1 && = i^2 + (C_1 + 2)i + C_1 + C_0 + 1 \geq 0 \\ M(v_1, v_2) = \quad & a_1 + a_2 - a_{12} && = -i^2 - (C_1 + 1)i + n - C_1 - C_0 - 1 \geq 0 \end{aligned} \tag{6.12}$$

Now the quadratic $M(v_1)$ has discriminant Δ, and roots ω_- and ω_+; similarly $M(v_2)$ has discriminant Δ, and roots $\omega_- - 1$ and $\omega_+ - 1$; and lastly $M(v_1, v_2)$ has discriminant Ω, and roots $\frac{1}{2}(-C_1 - 1 \pm \sqrt{\Omega})$. Therefore we obtain the

equivalences

$$\begin{aligned} M(v_1) \geq 0 &\Leftrightarrow \Delta \leq 0 \text{ or } i \notin (\omega_-, \omega_+) \\ M(v_2) \geq 0 &\Leftrightarrow \Delta \leq 0 \text{ or } i \notin (\omega_- - 1, \omega_+ - 1) \\ M(v_1, v_2) \geq 0 &\Leftrightarrow \Omega \geq 0 \text{ and } i \in \left[\frac{-C_1 - 1 - \sqrt{\Omega}}{2}, \frac{-C_1 - 1 + \sqrt{\Omega}}{2}\right]. \end{aligned}$$

Combining these together we find that $M(v_1)$, $M(v_2)$, and $M(v_1, v_2)$ are all non-negative if and only if $i \in \Gamma$.

For $\Delta \leq 0$, there is guaranteed to be an integer $i \in \Gamma$ if $\Omega \geq 1$; rearranging this gives $n \geq \frac{1}{4}(2C_1 + 3 - \Delta)$. For $\Delta > 0$, there is guaranteed to be an integer $i \in \Gamma$ if $\Omega \geq 1$ and $\frac{1}{2}(-C_1 - 1 + \sqrt{\Delta}) - \omega_+ \geq 1$; rearranging the second inequality gives $n \geq \frac{1}{2}(C_1 + 3\sqrt{\Delta} + 6)$, and for positive Δ this implies that $\Omega \geq 1$. Therefore if $n \geq n_0$ then Γ will have a non-trivial intersection with $\mathbb{Z}$, as required. □

We may use this result to determine the Galois group of the interesting factor.

Proposition 6.10 *Let G be a $(2, k)$-biclique with 2-clique $V_2 = \{v_1, v_2\}$. The splitting field of the interesting factor over $\mathbb{Q}$ has the trivial Galois group if and only if*

$$\begin{aligned} M(v_1) &= st \\ M(v_2) &= (s+1)(t+1) \end{aligned}$$

for some non-negative integers s and t. The Galois group is S_2 otherwise.

Proof. The Galois group of a quadratic polynomial can only be trivial or S_2. The Galois group of the interesting factor is trivial if and only if the interesting factor splits over $\mathbb{Z}$, that is if

$$g(G; x) = (x - \alpha)(x - \beta) = x^2 + (\alpha + \beta)x + \alpha\beta$$

for some integers α and β. Taking $C_1 = \alpha + \beta$ and $C_0 = \alpha\beta$ in (6.12) yields

$$\begin{aligned} M(v_1) &= i^2 + (\alpha + \beta)i + \alpha\beta \\ &= (i + \alpha)(i + \beta) \\ M(v_2) &= i^2 + (\alpha + \beta + 2)i + \alpha\beta + \alpha + \beta + 1 \\ &= (i + \alpha + 1)(i + \beta + 1) \end{aligned}$$

Setting $s = i + \alpha$ and $t = i + \beta$ and noting that this corresponds to a biclique only when s and t are both non-negative completes the proof. $\square$

6.4 Cubic integers

For cubic polynomials it is harder to describe all bicliques G and non-negative integers n such that $g(G;x) = p(x-n)$; we present here an infinite set of solutions and explain briefly how they were found.

Theorem 6.11 *Let $p(x) = x^3 + C_2x^2 + C_1x + C_0$ be an arbitrary monic polynomial in $\mathbb{Z}[x]$ and $V_3 = \{v_1, v_2, v_3\}$. For each set of integers i, j, k, l define a semi-biclique $B = (V_3, N)$ by setting parameters*

$$\begin{aligned}
N(v_1) &= -6i - j - 2C_2 - 3 \\
N(v_2) &= 6i + C_2 \\
N(v_3) &= j \\
N(v_1, v_2) &= 12i^2 + (12j + 20C_2 + 18)i + j^2 + (2C_2 + 3)j \\
&\qquad - 2k - 2l + 2C_2^2 + 3C_2 - C_2C_1 - C_0 \\
N(v_1, v_3) &= 12i^2 + 2k + C_1 + 1 \\
N(v_2, v_3) &= 12i^2 - (6j + 2C_2)i + 2l + C_2 + C_2C_1 + C_0 \\
N(v_1, v_2, v_3) &= 18i^2 + (-6j^2 - (8C_2 + 9)j - 6k + 6l \\
&\qquad + 3C_2C_1 - 2C_2^2 - 3 + 3C_0 - 3C_1)i \\
&\quad - \frac{1}{2}j^3 - \frac{1}{2}(C_2 + 3)j^2 \\
&\quad + (k + 2l + \frac{1}{2}C_2 + C_2C_1 + C_0)j \\
&\quad - C_2k + (2C_2 + 3)l \\
&\quad + C_2^2C_1 + C_2^2 + C_2C_0 + C_2C_1 + C_2 + C_0.
\end{aligned} \tag{6.13}$$

Moreover, for every choice of $j, k, l \in \mathbb{Z}$ there exists an integer i and non-negative integer n, such that $B + n$ is a biclique and $g(B + n; x) = p(x - n)$.

Proof. We begin by finding semi-bicliques $B = (V_3, N)$ such that $g(B;x) = p(x)$. Let $N(v_1) = a_1$, $N(v_2) = a_2$, $N(v_2) = a_1$, $N(v_1, v_2) = a_{12}$, $N(v_1, v_3) =$

a_{13}, $N(v_2, v_3) = a_{23}$, and $N(v_1, v_2, v_3) = a_{123}$. The interesting factor of B is

$$\begin{aligned} g(B; x) = x^3 &- (a_1 + a_2 + a_3 + 3)x^2 \\ &+ (a_1 + a_2 + a_3 + a_1a_2 + a_1a_3 + a_2a_3 + a_{12} + a_{13} + a_{23} + 2)x \\ &- (a_1a_2a_3 + a_1a_{23} + a_2a_{13} + a_3a_{12} + 2a_{123}). \end{aligned}$$

So we see that $g(B; x) = p(x)$ if and only if

$$\begin{aligned} a_1 &= -a_2 - a_3 - (C_2 + 3) \\ a_{12} &= -(a_2 + a_3)(a_2 + a_3 + C_2 + 3) - a_{13} - a_{23} + C_2 + C_1 \\ a_{123} &= \frac{1}{2}\big(-a_3^3 - (C_2 + 3)a_3^2 + (2a_{23} + a_{13} - C_2 - C_1 - 1)a_3 \\ &\quad + (C_2 + 3)a_{23} + a_2(a_{23} - a_{13}) - C_0\big). \end{aligned} \tag{6.14}$$

This expression for a_{123} has integer values provided

$$\begin{aligned} a_2 &\equiv C_2 && \pmod 2 \\ a_{13} &\equiv C_1 + 1 && \pmod 2 \\ a_{23} &\equiv C_2(C_1 + 1) + C_0 && \pmod 2 \end{aligned} \tag{6.15}$$

Recall that if $B + n$ is to be a biclique for some n then we must have $M(X) \geq 0$ for every X such that $\emptyset \subsetneqq X \subsetneqq V_3$ (Proposition 6.8). In other words, we require

$$\begin{aligned} M(v_1) &= a_{123} - a_{23} \geq 0 \\ M(v_2) &= a_{123} - a_{13} \geq 0 \\ M(v_3) &= a_{123} - a_{12} \geq 0 \\ M(v_1, v_2) &= -a_{123} + a_{13} + a_{23} - a_3 \geq 0 \\ M(v_1, v_3) &= -a_{123} + a_{12} + a_{23} - a_2 \geq 0 \\ M(v_2, v_3) &= -a_{123} + a_{12} + a_{13} - a_1 \geq 0. \end{aligned} \tag{6.16}$$

If we make the substitutions in (6.14) and also set $a_{13} = Aa_2^2$ and $a_{23} - a_{13} = Ba_2$, then the coefficients of a_2^2 in the inequalities in (6.16) are

$$\begin{aligned}
&\frac{1}{2}A(3a_3 + C_2 + 1) + \frac{1}{2}B \\
&\frac{1}{2}A(3a_3 + C_2 + 7) + \frac{1}{2}B + 1 \\
-&\frac{1}{2}A(3a_3 + C_2 - 1) - \frac{1}{2}B \\
-&\frac{1}{2}A(3a_3 + C_2 + 5) - \frac{1}{2}B + 1
\end{aligned}$$

and none of them has any higher order terms in a_2. By making suitable choices for A and B, we can make all of these positive (e.g. $A = \frac{1}{3}$ and $B = -a_3 - \frac{1}{3}C_2$). Therefore, if such a choice is made for A and B, then each $M(X)$ will be positive for large values of a_2. For any integers i, j, k, l the substitutions

$$\begin{aligned}
a_2 &= 6i + C_2 \\
a_3 &= j \\
a_{13} &= 12i^2 + 2k + C_1 + 1 \\
a_{23} &= 12i^2 - (6j + 2C_2)i + 2l + C_2(C_1 + 1) + C_0
\end{aligned} \tag{6.17}$$

satisfy the congruences in (6.15) and also have $a_{13} \sim \frac{1}{3}a_2^2$ and $a_{23} - a_{13} \sim -a_2(a_3 + \frac{1}{3}C_2)$, so the coefficient of i^2 in each $M(X)$ in (6.16) is guaranteed to be positive.

