p-Adic Roots of Chromatic Polynomials

Paul Buckingham[1]

Abstract

The complex roots of the chromatic polynomial $P_G(x)$ of a graph G have been well studied, but the p-adic roots have received no attention as yet. We consider these roots, specifically the roots in the ring $\mathbb{Z}_p$ of p-adic integers. We first describe how the existence of p-adic roots is related to the p-divisibility of the number of colourings of a graph—colourings by at most k colours and also ones by exactly k colours. Then we turn to the question of the circumstances under which $P_G(x)$ splits completely over $\mathbb{Z}_p$, giving some generalities before considering in detail an infinite family of graphs whose chromatic polynomials have been discovered, by Morgan [10], to each have a cubic abelian splitting field.

Keywords: chromatic polynomials; chromatic roots; p-adic numbers

Mathematics Subject Classification (2010): 05C31, 05C15

1 Introduction

The chromatic polynomial $P_G(x)$ of a graph, being a monic polynomial with integer coefficients, has naturally attracted attention for its potential algebraic properties. The roots of $P_G(x)$ in $\mathbb{C}$, called *chromatic roots*, are algebraic integers in the sense of algebraic number theory, and of course generate finite extensions of $\mathbb{Q}$, i.e., number fields.

Chromatic roots are known to be dense in the complex plane by a theorem of Sokal [14]. Cameron's conjecture that every algebraic integer differs from a chromatic root by a natural number has been proven for algebraic integers of degree 2 and of degree 3—see [3] and [1] respectively. The Galois groups of chromatic polynomials have been worked out for several infinite families of graphs—in [4] and [10], for example. Intriguingly, the coefficients of chromatic polynomials have homological interpretations [6, 7].

Missing so far from the study of chromatic polynomials is consideration of their p-adic roots. The fields of p-adic numbers—by definition, the completions of $\mathbb{Q}$ at the non-archimedean absolute values—are central to algebraic number theory and appear in many other areas of mathematics besides. The p-adic numbers play a role in number theory akin to the role of power series in analysis and are therefore indispensible.

To the best of our knowledge, the present paper is the first to consider the p-adic roots of chromatic polynomials. We begin by briefly introducing p-adic numbers, and in particular the ring $\mathbb{Z}_p$ of p-adic integers. We then describe how the p-adic roots of a chromatic polynomial are related to the p-divisibility of

[1]E-mail address: p.r.buckingham@ualberta.ca

$P_G(k)$, i.e., the number of colourings of G by (at most) k colours, and also to the p-divisibility of the number of colourings by exactly k colours (Proposition 2). These relationships are straightforward but worth mentioning for completeness.

In the rest of the paper, we consider the question of when $P_G(x)$ has as many p-adic roots as possible for a polynomial of its degree. In other words, we consider when $P_G(x)$ splits completely over $\mathbb{Z}_p$. The question of when a polynomial with integer coefficients splits completely over $\mathbb{Z}_p$ has a well-known general interpretation (Theorem 8), but inspired by a certain family of graphs studied by Morgan [10] whose chromatic polynomials have abelian splitting fields, we focus on the abelian case. Here, results from class field theory may be brought to bear, and after describing some general consequences for chromatic polynomials in Section 5.1, we examine Morgan's family in detail in Section 5.2. In Theorem 19, we establish that the graphs in Morgan's family are *chromatically contained* (see Definition 15) in explicitly determined cycle graphs. From this fact we deduce certain results on the splitting over $\mathbb{Z}_p$ of the chromatic polynomials in Morgan's family.

Very few infinite families of graphs have been found in which the chromatic polynomials all have abelian Galois group. Examples are cycle graphs, certain rings of cliques where quadratic integers come into play [3], Morgan's family just referred to, and one more family of Morgan, but aside from cycle graphs, the proofs that they have abelian Galois groups are all quite recent. This paper treats splitting over $\mathbb{Z}_p$ for all these except for the quadratic case, but it is clear how the methods of this paper can be applied in that case.