Now the substitutions in (6.14) together with those in (6.17) give the function N defined in (6.13), so the semi-biclique $B = (V_3, N)$ has $g(B; x) = p(x)$. In addition, for any integers j, k, and l, there will be some integer i such that $M(X) \geq 0$ for every X such that $\emptyset \subsetneqq X \subsetneqq V_3$. Therefore, by Proposition 6.8, given any $j, k, l \in \mathbb{Z}$ there will be an integer i and non-negative integer n, such that $B + n$ is a biclique with $g(B; x) = p(x - n)$. □

From these results, it seems plausible that the Conjecture 6.3 can also be proved for algebraic integers of higher degree using bicliques. This will be further supported by the computational evidence in the next chapter. However

solving the inequalities given by equation (6.8) presents quite a challenge. If for quartic integers we follow the same method that we have used for quadratic and cubic integers, we arrive at a system of 14 polynomial inequalities in 11 variables. Currently the best known method for solving such a system is 'cylindrical algebraic decomposition', which implemented by the software QEPCAD-B [5] [13]). However the computational complexity of this method is doubly exponential in the number of variables and is therefore unsuitable for such a large system.

Chapter 7

Computational search results for $(4, k)$- and $(5, k)$-bicliques

In this chapter we will provide computational evidence that every quartic and quintic extension of $\mathbb{Q}$ arises as the splitting field of the chromatic polynomial of a graph. Specifically we investigate the following conjecture, a weakened form of Conjecture 6.3, in the cases where $j = 4$ and $j = 5$.

Conjecture 7.1 *For every algebraic extension $F/\mathbb{Q}$ that is the splitting field of a polynomial in $\mathbb{Q}[x]$ of degree j, there exists a (j, k)-biclique G such that F is the splitting field of $P(G; x)$.*

We note that this conjecture has been proven to be true for $j = 2$ and $j = 3$ in the previous chapter.

Before describing the computation we wish to perform we will discuss some constraints we will place on bicliques in our search. Let G be a (j, k)-biclique with j-clique V_j and $M(V_j) = n$ (that is, there are n vertices in the k-clique adjacent to every vertex in the j clique). Such a biclique is actually isomorphic to $H + K_n$ where H is a $(j, k - n)$-biclique, it follows from Example 2.21 that $P(G; x)$ and $P(H; x)$ have the same splitting fields. Therefore in our search we only need to look for bicliques that have $M(V_j) = 0$. Furthermore, the interesting factor of a (j, k)-biclique does not depend on k, we are free to choose any value so long as $k \geq N(V_j)$. We will therefore assume that $k = N(V_j)$.

Now in such a biclique, the number of birding edges (that is, edges with one end vertex in the j-clique and the other end-vertex in the k-clique) is $k = V(V_j)$, the total number of vertices is $j+k$ and the total number of edges is $\binom{j}{2}+k+\binom{k}{2}$. If we take j to be fixed, the these are monotonically increasing functions of k. Therefore if a (j,k)-biclique (with the constraints we have outlined) is the (j,k)-biclique with the fewest bridging edges to have a certain property, then it is also the smallest in terms of size (number of vertices) and order (number of edges) to have that property. With this understanding we will simply refer to a biclique as being the 'smallest' biclique to have a certain property, this will mean it has both the fewest edges and the fewest vertices.

Now we will outline the nature of the evidence we need to support this conjecture and then propose a method for finding it.

Complete tables of quartic number fields F such that $|\Delta_F| \leq 10^6$ are available from

`ftp://pari.math.u-bordeaux1.fr/pub/pari/packages/nftables`

and details of their construction may be found in [6], [7], and [12]. Also available are complete tables of quintic number fields with $|\Delta_F| \leq 10^6$ (and $|\Delta_F| \leq 2 \times 10^7$ for completely real fields), their constructions are described in [18]. T

he tables are essentially lists of irreducible quartic and quintic polynomials, each with a distinct splitting field, and our goal is to reconstruct these tables using interesting factors of bicliques.

The method we use to construct tables of bicliques with interesting factors that have distinct splitting fields is outlined in Algorithm 1. This algorithm will find all unique algebraic extensions of $\mathbb{Q}$ arising as splitting fields of irreducible interesting factors of (j,k)-bicliques with a given number of bridging edges and fixed value of j. The function `nfdisc(f)` is a PARI/GP function that computes the discriminant of the splitting fields of a given polynomial. The

function `polredabs(f)` is also a PARI/GP function, given a polynomial $f(x)$ it returns a polynomial with the same splitting field such that if $K_{f(x)} \cong K_{g(x)}$ are isomorphic then `polredabs(f(x))` and `polredabs(f(x))` will return the same value. This is the function we use to determine if two bicliques have interesting factors with the same splitting fields.

Algorithm 1: Finds all number fields of given degree that arise as splitting fields of chromatic polynomials of bicliques.

Input: The degree of the number field to search for, j; the number of bridging edges in the bicliques that will be searched, k; the minimum and maximum number field discriminants, $minDisc$ and $maxDisc$.

Output: Every number field of degree j, and discriminant Δ such that $minDisc \leq \Delta \leq maxDisc$, that arises as the splitting field of a (j,k)-biclique with $M(V_j) = 0$ and $N(V_j) = k$ (whereV_j is the j-clique), and an example of such a biclique for each field.

```
1  R ← ∅
2  foreach (j,k)-biclique G with N(V_j) = k and M(V_j) = 0 do
3      g(x) ← g(G;x)
4      if g(x) is irreducible then
5          Δ ← nfdisc(g(x))
6          if minDisc ≤ Δ ≤ maxDisc then
7              r(x) ← polredabs(g(x))
8              if r(x) ∉ R then
9                  R ← R ∪ {r(x)}
10                 print(G)
```

Thus to construct a complete table of fields arising as splitting fields of irreducible interesting factors of fixed degree j, and with discriminant within certain bounds, we run Algorithm 1 with increasing values of k until the required number of distinct fields has been found (since we know *a priori* how may fields there are to find). Of course this process will only stop if Conjecture 7.1 is indeed true. Fortunately our results provide strong evidence that it is.

It is worth noting that the most computationally intensive part of this algorithm is the calculation of the reduced polynomial by `polredabs(f)`. Therefore widening the range of field discriminants we consider significantly increases the time it takes for the program to run.

With this in mind, we give a second algorithm, Algorithm 2, that will search for bicliques with interesting factors that have the same splitting field as a given polynomial, say $p(x)$. Since for each interesting factor $g(x)$ we only need to compute the reduced polynomial if $\Delta_{K_{g(x)}} = \Delta_{K_{p(x)}}$, the number of calls to `nfdisc(f)` is greatly reduced.

We may increase the speed of the algorithm further by noting , by Proposition 3.41, that we can only have $\Delta_{K_{g(x)}} = \Delta_{K_{p(x)}}$ if $\Delta_{K_{p(x)}} \mid \Delta_{g(x)}$. The value of $\Delta_{K_{p(x)}}$ only needs to be computed once and the calculation of the polynomial discriminant is much quicker than the calculation of the field discriminant.

Furthermore, the sign of the polynomial discriminant is the same as the sign of the field discriminant so if we are searching for fields with a specific signature we may use Proposition 3.42 to further increase the speed of the search. In practice, Algorithm 2 is quicker to run once there are fewer than $\sim 10^3$ splitting fields left to find to construct a complete table.

Algorithm 2: Searches for bicliques with interesting factors that have that have the same splitting field as a given polynomial.

Input: An irreducible polynomial $p(x)$ and the number of bridging edges in the bicliques that will be searched, k.

Output: Bicliques G of degree (j, k) with $N(V_j) = k$ and $M(V_j) = 0$ (where $j = \deg(p(x))$ such that $K_{g(G;x)} \cong K_{p(x)}$.

```
1  Δ_{K_p} ← nfdisc(p(x))
2  r(x) ← polredabs(p(x))
3  j ← deg(p(x))
4  foreach (j,k)-biclique G with N(V_j) = k and M(V_j) = 0 do
5      g(x) ← g(G;x)
6      Δ_g ← poldisc(g(x))
7      if Δ_{K_p} | Δ_g then
8          Δ_{K_g} ← nfdisc(g(x))
9          if Δ_{K_g} = Δ_{K_p} then
10             q(x) ← redpolabs(g(x))
11             if q(x) = r(x) then
12                 print(G)
```

7.1 Results for $(4, k)$-bicliques

By generating $(4, k)$-bicliques randomly with $0 \leq M(X) \leq 25$ for each $X \subseteq V_4$ (where V_4 is the 4-clique), we have found for every quartic field F with $|\Delta_F| \leq 10^6$ a $(4, k)$-biclique whose interesting factor has F as its splitting field. The largest of these bicliques has 284 bridging edges. We are therefore able to conclude the following.

Proposition 7.2 *Every quartic field F with $|\Delta_F| < 10^6$ arises as the splitting field of a $(4, k)$-biclique with fewer than 4×10^6 edges and 300 vertices.*

For quartic fields with $|\Delta_F| \leq 10^5$ we are able to do considerably better, these all occurred as the splitting field of the chromatic polynomial of a $(4, k)$-biclique in an exhaustive search of all $(4, k)$-bicliques with up to 31 bridging edges.

Proposition 7.3 *Every quartic field F with $|\Delta_F| < 10^5$ arises as the splitting field of a $(4, k)$-biclique with no more than 502 edges and 36 vertices.*

Because the search for fields with $|\Delta_F| < 10^5$ was exhaustive, this means that we have actually determined the smallest biclique that has each of the given fields occurring as the splitting field of its chromatic polynomial.

7.2 Results for $(5, k)$-bicliques

For quintic number fields we performed separate searches for each possible signature.

For quintic fields with signature $(1, 2)$ we performed exhaustive searches of $(5, k)$-bicliques with up to 14 bridging edges, and further non-exhaustive searches up to 22 bridging edges, and found every non-real quintic number field F with $|\Delta_F| \leq 10^6$ to be the splitting field of at least one of the interesting factors.

Proposition 7.4 *Every quintic field F with $|\Delta_F| < 10^6$ and signature $(1, 2)$ or $(3, 1)$ is the splitting field of a $(5, k)$-biclique with no more than 263 edges and 27 vertices.*

Totally real quintic fields are much rarer (of the 62,533 fields with $|\Delta_F| \leq 10^6$, only 414 are totally real) and required larger $(5,k)$-bicliques to construct a complete table. A non-exhaustive search of bicliques with up to 35 bridging edges found all totally real quintic number fields with discriminant $|\Delta_F| \leq 10^6$.

Proposition 7.5 *Every quintic field F with $|\Delta_F| \leq 10^6$ and signature $(5,0)$ is the splitting field of a $(5,k)$-biclique with no more than 640 edges and 40 vertices.*

It is of particular interest that these searches revealed $(5,k)$-bicliques with interesting factors having Galois group $C(5)$ since, as we mentioned in Section 4.2, this Group was not previously known to be the Galois group of the chromatic polynomial of any graph. There are 5 quintic number fields with Galois group $C(5)$ and discriminant $|\Delta_F| \leq 2 \times 10^7$. None of these arose as the splitting field of the interesting factors of any bicliques in an exhaustive search of all $(5,k)$-bicliques with 17 or fewer bridging edges (using Algorithm 2).

Proposition 7.6 *The $(5,k)$-biclique with parameters given in Table 7.1 has 181 edges, 23 vertices and interesting factor $g(x) = x^5 - 65x^4 + 1679x^3 - 21530x^2 + 136953x - 345421$. The Galois group of this interesting factor is $C(5)$. There is no smaller $(5,k)$-biclique, either in terms of size or order, to have an interesting factor with splitting field having Galois group $C(5)$ and $|\Delta_F| \leq 2 \times 10^7$.*

However not every possible Galois group for a totally real quintic field arises as the Galois group of a totally real quintic field with $|\Delta_F| \leq 10^6$. Specifically, the Galois groups A_5 and $F(5)$ only arise as Galois groups of real quintic fields with $|\Delta_F| > 10^6$). Using Algorithm 2 we have found $(5,k)$-bicliques having interesting factors with real splitting fields and Galois groups A_5 and $F(5)$. Table 7.1 gives the parameters of a $(5,k)$-biclique with interesting factor $g(x) = x^5 - 43x^4 + 747x^3 - 6544x^2 + 28846x - 51038$ which has Galois group

	Galois group		
	$C(5)$	A_5	$F(5)$
$X \subseteq V_5$	$N(X)$		
$\{v_1\}$	4	2	4
$\{v_2\}$	7	8	8
$\{v_3\}$	13	5	10
$\{v_4\}$	14	7	15
$\{v_5\}$	17	11	18
$\{v_1, v_2\}$	9	9	11
$\{v_1, v_3\}$	16	6	12
$\{v_1, v_4\}$	16	8	15
$\{v_1, v_5\}$	17	12	19
$\{v_2, v_3\}$	16	10	13
$\{v_2, v_4\}$	17	11	18
$\{v_2, v_5\}$	18	12	19
$\{v_3, v_4\}$	16	8	20
$\{v_3, v_5\}$	18	12	20
$\{v_4, v_5\}$	18	13	20
$\{v_1, v_2, v_3\}$	17	10	15
$\{v_1, v_2, v_4\}$	17	12	18
$\{v_1, v_2, v_5\}$	18	12	19
$\{v_1, v_3, v_4\}$	18	8	20
$\{v_1, v_3, v_5\}$	18	13	20
$\{v_1, v_4, v_5\}$	18	13	20
$\{v_2, v_3, v_3\}$	18	12	20
$\{v_2, v_3, v_5\}$	18	13	20
$\{v_2, v_4, v_5\}$	18	13	20
$\{v_3, v_4, v_5\}$	18	13	20
$\{v_1, v_2, v_3, v_4\}$	18	12	20
$\{v_1, v_2, v_3, v_5\}$	18	13	20
$\{v_1, v_2, v_4, v_5\}$	18	13	20
$\{v_1, v_3, v_4, v_5\}$	18	13	20
$\{v_2, v_3, v_4, v_5\}$	18	13	20
$\{v_1, v_2, v_3, v_4, v_5\}$	18	13	20

Table 7.1: Parameters of some $(5, k)$-bicliques with chromatic polynomials that have totally real splitting fields, and the Galois groups of those splitting field.

A_5, and of a $(5, k)$-biclique with interesting factor $g(x) = x^5 - 65x^4 + 1680x^3 - 21580x^2 + 137755x - 349593$ which has Galois group $F(5)$. This allows us to make the following proposition.

Proposition 7.7 *For every possible signature (r_1, r_2) and group G of a quintic number field, there is a $(5, k)$-biclique with a chromatic polynomial whose splitting field has that signature and Galois group.*

References

[1] R. A. Mollin. Algebraic number theory, CRC Press LLC, 1999.

[2] A. Bohn. Chromatic roots as algebraic integers. *DMTCS Proceedings, 24th Int. Conf. on Formal Power Series and Algebraic Combinatorics (FPSAC 2012)*, pp. 539-550, 2012.

[3] A. Bohn. Algebraic number-theoretic properties of graph and matroid polynomials. PhD thesis, University of London, 2013.

[4] K. BRaun, M. Kretz, B. Walter, and M. Walter. Die chromatischen polynome unterringfreier graphen. *Manuscripa Math.* 14, 223-234, 1975.

[5] C.W. Brown. QEPCAD-B: a program for computing with semi-algebraic sets usign CADs. *SIGSAM Bulletin* 37(4), 97-108, 2003.

[6] J. Buchmann and D. Ford. On the computation of totally real quartic fields of small discriminant. *Math. Comp.* 52, 161-174, 1989.

[7] J. Buchmann, D. Ford, and M. Pohst. Enumeration of quartic fields of small discriminant. *Math. Comp.* 61, 873-879, 1993.

[8] P.J. Cameron and K. Morgan. Algebraic properties of chromatic roots. Under review; summary online at `http://www.maths.qmul.ac.uk/~pjc/slides/beamer/alchrom.pdf`, 2011.

[9] D. Delbourgo and K. Morgan. Algebraic invariants arising from the chromatic polynomials of theta graphs. *Australas. J. Comin.* 59(2), 293-310, 2014.

[10] F. M. Dong, K. M. Koh, K. L. Teo. Chromatic polynomials and chromaticity of graphs, World Scientific Publishing Company, 2005.

[11] D. S. Dummite and R. M. Foote. Abstract Algebra, John Wiley and Sons Inc., 3rd edition,2004.

[12] D. Ford. Enumeration of totally complex quartic fields of small discriminant. *Computational Number Theory*, 129-138, 1989.

[13] H. Hong. QEPCA Quantifier elimination by partial cylindrical algebraic decomposition. Sources and documentation are available from `http://www.cs.usna.edu/~qepcad/B/QEPCAD.html`.

[14] B. Jackson. A zero-free interval for chromatic polynomials of graphs. *Combin. Probab. Comput. 2*, 325-336, 1993.

[15] K. Morgan. Galois groups of chromatic polynomials. *LMS J. Comput. Math* 15, 281-307, 2012.

[16] K. Morgan and G. Farr. Certificates of factorisation for chromatic polynomials. *Electron. J. Combin.*, 16: Research Paper R74, 2009.

[17] The PARI Group, PARI/GP version `2.7.1`, Bordeaux, 2014, `http://pari.math.u-bordeaux.fr/`.

[18] A. Schwarz, M. Pohst and F. Diaz y Diaz. A table of quintic number fields. *Math. Comp.* 63, 361-376, 1994.

[19] R.C. Read. Review. *Mathematical Reviews*, 50, Review 6096, 1975

[20] J. Rotman. Galois Theory, Springer Science+Business Media New York, 2nd edition, 1998.

[21] A.D. Sokal. Chromatic polynomials, Potts models and all that. *Phys. A* 279, 324-332, 2000.

[22] A.D. Sokal. Chromatic roots are dense in the whole complex plane. *Combin. Probab. Comput.* 13, 221-261, 2004.

[23] C. Thomassen. The zero-free intervals for chromatic polynomials of graphs. *Combin. Probab. Comput.* 6, 497-506, 1997.

[24] L. Washington. Introduction to Cyclotomic Fields, Graduate Texts in Mathematics 83 (2 nd ed.), Berlin, New York: Springer-Verlag, 1997.

[25] D. R. Woodall. Zeros of chromatic polynomials. *Combinatorial Survey, Proc. Sixth British Combin. Conf. (ed. P.J. Cameron)*, 199-223, 1977.

Appendices

Appendix A

Program listings

This appendix contains listings of the programs used to construct the tables refereed to in Chapter 7.

The C programs `gen_if_4.c` and `gen_if_5.c` generate all (j, k)-bicliques with $j = 4$ and $j = 5$ respectively, and prints the parameters and interesting factor for each one.

The C program `filter_disc.c` is used to filter out bicliques whose interesting factor has a splitting field with discriminant outside the required bounds.

The Java program `UniqRedPol.java` filters out bicliques that have an interesting factor with a splitting field that has already been seen.

The Java program `ComputeIF.java` computes the interesting factor of a biclique suitable for use in computer algebra package.

The remaining C programs, `nf_disc.c` and `red_pol.c`, are simply wrapper programs for the PARI/GP functions `nfdisc(f)` and `polredabs(f)`.

As an example, the Bash script `search_quartic.sh` run using the command

```
$> ./search_quartic.sh 5 10 -1000 1000
```

will print the parameters and interesting factor of one $(4, k)$-biclique for each number field with discriminant Δ such that $-1000 \leq \Delta \leq 1000$ that arises as the splitting field of the chromatic polynomial of a $(4, k)$-biclique with between

5 and 10 bridging edges. That is, `search_quartic.sh` is an implementation of Algorithm 1 in Chapter 7 for $j = 4$.