There is hope that new families with abelian Galois groups will be found soon. Delbourgo and Morgan [5] have very recently described an algorithm to produce a (d, N)-biclique for which the splitting field of the chromatic polynomial is the splitting field of a given monic polynomial of degree $d \leq 4$, if such a biclique exists. (Bohn [1] had an earlier algorithm in the case $d = 3$.)

2 Notation and key concepts

2.1 Vertex colourings

Throughout, G will be a simple graph, i.e., it will have no loops or multiple edges. We denote its chromatic polynomial by $P_G(x)$. Then for a positive integer k, $P_G(k)$ is the number of (proper) vertex colourings of G by a set of k colours.

We will also consider the notion of *colourings with colour indifference*, as Read [12] puts it. Under this notion, two colourings are considered the same if one may be obtained from the other simply via a permutation of the colours. Thus, a colouring with colour indifference is a partition of the vertex set such that adjacent vertices are in different sets. Further, if k is a positive integer, we will denote by $c_{G,k}$ the number of colourings, with colour indifference, that use *exactly* k colours. Thus, $c_{G,k}$ is the number of vertex partitions of size exactly k where adjacent vertices are in different sets.

As Read shows,

$$P_G(x) = \sum_{k=1}^{n} c_{G,k}(x)_k,$$

where n is the number of vertices in G and $(x)_k = x(x-1)(x-2)\cdots(x-k+1)$.

2.2 p-Adic integers

We provide a brief overview of the basics of p-adic integers and p-adic numbers. For a fuller account, the reader may consult the book by Koblitz [8], for example.

Let p be a prime number. A p-adic integer may be thought of as an infinite sum

$$a_0 + a_1 p + a_2 p^2 + \cdots \tag{1}$$

where $a_n \in \{0, 1, \ldots, p-1\}$ for each n. The set of all p-adic integers is denoted $\mathbb{Z}_p$ (not to be confused with the integers mod p). It forms a ring in which addition and multiplication are defined rather like in the ring of power series in a variable x, except that if adding or multiplying coefficients results in a number greater than or equal to p, then we leave the remainder mod p where it is and carry everything else over to the next term along.

The usual ring of integers $\mathbb{Z}$ is a subring of $\mathbb{Z}_p$. Any non-negative element of $\mathbb{Z}$ may be considered to be a sum as in (1) where all the a_n after some a_N are zero. A negative integer $-a \in \mathbb{Z}$ is the infinite sum resulting from multiplying the finite sum representing $a \geq 0$ by the infinite sum

$$-1 = (p-1) + (p-1)p + (p-1)p^2 + \cdots .$$

We will also need the field $\mathbb{Q}_p$ of p-adic numbers. It is the field of fractions of $\mathbb{Z}_p$, and its elements are the infinite sums

$$\alpha = \sum_{n=N}^{\infty} a_n p^n \tag{2}$$

where now N may be negative. Being the field of fractions of $\mathbb{Z}_p$, which contains $\mathbb{Z}$, $\mathbb{Q}_p$ contains the field $\mathbb{Q}$ of rational numbers, the field of fractions of $\mathbb{Z}$.

Other constructions of $\mathbb{Z}_p$ and $\mathbb{Q}_p$ exist. For example, one often constructs $\mathbb{Q}_p$ as the completion of $\mathbb{Q}$ with respect to the p-adic absolute value $|a|_p = p^{-v_p(a)}$, where v_p denotes the p-adic valuation on $\mathbb{Q}$. The p-adic valuation (along with the p-adic absolute value) extends to $\mathbb{Q}_p$ by continuity, and then for α as in (2), $v_p(\alpha) = N$ if $a_N \neq 0$.

Because $\mathbb{Q}_p$ is a field containing $\mathbb{Q}$, we may evaluate polynomials in $\mathbb{Q}[x]$ at p-adic numbers and, in particular, p-adic integers. Of special significance are the monic polynomials in $\mathbb{Z}[x]$, since any root in $\mathbb{Q}_p$ of such a polynomial is necessarily in $\mathbb{Z}_p$.