Little modification is required to implement Algorithm 2 .

search_quartic.sh

```
#! /usr/bin/env bash

./gen_if_4 $1 $2 | ./nf_disc 1 | ./filter_disc 1 $3 $4 | \
                   ./red_pol 2 | java UniqRedPol 1 4
```

gen_if_4.c

```
#include <stdio.h>

// Number of parameters.
#define NUM_PARAMS 15

// Degree of interesting factor.
#define DEG_IF 4

// Indices of parameters in array ( e.g. M[4] = M[I12] = M({v_1,v_2} ).
#define I1      0
#define I2      1
#define I3      2
#define I4      3
#define I12     4
#define I13     5
#define I14     6
#define I23     7
#define I24     8
#define I34     9
#define I123    10
#define I124    11
#define I134    12
#define I234    13
#define I1234   14

// Convert parameters M to N.
void convertMtoN(long long int M[], long long int N[]) {

    N[I1] = M[I1] + M[I12]+M[I13]+M[I14] + M[I123]+M[I124]+M[I134] + M[I1234];
    N[I2] = M[I2] + M[I12]+M[I23]+M[I24] + M[I123]+M[I124]+M[I234] + M[I1234];
    N[I3] = M[I3] + M[I13]+M[I23]+M[I34] + M[I123]+M[I134]+M[I234] + M[I1234];
    N[I4] = M[I4] + M[I14]+M[I24]+M[I34] + M[I124]+M[I134]+M[I234] + M[I1234];

    N[I12] = M[I1]+M[I2] + M[I12]+M[I13]+M[I14]+M[I23]+M[I24] + \
                M[I123]+M[I124]+M[I134]+M[I234] + M[I1234];
    N[I13] = M[I1]+M[I3] + M[I12]+M[I13]+M[I14]+M[I23]+M[I34] + \
                M[I123]+M[I124]+M[I134]+M[I234] + M[I1234];
    N[I14] = M[I1]+M[I4] + M[I12]+M[I13]+M[I14]+M[I24]+M[I34] + \
                M[I123]+M[I124]+M[I134]+M[I234] + M[I1234];
    N[I23] = M[I2]+M[I3] + M[I12]+M[I13]+M[I23]+M[I24]+M[I34] + \
                M[I123]+M[I124]+M[I134]+M[I234] + M[I1234];
```

```
    N[I24] = M[I2]+M[I4] + M[I12]+M[I14]+M[I23]+M[I24]+M[I34] + \
                M[I123]+M[I124]+M[I134]+M[I234] + M[I1234];
    N[I34] = M[I3]+M[I4] + M[I13]+M[I14]+M[I23]+M[I24]+M[I34] + \
                M[I123]+M[I124]+M[I134]+M[I234] + M[I1234];


    N[I123] = M[I1]+M[I2]+M[I3] + M[I12]+M[I13]+M[I14]+M[I23]+M[I24]+M[I34] + \
                M[I123]+M[I124]+M[I134]+M[I234] + M[I1234];
    N[I124] = M[I1]+M[I2]+M[I4] + M[I12]+M[I13]+M[I14]+M[I23]+M[I24]+M[I34] + \
                M[I123]+M[I124]+M[I134]+M[I234] + M[I1234];
    N[I134] = M[I1]+M[I3]+M[I4] + M[I12]+M[I13]+M[I14]+M[I23]+M[I24]+M[I34] + \
                M[I123]+M[I124]+M[I134]+M[I234] + M[I1234];
    N[I234] = M[I2]+M[I3]+M[I4] + M[I12]+M[I13]+M[I14]+M[I23]+M[I24]+M[I34] + \
                M[I123]+M[I124]+M[I134]+M[I234] + M[I1234];

    N[I1234] = M[I1]+M[I2]+M[I3]+M[I4] + \
                M[I12]+M[I13]+M[I14]+M[I23]+M[I24]+M[I34] + \
                M[I123]+M[I124]+M[I134]+M[I234] + M[I1234];

}

// Returns the coefficient of x^n in the interesting
// factor of the (4,k)-biclique with parameters N[].
long long int coeffIntFact(long long int N[], int n) {

    long long int coeff;

    switch(n) {

        case 4:
            coeff = 1;
            break;

        case 3:
            coeff = -(N[I1]+N[I2]+N[I3]+N[I4]+6);
            break;

        case 2:
            coeff = 3*(N[I1]+N[I2]+N[I3]+N[I4]) + \
                    N[I1]*N[I2]+N[I1]*N[I3]+N[I1]*N[I4] + \
                        N[I2]*N[I3]+N[I2]*N[I4]+N[I3]*N[I4] + \
                    N[I12]+N[I13]+N[I14]+N[I23]+N[I24]+N[I34] + 11;
            break;

        case 1:
            coeff = -( 2*(N[I1]+N[I2]+N[I3]+N[I4]) + \
                        N[I1]*N[I2]+N[I1]*N[I3]+N[I1]*N[I4] + \
                            N[I2]*N[I3]+N[I2]*N[I4]+N[I3]*N[I4] + \
                        N[I1]*N[I2]*N[I3]+N[I1]*N[I2]*N[I4] + \
                            N[I1]*N[I3]*N[I4]+N[I2]*N[I3]*N[I4] + \
                        N[I1]*(N[I23]+N[I24]+N[I34]) + \
                            N[I2]*(N[I13]+N[I14]+N[I34]) + \
                            N[I3]*(N[I12]+N[I14]+N[I24]) + \
                            N[I4]*(N[I12]+N[I13]+N[I23]) + \
                        N[I12]+N[I13]+N[I14]+N[I23]+N[I24]+N[I34]  + \
                        2*(N[I123]+N[I124]+N[I134]+N[I234]) + 6 );
            break;

        case 0:
            coeff = N[I1]*N[I2]*N[I3]*N[I4] + \
```

```
                    2*(N[I1]*N[I234]+N[I2]*N[I134] + \
                        N[I3]*N[I124]+N[I4]*N[I123]) + \
                    N[I1]*N[I2]*N[I34]+N[I1]*N[I3]*N[I24] + \
                        N[I1]*N[I4]*N[I23]+N[I2]*N[I3]*N[I14] + \
                        N[I2]*N[I4]*N[I13]+N[I3]*N[I4]*N[I12] + \
                    N[I12]*N[I34] + N[I13]*N[I24] + N[I14]*N[I23] + 6*N[I1234];
            break;

    }

    return coeff;

}

// Returns the number of bridging edges in a  (4,k)-biclique
// with parameters M[] adjecent to vertices v_1, ..., v_{i+1}.
long long int numEdges(long long int M[], int i) {

    long long int n = 0;
    int j;
    for(j=0; j<=i; j++) n += M[j];
    return n;

}

// Returns the largest minimum value that the parameter M[i] can
// have if all bicliques are to be generated (up to isomorphism) given
// that parameters M[0],...,M[i-1] have already been set. (In its current
// form, this code will still generate some pairs of isomorphic graphs.)
long long int minM(int i, long long int M[]) {

    long long int min = 0;

    switch(i) {

        // Assume the ordering M(v_1)<=M(v_2)<=M(v_3)<=M(v_4).
        case I1: min = 0; break;
        case I2: min = M[I1]; break;
        case I3: min = M[I2]; break;
        case I4: min = M[I3]; break;

        case I123: min = 0; break;
        case I124: min = 0; break;
        case I134: min = 0; break;
        case I234: min = 0; break;

        default: min = 0;

    }

    return min;

}

// Prints parameters for all (4,k)-bicliques . . .
int main(int argc, char *argv[]) {

    // Number of bridging edges.
    long long int minEdges = atoi(argv[1]);
    long long int maxEdges = atoi(argv[2]);;
```

```
long long int nEdges;
long long int nRemEdges[NUM_PARAMS];

// Biclique parameters.
long long int M[NUM_PARAMS];
long long int N[NUM_PARAMS];

// Counters for miscellaneous 'for' loops.
int i;
int n;

// Any (4,k)-biclique with M[I1234]=n is isomorphic to K_n joined to a
// (4,k)-biclique with M[I1234]=0. Therefore every splitting field of
// the interesting factor of a (4,k)-biclique is the splitting field of
// the interesting factor of a (4,k)-biclique with M[I1234]=0.
M[I1234] = 0;

for(nEdges=minEdges; nEdges<=maxEdges; nEdges++) {

for(M[I1]=minM(I1,M); M[I1]<=nEdges; M[I1]++) {
    nRemEdges[I2] = nEdges-numEdges(M,I1);
for(M[I2]=minM(I2,M); M[I2]<=nRemEdges[I2]; M[I2]++) {
    nRemEdges[I3] = nEdges-numEdges(M,I2);
for(M[I3]=minM(I3,M); M[I3]<=nRemEdges[I3]; M[I3]++) {
    nRemEdges[I4] = nEdges-numEdges(M,I3);
for(M[I4]=minM(I4,M); M[I4]<=nRemEdges[I4]; M[I4]++) {

    nRemEdges[I12] = nEdges-numEdges(M,I4);
for(M[I12]=minM(I12,M); M[I12]<=nRemEdges[I12]; M[I12]++) {
    nRemEdges[I13] = nEdges-numEdges(M,I12);
for(M[I13]=minM(I13,M); M[I13]<=nRemEdges[I13]; M[I13]++) {
    nRemEdges[I14] = nEdges-numEdges(M,I13);
for(M[I14]=minM(I14,M); M[I14]<=nRemEdges[I14]; M[I14]++) {
    nRemEdges[I23] = nEdges-numEdges(M,I14);
for(M[I23]=minM(I23,M); M[I23]<=nRemEdges[I23]; M[I23]++) {
    nRemEdges[I24] = nEdges-numEdges(M,I23);
for(M[I24]=minM(I24,M); M[I24]<=nRemEdges[I24]; M[I24]++) {
    nRemEdges[I34] = nEdges-numEdges(M,I24);
for(M[I34]=minM(I34,M); M[I34]<=nRemEdges[I34]; M[I34]++) {

    nRemEdges[I123] = nEdges-numEdges(M,I34);
for(M[I123]=minM(I123,M); M[I123]<=nRemEdges[I123]; M[I123]++) {
    nRemEdges[I124] = nEdges-numEdges(M,I123);
for(M[I124]=minM(I124,M); M[I124]<=nRemEdges[I124]; M[I124]++) {
    nRemEdges[I134] = nEdges-numEdges(M,I124);
for(M[I134]=minM(I134,M); M[I134]<=nRemEdges[I134]; M[I134]++) {

    // Set M[I234] so that the number of edges in the biclique is 'nEdges'.
    M[I234] = nEdges-numEdges(M, I134);

    // Convert M[] to N[].
    convertMtoN(M, N);

    // Print coefficients of interesting factor.
    for(n=DEG_IF; n>=0; n--)
        printf("%ld%c", coeffIntFact(N, n), n>0 ? ',' : ':');

    // Print parameters of biclique.
    for(i=0; i<NUM_PARAMS; i++)
        printf("%ld%c", N[i], i<NUM_PARAMS-1 ? ',' : '\n');
```

```
    }}}}}}}}}}}}}

}
```

gen_if_5.c

```
#include <stdio.h>

// Number of parameters.
#define NUM_PARAMS 31

// Degree of interesting factor.
#define DEG_IF 5

// Indices of parameters in array ( e.g. M[5] = M[I12] = M({v_1,v_2} ).
#define I1      0
#define I2      1
#define I3      2
#define I4      3
#define I5      4

#define I12     5
#define I13     6
#define I14     7
#define I15     8
#define I23     9
#define I24     10
#define I25     11
#define I34     12
#define I35     13
#define I45     14

#define I123    15
#define I124    16
#define I125    17
#define I134    18
#define I135    19
#define I145    20
#define I234    21
#define I235    22
#define I245    23
#define I345    24

#define I1234   25
#define I1235   26
#define I1245   27
#define I1345   28
#define I2345   29

#define I12345  30

// Convert parameters M to N.
void convertMtoN(long long int M[], long long int N[]) {

    N[I1] = M[I1] + M[I12]+M[I13]+M[I14]+M[I15] \
                + M[I123]+M[I124]+M[I125]+M[I134]+M[I135]+M[I145] \
                + M[I1234]+M[I1235]+M[I1245]+M[I1345] + M[I12345];
```

```
N[I2] = M[I2] + M[I12]+M[I23]+M[I24]+M[I25] \
            + M[I123]+M[I124]+M[I125]+M[I234]+M[I235]+M[I245] \
            + M[I1234]+M[I1235]+M[I1245]+M[I2345] + M[I12345];
N[I3] = M[I3] + M[I13]+M[I23]+M[I34]+M[I35] \
            + M[I123]+M[I134]+M[I135]+M[I234]+M[I235]+M[I345] \
            + M[I1234]+M[I1235]+M[I1345]+M[I2345] + M[I12345];
N[I4] = M[I4] + M[I14]+M[I24]+M[I34]+M[I45] \
            + M[I124]+M[I134]+M[I145]+M[I234]+M[I245]+M[I345] \
            + M[I1234]+M[I1245]+M[I1345]+M[I2345] + M[I12345];
N[I5] = M[I5] + M[I15]+M[I25]+M[I35]+M[I45] \
            + M[I125]+M[I135]+M[I145]+M[I235]+M[I245]+M[I345] \
            + M[I1235]+M[I1245]+M[I1345]+M[I2345] + M[I12345];

N[I12] = M[I1]+M[I2] + M[I12]+M[I13]+M[I14]+M[I15]+M[I23]+M[I24]+M[I25] \
            + M[I123]+M[I124]+M[I125] \
            + M[I134]+M[I135]+M[I145] \
            + M[I234]+M[I235]+M[I245] \
            + M[I1234]+M[I1235]+M[I1245]+M[I1345]+M[I2345] + M[I12345];
N[I13] = M[I1]+M[I3] + M[I12]+M[I13]+M[I14]+M[I15]+M[I23]+M[I34]+M[I35] \
            + M[I123]+M[I124]+M[I125] \
            + M[I134]+M[I135]+M[I145] \
            + M[I234]+M[I235]+M[I345] \
            + M[I1234]+M[I1235]+M[I1245]+M[I1345]+M[I2345] + M[I12345];
N[I14] = M[I1]+M[I4] + M[I12]+M[I13]+M[I14]+M[I15]+M[I24]+M[I34]+M[I45] \
            + M[I123]+M[I124]+M[I125] \
            + M[I134]+M[I135]+M[I145] \
            + M[I234]+M[I245]+M[I345] \
            + M[I1234]+M[I1235]+M[I1245]+M[I1345]+M[I2345] + M[I12345];
N[I15] = M[I1]+M[I5] + M[I12]+M[I13]+M[I14]+M[I15]+M[I25]+M[I35]+M[I45] \
            + M[I123]+M[I124]+M[I125] \
            + M[I134]+M[I135]+M[I145] \
            + M[I235]+M[I245]+M[I345] \
            + M[I1234]+M[I1235]+M[I1245]+M[I1345]+M[I2345] + M[I12345];
N[I23] = M[I2]+M[I3] + M[I12]+M[I13]+M[I23]+M[I24]+M[I25]+M[I34]+M[I35] \
            + M[I123]+M[I124]+M[I125] \
            + M[I134]+M[I135]+M[I234] \
            + M[I235]+M[I245]+M[I345] \
            + M[I1234]+M[I1235]+M[I1245]+M[I1345]+M[I2345] + M[I12345];
N[I24] = M[I2]+M[I4] + M[I12]+M[I14]+M[I23]+M[I24]+M[I25]+M[I34]+M[I45] \
            + M[I123]+M[I124]+M[I125] \
            + M[I134]+M[I145]+M[I234] \
            + M[I235]+M[I245]+M[I345] \
            + M[I1234]+M[I1235]+M[I1245]+M[I1345]+M[I2345] + M[I12345];
N[I25] = M[I2]+M[I5] + M[I12]+M[I15]+M[I23]+M[I24]+M[I25]+M[I35]+M[I45] \
            + M[I123]+M[I124]+M[I125] \
            + M[I135]+M[I145]+M[I234] \
            + M[I235]+M[I245]+M[I345] \
            + M[I1234]+M[I1235]+M[I1245]+M[I1345]+M[I2345] + M[I12345];
N[I34] = M[I3]+M[I4] + M[I13]+M[I14]+M[I23]+M[I24]+M[I34]+M[I35]+M[I45] \
            + M[I123]+M[I124]+M[I134] \
            + M[I135]+M[I145]+M[I234] \
            + M[I235]+M[I245]+M[I345] \
            + M[I1234]+M[I1235]+M[I1245]+M[I1345]+M[I2345] + M[I12345];
N[I35] = M[I3]+M[I5] + M[I13]+M[I15]+M[I23]+M[I25]+M[I34]+M[I35]+M[I45] \
            + M[I123]+M[I125]+M[I134] \
            + M[I135]+M[I145]+M[I234] \
            + M[I235]+M[I245]+M[I345] \
            + M[I1234]+M[I1235]+M[I1245]+M[I1345]+M[I2345] + M[I12345];
N[I45] = M[I4]+M[I5] + M[I14]+M[I15]+M[I24]+M[I25]+M[I34]+M[I35]+M[I45] \
            + M[I124]+M[I125]+M[I134] \
```

```
            + M[I135]+M[I145]+M[I234] \
            + M[I235]+M[I245]+M[I345] \
            + M[I1234]+M[I1235]+M[I1245]+M[I1345]+M[I2345] + M[I12345];

N[I123] = M[I1]+M[I2]+M[I3] \
            + M[I12]+M[I13]+M[I14] \
            + M[I15]+M[I23]+M[I24] \
            + M[I25]+M[I34]+M[I35] \
            + M[I123]+M[I124]+M[I125]+M[I134]+M[I135] \
            + M[I145]+M[I234]+M[I235]+M[I245]+M[I345] \
            + M[I1234]+M[I1235]+M[I1245]+M[I1345]+M[I2345] + M[I12345];
N[I124] = M[I1]+M[I2]+M[I4] \
            + M[I12]+M[I13]+M[I14] \
            + M[I15]+M[I23]+M[I24] \
            + M[I25]+M[I34]+M[I45]  \
            + M[I123]+M[I124]+M[I125]+M[I134]+M[I135] \
            + M[I145]+M[I234]+M[I235]+M[I245]+M[I345] \
            + M[I1234]+M[I1235]+M[I1245]+M[I1345]+M[I2345] + M[I12345];
N[I125] = M[I1]+M[I2]+M[I5] \
            + M[I12]+M[I13]+M[I14] \
            + M[I15]+M[I23]+M[I24] \
            + M[I25]+M[I35]+M[I45] \
            + M[I123]+M[I124]+M[I125]+M[I134]+M[I135] \
            + M[I145]+M[I234]+M[I235]+M[I245]+M[I345] \
            + M[I1234]+M[I1235]+M[I1245]+M[I1345]+M[I2345] + M[I12345];
N[I134] = M[I1]+M[I3]+M[I4] \
            + M[I12]+M[I13]+M[I14] \
            + M[I15]+M[I23]+M[I24] \
            + M[I34]+M[I35]+M[I45] \
            + M[I123]+M[I124]+M[I125]+M[I134]+M[I135] \
            + M[I145]+M[I234]+M[I235]+M[I245]+M[I345] \
            + M[I1234]+M[I1235]+M[I1245]+M[I1345]+M[I2345] + M[I12345];
N[I135] = M[I1]+M[I3]+M[I5] \
            + M[I12]+M[I13]+M[I14] \
            + M[I15]+M[I23]+M[I25] \
            + M[I34]+M[I35]+M[I45] \
            + M[I123]+M[I124]+M[I125]+M[I134]+M[I135] \
            + M[I145]+M[I234]+M[I235]+M[I245]+M[I345] \
            + M[I1234]+M[I1235]+M[I1245]+M[I1345]+M[I2345] + M[I12345];
N[I145] = M[I1]+M[I4]+M[I5] \
            + M[I12]+M[I13]+M[I14] \
            + M[I15]+M[I24]+M[I25] \
            + M[I34]+M[I35]+M[I45] \
            + M[I123]+M[I124]+M[I125]+M[I134]+M[I135] \
            + M[I145]+M[I234]+M[I235]+M[I245]+M[I345] \
            + M[I1234]+M[I1235]+M[I1245]+M[I1345]+M[I2345] + M[I12345];
N[I234] = M[I2]+M[I3]+M[I4] \
            + M[I12]+M[I13]+M[I14] \
            + M[I23]+M[I24]+M[I25] \
            + M[I34]+M[I35]+M[I45] \
            + M[I123]+M[I124]+M[I125]+M[I134]+M[I135] \
            + M[I145]+M[I234]+M[I235]+M[I245]+M[I345] \
            + M[I1234]+M[I1235]+M[I1245]+M[I1345]+M[I2345] + M[I12345];
N[I235] = M[I2]+M[I3]+M[I5] \
            + M[I12]+M[I13]+M[I15] \
            + M[I23]+M[I24]+M[I25] \
            + M[I34]+M[I35]+M[I45] \
            + M[I123]+M[I124]+M[I125]+M[I134]+M[I135] \
            + M[I145]+M[I234]+M[I235]+M[I245]+M[I345] \
            + M[I1234]+M[I1235]+M[I1245]+M[I1345]+M[I2345] + M[I12345];
```

```
    N[I245] = M[I2]+M[I4]+M[I5] \
                + M[I12]+M[I14]+M[I15] \
                + M[I23]+M[I24]+M[I25] \
                + M[I34]+M[I35]+M[I45] \
                + M[I123]+M[I124]+M[I125]+M[I134]+M[I135] \
                + M[I145]+M[I234]+M[I235]+M[I245]+M[I345] \
                + M[I1234]+M[I1235]+M[I1245]+M[I1345]+M[I2345] + M[I12345];
    N[I345] = M[I3]+M[I4]+M[I5] \
                + M[I13]+M[I14]+M[I15] \
                + M[I23]+M[I24]+M[I25] \
                + M[I34]+M[I35]+M[I45] \
                + M[I123]+M[I124]+M[I125]+M[I134]+M[I135] \
                + M[I145]+M[I234]+M[I235]+M[I245]+M[I345] \
                + M[I1234]+M[I1235]+M[I1245]+M[I1345]+M[I2345] + M[I12345];

    N[I1234] = M[I1]+M[I2]+M[I3]+M[I4] + M[I12]+M[I13]+M[I14]+M[I15]+M[I23] \
                + M[I24]+M[I25]+M[I34]+M[I35]+M[I45] \
                + M[I123]+M[I124]+M[I125]+M[I134]+M[I135] \
                + M[I145]+M[I234]+M[I235]+M[I245]+M[I345] \
                + M[I1234]+M[I1235]+M[I1245]+M[I1345]+M[I2345] + M[I12345];
    N[I1235] = M[I1]+M[I2]+M[I3]+M[I5] + M[I12]+M[I13]+M[I14]+M[I15]+M[I23] \
                + M[I24]+M[I25]+M[I34]+M[I35]+M[I45] \
                + M[I123]+M[I124]+M[I125]+M[I134]+M[I135] \
                + M[I145]+M[I234]+M[I235]+M[I245]+M[I345] \
                + M[I1234]+M[I1235]+M[I1245]+M[I1345]+M[I2345] + M[I12345];
    N[I1245] = M[I1]+M[I2]+M[I4]+M[I5] + M[I12]+M[I13]+M[I14]+M[I15]+M[I23] \
                + M[I24]+M[I25]+M[I34]+M[I35]+M[I45] \
                + M[I123]+M[I124]+M[I125]+M[I134]+M[I135] \
                + M[I145]+M[I234]+M[I235]+M[I245]+M[I345] \
                + M[I1234]+M[I1235]+M[I1245]+M[I1345]+M[I2345] + M[I12345];
    N[I1345] = M[I1]+M[I3]+M[I4]+M[I5] + M[I12]+M[I13]+M[I14]+M[I15]+M[I23] \
                + M[I24]+M[I25]+M[I34]+M[I35]+M[I45] \
                + M[I123]+M[I124]+M[I125]+M[I134]+M[I135] \
                + M[I145]+M[I234]+M[I235]+M[I245]+M[I345] \
                + M[I1234]+M[I1235]+M[I1245]+M[I1345]+M[I2345] + M[I12345];
    N[I2345] = M[I1]+M[I2]+M[I3]+M[I4]+M[I5] + M[I12]+M[I13]+M[I14]+M[I15]+M[I23] \
                + M[I24]+M[I25]+M[I34]+M[I35]+M[I45] \
                + M[I123]+M[I124]+M[I125]+M[I134]+M[I135] \
                + M[I145]+M[I234]+M[I235]+M[I245]+M[I345] \
                + M[I1234]+M[I1235]+M[I1245]+M[I1345]+M[I2345] + M[I12345];

    N[I12345] = M[I1]+M[I2]+M[I3]+M[I4]+M[I5] \
                + M[I12]+M[I13]+M[I14]+M[I15]+M[I23] \
                + M[I24]+M[I25]+M[I34]+M[I35]+M[I45] \
                + M[I123]+M[I124]+M[I125]+M[I134]+M[I135] \
                + M[I145]+M[I234]+M[I235]+M[I245]+M[I345] \
                + M[I1234]+M[I1235]+M[I1245]+M[I1345]+M[I2345] + M[I12345];

}

// Returns the coefficient of x^n in the interesting
// factor of the (5,k)-biclique with parameters N[].
long long int coeffIntFact(long long int N[], int n) {

    long long int coeff;

    switch(n) {

        case 5:
            coeff = 1;
```

```
    break;

case 4:
    coeff = -(N[I1]+N[I2]+N[I3]+N[I4]+N[I5]+10);
    break;

case 3:
    coeff = 6*(N[I1]+N[I2]+N[I3]+N[I4]+N[I5]) \
                +N[I45]+N[I35]+N[I34]+N[I12]+N[I25] \
                +N[I24]+N[I13]+N[I23]+N[I14]+N[I15] \
                +N[I1]*N[I2]+N[I2]*N[I3]+N[I1]*N[I5]+N[I3]*N[I5] \
                +N[I4]*N[I5]+N[I1]*N[I4]+N[I3]*N[I4]+N[I2]*N[I5] \
                +N[I1]*N[I3]+N[I2]*N[I4] + 35;
    break;

case 2:
    coeff = -(11*N[I5]+11*N[I4]+2*N[I123]+3*N[I45]+11*N[I3]+2*N[I124] \
                +3*N[I35]+2*N[I125]+3*N[I34]+3*N[I12]+2*N[I345] \
                +11*N[I2]+2*N[I134]+3*N[I25]+2*N[I135]+3*N[I24] \
                +3*N[I13]+2*N[I245]+2*N[I145]+3*N[I23]+3*N[I14] \
                +2*N[I235]+3*N[I15]+2*N[I234]+11*N[I1]+50 \
                +N[I1]*N[I2]*N[I3]+N[I2]*N[I4]*N[I5]+N[I2]*N[I3]*N[I5] \
                +N[I2]*N[I3]*N[I4]+N[I1]*N[I4]*N[I5]+N[I1]*N[I3]*N[I5] \
                +N[I1]*N[I3]*N[I4]+N[I1]*N[I2]*N[I5]+N[I1]*N[I2]*N[I4] \