Polynomials that do not have rational roots may nonetheless have p-adic roots for various p. For example, the polynomial $x^2 + 1$ has two roots $\alpha, \beta \in \mathbb{Z}_5$,

beginning as follows:

$$\begin{aligned}\alpha &= 2+5+2\cdot 5^2+5^3+3\cdot 5^4+\cdots\\ \beta &= 3+3\cdot 5+2\cdot 5^2+3\cdot 5^3+5^4+\cdots.\end{aligned}$$

In fact, x^2+1 has roots in $\mathbb{Z}_p$ if and only if $p\equiv 1 \bmod 4$. One may compute p-adic roots of a polynomial in $\mathbb{Z}[x]$ using Hensel's Lemma [9, Chap. II, Sect. 2, Prop. 2].

Let us consider our first example arising from a graph. If C_4 is the cycle graph on 4 vertices, then $P_G(x)=x(x-1)(x^2-3x+3)$. This polynomial certainly has the p-adic roots 0 and 1, but for infinitely many primes p it has two more, the roots of x^2-3x+3 in $\mathbb{Z}_p$. For example, in $\mathbb{Z}_7$ this factor has roots α,β beginning

$$\begin{aligned}\alpha &= 4+4\cdot 7+6\cdot 7^2+3\cdot 7^3+2\cdot 7^4+\cdots\\ \beta &= 6+2\cdot 7+3\cdot 7^2+6\cdot 7^3+4\cdot 7^4+\cdots.\end{aligned}$$

The factor x^2-3x+3 has roots in $\mathbb{Z}_p$ if and only if $p\equiv 1 \bmod 3$.

Of special importance is the group of units in the ring $\mathbb{Z}_p$, denoted $\mathbb{Z}_p^\times$. It consists of all those p-adic integers $a_0+a_1p+\cdots$ where $a_0\in\{1,\ldots,p-1\}$, i.e., $a_0\neq 0$. Equivalently, a p-adic integer α is in $\mathbb{Z}_p^\times$ if and only if $v_p(\alpha)=0$.

We also extend the notion of congruence to $\mathbb{Z}_p$. If $r\geq 0$ and $\alpha,\beta\in\mathbb{Z}_p$, we say that $\alpha\equiv\beta \bmod p^r$ if $p^r\,|\,\alpha-\beta$, i.e., $v_p(\alpha-\beta)\geq r$. For example, $2+7+5\cdot 7^2+4\cdot 7^3+\cdots$ and $2+7+5\cdot 7^2+6\cdot 7^3+\cdots$ are congruent to each other mod 7^3 but not mod 7^4.

3 Interpreting the p-adic roots of a chromatic polynomial

Suppose $\alpha=a_0+a_1p+a_2p^2+\cdots$ is a root of $P_G(x)$ in $\mathbb{Z}_p$. A first approximation shows that p divides the number of a_0-colourings of G. Indeed, in $\mathbb{Z}/p\mathbb{Z}$,

$$\begin{aligned}\overline{P_G(a_0)} &= P_G(\overline{a}_0)\\ &= P_G(\overline{\alpha})\\ &= \overline{P_G(\alpha)}\\ &= \overline{0},\end{aligned}$$

where $\overline{\beta}$ is the residue class mod p of an element $\beta\in\mathbb{Z}_p$. Given any $r\geq 1$, we may extend this idea to find a positive integer b_r such that p^r divides the number of b_r-colourings of G. If we define $b_r=\sum_{k=0}^{r-1}a_kp^k$, then $b_r\equiv\alpha \bmod p^r$, so the same calculation as above, performed this time in $\mathbb{Z}/p^r\mathbb{Z}$, shows that $p^r\,|\,P_G(b_r)$.

We remark in passing that we may use this simple argument to make the following observation.