                +N[I12]*N[I3]+N[I13]*N[I2]+N[I1]*N[I23]+N[I14]*N[I2] \
                +N[I1]*N[I24]+N[I15]*N[I2]+N[I1]*N[I25]+3*N[I1]*N[I2] \
                +N[I13]*N[I5]+3*N[I2]*N[I3]+N[I25]*N[I3]+N[I24]*N[I3] \
                +N[I1]*N[I35]+N[I25]*N[I4]+N[I14]*N[I5]+N[I14]*N[I3] \
                +N[I2]*N[I34]+3*N[I1]*N[I5]+3*N[I3]*N[I5]+N[I1]*N[I45] \
                +3*N[I4]*N[I5]+N[I2]*N[I45]+N[I15]*N[I4]+N[I23]*N[I4] \
                +3*N[I1]*N[I4]+N[I24]*N[I5]+3*N[I3]*N[I4] \
                +3*N[I2]*N[I5]+N[I3]*N[I45]+N[I12]*N[I5]+N[I35]*N[I4] \
                +3*N[I1]*N[I3]+N[I23]*N[I5]+N[I34]*N[I5]+N[I1]*N[I34] \
                +N[I15]*N[I3]+N[I2]*N[I35]+N[I12]*N[I4]+N[I13]*N[I4] \
                +3*N[I2]*N[I4]+N[I3]*N[I4]*N[I5]);

    break;

case 1:
    coeff = 6*N[I1234]+6*N[I5]+6*N[I1235]+6*N[I4]+2*N[I123]+2*N[I45] \
                +6*N[I1245]+6*N[I3]+2*N[I124]+2*N[I35]+2*N[I125] \
                +2*N[I34]+2*N[I12]+2*N[I345]+6*N[I1345]+6*N[I2] \
                +2*N[I134]+2*N[I25]+2*N[I135]+2*N[I24]+2*N[I13] \
                +2*N[I245]+2*N[I145]+2*N[I23]+2*N[I14]+2*N[I235] \
                +2*N[I15]+2*N[I234]+6*N[I1]+6*N[I2345]+24 \
                +N[I12]*N[I3]*N[I4]+N[I13]*N[I2]*N[I4] \
                +N[I1]*N[I23]*N[I4]+N[I14]*N[I2]*N[I3] \
                +N[I1]*N[I24]*N[I3]+N[I1]*N[I2]*N[I34] \
                +N[I15]*N[I2]*N[I3]+N[I1]*N[I25]*N[I3] \
                +N[I1]*N[I2]*N[I35]+N[I1]*N[I2]*N[I3] \
                +N[I1]*N[I2]*N[I3]*N[I4]+N[I2]*N[I4]*N[I5] \
                +N[I2]*N[I3]*N[I5]+N[I2]*N[I3]*N[I4]+N[I1]*N[I4]*N[I5] \
                +N[I1]*N[I3]*N[I5]+N[I1]*N[I3]*N[I4]+N[I1]*N[I2]*N[I5] \
                +N[I1]*N[I2]*N[I4]+N[I24]*N[I3]*N[I5] \
                +N[I1]*N[I24]*N[I5]+N[I2]*N[I34]*N[I5] \
                +N[I1]*N[I34]*N[I5]+N[I15]*N[I3]*N[I4] \
                +N[I15]*N[I2]*N[I4]+N[I25]*N[I3]*N[I4] \
                +N[I1]*N[I25]*N[I4]+N[I2]*N[I35]*N[I4] \
                +N[I1]*N[I35]*N[I4]+N[I2]*N[I3]*N[I45] \
                +N[I1]*N[I3]*N[I45]+N[I1]*N[I2]*N[I45] \
```

```
                        +N[I12]*N[I4]*N[I5]+N[I12]*N[I3]*N[I5] \
                        +N[I13]*N[I4]*N[I5]+N[I13]*N[I2]*N[I5] \
                        +N[I23]*N[I4]*N[I5]+N[I1]*N[I23]*N[I5] \
                        +N[I14]*N[I3]*N[I5]+N[I14]*N[I2]*N[I5]+N[I12]*N[I34] \
                        +N[I12]*N[I35]+N[I12]*N[I3]+N[I13]*N[I24] \
                        +N[I13]*N[I25]+N[I13]*N[I2]+N[I15]*N[I23]+N[I1]*N[I23] \
                        +N[I14]*N[I25]+N[I14]*N[I2]+N[I15]*N[I24]+N[I1]*N[I24] \
                        +N[I15]*N[I2]+N[I1]*N[I25]+2*N[I1]*N[I2] \
                        +2*N[I1]*N[I245]+N[I2]*N[I3]*N[I4]*N[I5] \
                        +N[I1]*N[I3]*N[I4]*N[I5]+N[I1]*N[I2]*N[I4]*N[I5] \
                        +N[I1]*N[I2]*N[I3]*N[I5]+N[I13]*N[I5]+2*N[I2]*N[I3] \
                        +N[I25]*N[I3]+N[I24]*N[I3]+N[I1]*N[I35]+N[I25]*N[I4] \
                        +N[I14]*N[I5]+N[I14]*N[I3]+N[I2]*N[I34]+2*N[I1]*N[I5] \
                        +2*N[I3]*N[I5]+N[I1]*N[I45]+2*N[I4]*N[I5]+N[I2]*N[I45] \
                        +N[I15]*N[I4]+N[I23]*N[I4]+2*N[I1]*N[I4]+N[I24]*N[I5] \
                        +2*N[I3]*N[I4]+2*N[I2]*N[I5]+N[I3]*N[I45]+N[I12]*N[I5] \
                        +N[I35]*N[I4]+2*N[I245]*N[I3]+2*N[I1]*N[I3] \
                        +N[I23]*N[I5]+N[I13]*N[I45]+N[I34]*N[I5]+N[I1]*N[I34] \
                        +N[I15]*N[I3]+N[I2]*N[I35]+2*N[I235]*N[I4] \
                        +2*N[I135]*N[I4]+N[I14]*N[I35]+N[I12]*N[I45] \
                        +2*N[I125]*N[I4]+2*N[I123]*N[I5]+2*N[I234]*N[I5] \
                        +N[I23]*N[I45]+2*N[I2]*N[I345]+2*N[I1]*N[I345] \
                        +N[I25]*N[I34]+N[I24]*N[I35]+2*N[I134]*N[I5] \
                        +N[I15]*N[I34]+2*N[I124]*N[I5]+2*N[I145]*N[I3] \
                        +N[I12]*N[I4]+N[I13]*N[I4]+2*N[I2]*N[I4] \
                        +2*N[I125]*N[I3]+2*N[I134]*N[I2]+2*N[I123]*N[I4] \
                        +2*N[I124]*N[I3]+2*N[I1]*N[I235]+2*N[I145]*N[I2] \
                        +2*N[I135]*N[I2]+2*N[I1]*N[I234]+N[I14]*N[I23] \
                        +N[I3]*N[I4]*N[I5];
            break;

        case 0:
            coeff = -(24*N[I12345]+N[I15]*N[I23]*N[I4]+N[I1]*N[I23]*N[I45] \
                        +N[I14]*N[I25]*N[I3]+N[I14]*N[I2]*N[I35] \
                        +N[I15]*N[I24]*N[I3]+N[I1]*N[I24]*N[I35] \
                        +N[I15]*N[I2]*N[I34]+N[I1]*N[I25]*N[I34] \
                        +2*N[I1]*N[I245]*N[I3]+6*N[I1234]*N[I5] \
                        +6*N[I1235]*N[I4]+2*N[I123]*N[I45]+6*N[I1245]*N[I3] \
                        +N[I14]*N[I2]*N[I3]*N[I5]+N[I1]*N[I24]*N[I3]*N[I5] \
                        +N[I1]*N[I2]*N[I34]*N[I5]+N[I15]*N[I2]*N[I3]*N[I4] \
                        +N[I1]*N[I25]*N[I3]*N[I4]+N[I1]*N[I2]*N[I35]*N[I4] \
                        +N[I1]*N[I2]*N[I3]*N[I45]+N[I12]*N[I3]*N[I4]*N[I5] \
                        +N[I13]*N[I2]*N[I4]*N[I5]+N[I1]*N[I23]*N[I4]*N[I5] \
                        +2*N[I124]*N[I35]+2*N[I125]*N[I34]+2*N[I12]*N[I345] \
                        +6*N[I1345]*N[I2]+2*N[I134]*N[I25]+2*N[I135]*N[I24] \
                        +2*N[I13]*N[I245]+2*N[I145]*N[I23]+2*N[I14]*N[I235] \
                        +2*N[I15]*N[I234]+6*N[I1]*N[I2345] \
                        +N[I1]*N[I2]*N[I3]*N[I4]*N[I5]+N[I13]*N[I2]*N[I45] \
                        +N[I12]*N[I34]*N[I5]+N[I13]*N[I24]*N[I5] \
                        +N[I12]*N[I35]*N[I4]+N[I12]*N[I3]*N[I45] \
                        +N[I13]*N[I25]*N[I4]+2*N[I1]*N[I2]*N[I345] \
                        +2*N[I125]*N[I3]*N[I4]+2*N[I134]*N[I2]*N[I5] \
                        +2*N[I123]*N[I4]*N[I5]+2*N[I124]*N[I3]*N[I5] \
                        +2*N[I1]*N[I235]*N[I4]+2*N[I145]*N[I2]*N[I3] \
                        +2*N[I135]*N[I2]*N[I4]+2*N[I1]*N[I234]*N[I5] \
                        +N[I14]*N[I23]*N[I5]);
            break;

    }
```

```
    return coeff;

}

// Returns the number of bridging edges in a  (5,k)-biclique
// with parameters M[] adjecent to vertices v_1, ..., v_{i+1}.
long long int numEdges(long long int M[], int i) {

    long long int n = 0;
    int j;
    for(j=0; j<=i; j++) n += M[j];
    return n;

}

// Returns the largest minimum value that the parameter M[i] can
// have if all bicliques are to be generated (up to isomorphism) given
// that parameters M[0],...,M[i-1] have already been set.
long long int minM(int i, long long int M[]) {

    long long int min = 0;

    switch(i) {

        // Assume the ordering M(v_1)<=M(v_2)<=M(v_3)<=M(v_4)<=M(v_5).
        case I1: min = 0; break;
        case I2: min = M[I1]; break;
        case I3: min = M[I2]; break;
        case I4: min = M[I3]; break;
        case I5: min = M[I4]; break;

        default: min = 0;

    }

    return min;

}

// Prints parameters for all (5,k)-bicliques . . .
int main(int argc, char *argv[]) {

    // Number of bridging edges.
    long long int minEdges = atoi(argv[1]);
    long long int maxEdges = atoi(argv[2]);;
    long long int nEdges;
    long long int nRemEdges[NUM_PARAMS];

    // Biclique parameters.
    long long int M[NUM_PARAMS];
    long long int N[NUM_PARAMS];

    // Counters for miscellaneous 'for' loops.
    int i;
    int n;

    M[I12345] = 0;

    for(nEdges=minEdges; nEdges<=maxEdges; nEdges++) {
```

```
for(M[I1]=minM(I1,M); M[I1]<=nEdges; M[I1]++) {
    nRemEdges[I2] = nEdges-numEdges(M,I1);
for(M[I2]=minM(I2,M); M[I2]<=nRemEdges[I2]; M[I2]++) {
    nRemEdges[I3] = nEdges-numEdges(M,I2);
for(M[I3]=minM(I3,M); M[I3]<=nRemEdges[I3]; M[I3]++) {
    nRemEdges[I4] = nEdges-numEdges(M,I3);
for(M[I4]=minM(I4,M); M[I4]<=nRemEdges[I4]; M[I4]++) {
    nRemEdges[I5] = nEdges-numEdges(M,I4);
for(M[I5]=minM(I5,M); M[I5]<=nRemEdges[I5]; M[I5]++) {

    nRemEdges[I12] = nEdges-numEdges(M,I5);
for(M[I12]=minM(I12,M); M[I12]<=nRemEdges[I12]; M[I12]++) {
    nRemEdges[I13] = nEdges-numEdges(M,I12);
for(M[I13]=minM(I13,M); M[I13]<=nRemEdges[I13]; M[I13]++) {
    nRemEdges[I14] = nEdges-numEdges(M,I13);
for(M[I14]=minM(I14,M); M[I14]<=nRemEdges[I14]; M[I14]++) {
    nRemEdges[I15] = nEdges-numEdges(M,I14);
for(M[I15]=minM(I15,M); M[I15]<=nRemEdges[I15]; M[I15]++) {
    nRemEdges[I23] = nEdges-numEdges(M,I15);
for(M[I23]=minM(I23,M); M[I23]<=nRemEdges[I23]; M[I23]++) {
    nRemEdges[I24] = nEdges-numEdges(M,I23);
for(M[I24]=minM(I24,M); M[I24]<=nRemEdges[I24]; M[I24]++) {
    nRemEdges[I25] = nEdges-numEdges(M,I24);
for(M[I25]=minM(I25,M); M[I25]<=nRemEdges[I25]; M[I25]++) {
    nRemEdges[I34] = nEdges-numEdges(M,I25);
for(M[I34]=minM(I34,M); M[I34]<=nRemEdges[I34]; M[I34]++) {
    nRemEdges[I35] = nEdges-numEdges(M,I34);
for(M[I35]=minM(I35,M); M[I35]<=nRemEdges[I35]; M[I35]++) {
    nRemEdges[I45] = nEdges-numEdges(M,I35);
for(M[I45]=minM(I45,M); M[I45]<=nRemEdges[I45]; M[I45]++) {

    nRemEdges[I123] = nEdges-numEdges(M,I45);
for(M[I123]=minM(I123,M); M[I123]<=nRemEdges[I123]; M[I123]++) {
    nRemEdges[I124] = nEdges-numEdges(M,I123);
for(M[I124]=minM(I124,M); M[I124]<=nRemEdges[I124]; M[I124]++) {
    nRemEdges[I125] = nEdges-numEdges(M,I124);
for(M[I125]=minM(I125,M); M[I125]<=nRemEdges[I125]; M[I125]++) {
    nRemEdges[I134] = nEdges-numEdges(M,I125);
for(M[I134]=minM(I134,M); M[I134]<=nRemEdges[I134]; M[I134]++) {
    nRemEdges[I135] = nEdges-numEdges(M,I134);
for(M[I135]=minM(I135,M); M[I135]<=nRemEdges[I135]; M[I135]++) {
    nRemEdges[I145] = nEdges-numEdges(M,I135);
for(M[I145]=minM(I145,M); M[I145]<=nRemEdges[I145]; M[I145]++) {
    nRemEdges[I234] = nEdges-numEdges(M,I145);
for(M[I234]=minM(I234,M); M[I234]<=nRemEdges[I234]; M[I234]++) {
    nRemEdges[I235] = nEdges-numEdges(M,I234);
for(M[I235]=minM(I235,M); M[I235]<=nRemEdges[I235]; M[I235]++) {
    nRemEdges[I245] = nEdges-numEdges(M,I235);
for(M[I245]=minM(I245,M); M[I245]<=nRemEdges[I245]; M[I245]++) {
    nRemEdges[I345] = nEdges-numEdges(M,I245);
for(M[I345]=minM(I345,M); M[I345]<=nRemEdges[I345]; M[I345]++) {



    nRemEdges[I1234] = nEdges-numEdges(M,I345);
for(M[I1234]=minM(I1234,M); M[I1234]<=nRemEdges[I1234]; M[I1234]++) {
    nRemEdges[I1235] = nEdges-numEdges(M,I1234);
for(M[I1235]=minM(I1235,M); M[I1235]<=nRemEdges[I1235]; M[I1235]++) {
    nRemEdges[I1245] = nEdges-numEdges(M,I1234);
for(M[I1245]=minM(I1245,M); M[I1245]<=nRemEdges[I1245]; M[I1245]++) {
```

```
        nRemEdges[I1345] = nEdges-numEdges(M,I1245);
    for(M[I1345]=minM(I1345,M); M[I1345]<=nRemEdges[I1345]; M[I1345]++) {

        // Set M[I2345] so that the number of edges in the biclique is 'nEdges'.
        M[I2345] = nEdges-numEdges(M, I1345);

        // Convert M[] to N[].
        convertMtoN(M, N);

        // Print coefficients of interesting factor.
        for(n=DEG_IF; n>=0; n--)
            printf("%ld%c", coeffIntFact(N, n), n>0 ? ',' : ':');

        // Print parameters of biclique.
        for(i=0; i<NUM_PARAMS; i++)
            printf("%ld%c", N[i], i<NUM_PARAMS-1 ? ',' : '\n');

    }}}}}}}}}}}}}}}}}}}}}}}}}}}}

}
```

nf_disc.c

```
#include <stdio.h>
#include <stdlib.h>
#include <string.h>
#include <pari/pari.h>

// Computes the field discriminant of the polyomial in the field specified by
// the first command line argument (fields are delimited by ':') and prints it
// at the start of each line. Lines ared read from STDIN and written to STDOUT.
int main(int argc, char *argv[]) {

    int iPolField = atoi(argv[1]);

    char *line = NULL;
    char *lineCopy = NULL;
    char *strPoly = NULL;
    size_t len = 0;

    GEN p, x;
    pari_init(1000000, 2);
    x = pol_x(fetch_user_var("x"));
    pari_sp av = avma;

    while (getline(&line, &len, stdin) > 1) {

        // Remove end of line character from 'line'
        line[strlen(line)-1] = '\0';

        // Get string representing polynomial.
        lineCopy = strdup(line);
        strPoly = strtok(lineCopy, ":");
        int i = 0;
        for (i = 0; i<iPolField-1; i++) strPoly = strtok(NULL, ":"  );

        // Create polynomial from coefficients
        int j;
        int deg = 0;
```

```
        for(j=0; strPoly[j]!='\0'; j++) if(strPoly[j]==',') deg++;
        p = gmulsg(0, x);
        char *n;
        n = strtok(strPoly, ",");
        for(j=0; j<=deg; j++) {
            p = gadd(p, gmulsg(atoi(n), gpowgs(x,deg-j)));
            n = strtok(NULL, ",");
        }

        // Print discriminant if polynomial is irreducible.
        if (isirreducible(p)) {
            pari_printf("%Ps:", nfdisc(p));
            printf("%s\n", line);
        }

        free(lineCopy);
        avma = av;

    }

    if (line) free(line);
    pari_close();
    exit(EXIT_SUCCESS);

}
```