Proposition 1. *If $a\in\mathbb{Z}\setminus\{0,1,\ldots,\chi-1\}$, where χ is the chromatic number of G, then there are at most finitely many primes p such that $P_G(x)$ has a root in $\mathbb{Z}_p$ congruent to a mod p.*

Proof. If $P_G(x)$ has a root $\alpha \in \mathbb{Z}_p$ such that $\alpha \equiv a \bmod p$, then $p \,|\, P_G(a)$ by the same argument as above. But our assumption on a implies that $P_G(a)$ is non-zero, so only finitely many primes divide it. □

Recall from Section 2.1 that $c_{G,k}$ is the number of colourings of G, with colour indifference, that use exactly k colours ($k \geq 1$). Of course, $c_{G,k} = 0$ if $k < \chi$ or $k > n$, where χ is the chromatic number of G and n is the number of vertices.

We have the following relationship between p-adic roots of $P_G(x)$ and the numbers $c_{G,k}$.

Proposition 2. *Let G be a graph with chromatic number χ, and suppose p is a prime and r is a positive integer. Assume that, for some I with $\chi \leq I < p$, there are roots $\alpha_\chi, \alpha_{\chi+1}, \ldots, \alpha_I$ of $P_G(x)$ in $\mathbb{Z}_p$ such that $\alpha_i \equiv i \bmod p^r$ for $\chi \leq i \leq I$. Then $p^r \,|\, c_{G,i}$ for $\chi \leq i \leq I$.*

Before proving this proposition, we illustrate it with some examples.

Example. Let G be the graph obtained by identifying a vertex in C_8 with a vertex in K_5. Then $P_G(x) = \frac{1}{x}(x)_5 P_{C_8}(x)$, and $\chi = 5$. The chromatic polynomial of G has roots in $\mathbb{Z}_{29}$ congruent to 5, 6, and 7 mod 29, so according to Proposition 2, 29 should divide $c_{G,5}$, $c_{G,6}$, and $c_{G,7}$. And indeed, we have the following prime factorizations:

$$\begin{aligned} c_{G,5} &= 2^2 \cdot 29 \cdot 113 \\ c_{G,6} &= 11 \cdot 29 \cdot 163 \\ c_{G,7} &= 2 \cdot 3 \cdot 29 \cdot 353. \end{aligned}$$

It is possible to have arbitrarily large integers I appear in the proposition, as the following example shows.

Example. Let $G = C_p$, where $p \geq 5$ is prime. Then $p \,|\, c_{G,3}, c_{G,4}, \ldots, c_{G,p-1}$. To see how this follows from the proposition, observe that $P_{C_p}(x) = Q_p(x-1)$, where $Q_p(y) = y^p - y$, so Fermat's Little Theorem implies that every integer is a root of $P_{C_p}(x) \bmod p$. Therefore, for each $i \in \{0, \ldots, p-1\}$, there is a root α_i of $P_{C_p}(x)$ in $\mathbb{Z}_p$ congruent to i mod p by Hensel's Lemma. We may now apply the proposition, observing that the chromatic number χ of G is equal to 3. The prism graph (or circular ladder graph) on $2p$ vertices plays out the same way.

Strictly speaking, we did not need to invoke Hensel's Lemma in the above example. Proposition 2 remains true if we replace the assumption that each α_i be a root of $P_G(x)$ by the weaker assumption that $p^r \,|\, P_G(\alpha_i)$. Therefore, because we are taking $r = 1$ in this example, we could have chosen simply $\alpha_i = i$.

There is nonetheless an advantage in formulating the proposition in terms of p-adic *roots* rather than simply divisibility by p^r. All of the divisibilities $p^r \,|\, P_G(\alpha)$ are of course true for a p-adic root α, so if we have p-adic roots α_i in hand, then all we have to do to apply the proposition is check the congruence conditions $\alpha_i \equiv i \bmod p^r$.