filter_disc.c

```
#include <stdio.h>
#include <stdlib.h>
#include <string.h>

// Reads the field discriminant in the field (delimited by ':') specified by the
// first command line argument lines and prints the line if the disciminant is
// within the bounds specified by the second and third arguments.
int main(int argc, char *argv[]) {

    int iDiscField = atoi(argv[1]);
    long long int minDisc = atoi(argv[2]);
    long long int maxDisc = atoi(argv[3]);

    char *line = NULL;
    char *lineCopy = NULL;
    char *strDisc = NULL;
    size_t len = 0;

    int i;
    long long int D;

    while (getline(&line, &len, stdin) > 1) {

        // Remove end of line character from 'line'
        line[strlen(line)-1] = '\0';

        // Get number field discriminant,
        lineCopy = strdup(line);
        strDisc = strtok(lineCopy, ":");
        for (i = 0; i<iDiscField-1; i++) strDisc = strtok(NULL, ":" );
        D = atoll(strDisc);
```

```
        // Print 'line' if discriminant is within bounds.
        if (D >= minDisc && D <= maxDisc) printf("%s\n", line);

        free(lineCopy);

    }

    if (line) free(line);

    exit(EXIT_SUCCESS);

}
```

red_pol.c

```
#include <stdio.h>
#include <stdlib.h>
#include <string.h>
#include <pari/pari.h>

// Computes the reduced polynomial of the polyomial in the field specified
// by the first command line argument (fields are delimited by ':') and appends
// it to the end of each line. Lines ared read from STDIN and written to STDOUT.
int main(int argc, char *argv[]) {

    int iPolField = atoi(argv[1]);

    char *line = NULL;
    char *lineCopy = NULL;
    char *strPoly = NULL;
    size_t len = 0;

    GEN p,rp, x;
    pari_init(1000000, 2);
    x = pol_x(fetch_user_var("x"));
    pari_sp av = avma;

    int i;
    int deg;
    char *n;

    while (getline(&line, &len, stdin) > 1) {

        // Remove end of line character from 'line'.
        line[strlen(line)-1] = '\0';

        // Get string representing polynomial.
        lineCopy = strdup(line);
        strPoly = strtok(lineCopy, ":");
        for (i = 0; i<iPolField-1; i++) strPoly = strtok(NULL, ":"  );

        // Create polynomial from coefficients.
        deg = 0;
        for(i=0; strPoly[i]!='\0'; i++) if(strPoly[i]==',') deg++;
        p = gmulsg(0, x);
        n = strtok(strPoly, ",");
        for(i=deg; i>=0; i--) {
            p = gadd(p, gmulsg(atoi(n), gpowgs(x,i)));
```

```
            n = strtok(NULL, ",");
        }

        // Print reduced polynomial.
        if (isirreducible(p)) {
            printf("%s:", line);
            rp = polredabs(p);
            for (i=deg; i>=0; i--)
                pari_printf("%Ps%c", truecoeff(rp, i), i>0 ? ',' : '\n');
        }

        free(lineCopy);
        avma = av;

    }

    if (line) free(line);
    pari_close();
    exit(EXIT_SUCCESS);

}
```

UniqRedPol.java

```
import java.io.BufferedReader;
import java.io.InputStreamReader;
import java.util.Set;
import java.util.HashSet;
import java.util.HashMap;

// Reads reduced polynopmials from STDIN and prints each
// line to STDOUT if that reduced polynomial has not yet been seen.
public class UniqRedPol {

    public static void main(String[] args) {

        try {

            Integer iDiscField = new Integer(args[0]);
            Integer iPolField = new Integer(args[1]);
            String line;
            String[] tokens;
            Long disc;
            String redPol;
            Set<String> polys;

            BufferedReader br;
            br = new BufferedReader(new InputStreamReader(System.in));
            HashMap<Long,Set<String>> map = new HashMap<Long,Set<String>>();

            while( (line=br.readLine()) != null) {

                tokens = line.split(":");
                disc = new Long(tokens[iDiscField-1]);
                redPol = tokens[iPolField-1];

                if (map.containsKey(disc)) {
                    polys = map.get(disc);
                    if (polys.add(redPol)) System.out.println(line);
```

```
                }
                else {
                    polys = new HashSet<String>();
                    polys.add(redPol);
                    map.put(disc, polys);
                    System.out.println(line);
                }

            }

            br.close();

        }
        catch(Exception e) {
            System.out.println(e.toString());
        }

    }

}
```

ComputeIF.java

```
import java.util.*;

public class ComputeIF {

    // Print the interesting factor of a (j,k)-biclique suitable for use in
    // a computer algebra package. The degree of the intersting factor, j,
    // is given by the value of args[0].
    public static void main(String[] args) {
        int j = (new Integer(args[0])).intValue();
        System.out.println(interestingFactor(j));
    }

    // Returns a string representing the
    // interesting factor of an (n,k)-biclique.
    private static String interestingFactor(int n) {
        String iFact = "";
        ArrayList<ArrayList<String>> partitions = getPartitions(n);
        for (int i = 0; i < partitions.size(); i++) {
            ArrayList<String> partition = partitions.get(i);
            int c=1;
            String fact = "";
            for (int j=0; j < partition.size(); j++) {
                c = c*fact(partition.get(j).length() - 1);
                fact = fact + "(x-a" + partition.get(j) + ")";
                if (j < partition.size()-1) fact = fact + "*";
            }
            fact = c + "*" + fact;
            if ((partition.size()+n) % 2 == 0) iFact = iFact + " + " + fact;
            else iFact = iFact + " - " + fact;
        }
        return iFact;
    }

    // Returns an ArrayList of all partitions of the set {1,2,...,i}.
    // Each partition is represented by an ArrayList<String>.
    private static ArrayList<ArrayList<String>> getPartitions(int i) {
```

```
        ArrayList<ArrayList<String>> partitions = \
            new ArrayList<ArrayList<String>>();

        if (i == 1) {
            ArrayList<String> partition = new ArrayList<String>();
            partition.add("1");
            partitions.add(partition);
        }
        else {
            for (ArrayList<String> partition : getPartitions(i-1)) {
                for (int j = 0; j <= partition.size(); j++) {
                    ArrayList<String> newPart = cpyPartition(partition);
                    if (j < partition.size())
                        newPart.set(j,newPart.get(j).concat(String.valueOf(i)));
                    else
                        newPart.add(new String(String.valueOf(i)));
                    partitions.add(newPart);
                }
            }
        }

        return partitions;

    }

    // Creates and returns a new ArrayList<String>
    // with the same contents as 'partition'.
    private static ArrayList<String> cpyPartition(ArrayList<String> partition) {
        ArrayList<String> newPart = new ArrayList<String>();
        for (String s : partition) newPart.add(new String(s));
        return newPart;
    }

    // Converts an ArrayList<String> representing a partition to a String.
    private static String partitionToString(ArrayList<String> partition) {
        String s = "";
        for (String part : partition) s = s + part + ",";
        return s;
    }

    // The factorial function.
    private static int fact(int n) {
        if (n == 0) return 1;
        else return n*fact(n-1);
    }

}
```