Remark. *Although more rare, examples exist where $r \geq 2$ in Proposition 2, so the greater generality of allowing $r \geq 1$ rather than just $r = 1$ is not redundant.*

Example. We give a slightly more interesting example, involving theta graphs. For positive integers a_1, a_2, a_3, let θ_{a_1,a_2,a_3} be the graph obtained by taking three disjoint paths of lengths a_1, a_2, a_3 respectively and then identifying the three initial vertices with one another and also identifying the three terminal vertices with one another. The chromatic polynomials of these theta graphs (and their natural generalization that takes arbitrarily many paths) have been calculated already; see [2]. If $p \geq 7$ is prime, then the chromatic polynomial of $G = \theta_{p-2,p-1,p}$ has roots in $\mathbb{Z}_p$ congruent to all integers mod p. Indeed, $P_G(x)$ is divisible by the polynomial $(x-1)^p - (x-1)$, as demonstrated in [4, Section 2], for example. Therefore, since the chromatic number of G is 3, Proposition 2 shows that p divides $c_{G,3}, c_{G,4}, \ldots, c_{G,p-1}$.

We now turn to the proof of Proposition 2. For a polynomial $f(x) \in \mathbb{Q}[x]$ of degree n, the *factorial representation* of $f(x)$ is the representation of it as a sum

$$f(x) = \sum_{k=0}^{n} c_k (x)_k$$

with $c_k \in \mathbb{Q}$, where $(x)_k = x(x-1)(x-2)\cdots(x-k+1)$. The numbers c_k are uniquely determined by $f(x)$. As we remarked in the introduction, the factorial representation of $P_G(x)$ is

$$P_G(x) = \sum_{k=1}^{n} c_{G,k} (x)_k,$$

where n is the number of vertices in G.

Our proof of Proposition 2 rests on the following lemma. The symbol $\nmid$ means *does not divide*.

Lemma 3. *Let $f(x) \in \mathbb{Z}[x]$ be monic of degree n, and let $f(x) = \sum_{k=0}^{n} c_k (x)_k$ be its factorial representation. Choose a prime p and an integer $r \geq 1$, and let l be least such that $p^r \nmid c_l$. If $l < p$ and $\alpha \in \mathbb{Z}_p$ is congruent to l mod p^r, then $p^r \nmid f(\alpha)$.*

Proof. Note that a least l such that $p^r \nmid c_l$ exists because $c_n = 1$, $f(x)$ being monic. Now, because $\alpha \equiv l \bmod p^r$, we have $(\alpha)_k \in p^r \mathbb{Z}_p$ for $k > l$. Further, $c_k \in p^r \mathbb{Z}_p$ for $k < l$ by assumption, so

$$f(\alpha) - c_l (\alpha)_l = \sum_{k \neq l} c_k (\alpha)_k \in p\mathbb{Z}_p.$$

It therefore remains to show that $c_l (\alpha)_l \notin p^r \mathbb{Z}_p$. By definition of l, $c_l \notin p^r \mathbb{Z}_p$. As for $(\alpha)_l$, the l factors $\alpha, \alpha - 1, \ldots, \alpha - l + 1$ are congruent mod p to $l, l-1, \ldots, 1$ respectively, none of which is congruent to 0 mod p because $l < p$. Therefore, $(\alpha)_l \in \mathbb{Z}_p^\times$, so $c_l (\alpha)_l \notin p^r \mathbb{Z}_p$. □

Example. Let $p = 5$ and $r = 2$, and suppose $f(x)$ is a monic degree-6 polynomial in $\mathbb{Z}[x]$ whose factorial representation has coefficients c_k with the following 5-adic valuations:

k	0	1	2	3	4	5	6
$v_5(c_k)$	∞	3	4	1	1	1	0

(The symbol ∞ for $v_5(c_0)$ indicates that $c_0 = 0$.) The least l such that 5^2 does not divide c_l is $l = 3$. Therefore, because $3 < 5$, i.e., $l < p$, any 5-adic integer $\alpha \equiv 3 \bmod 5^2$ satisfies $5^2 \nmid f(\alpha)$.

Our proof of Proposition 2 is now finished as follows. Suppose that we have $\alpha_\chi, \alpha_{\chi+1}, \ldots, \alpha_I$ as in the statement of the proposition, so that α_i is a root of $P_G(x)$ in $\mathbb{Z}_p$ congruent to i mod p^r, and let $\alpha_i = i$ for $i \in \{0, \ldots, \chi - 1\}$. Then $P_G(\alpha_i) = 0$ for $i \in \{0, \ldots, I\}$. In particular, $p^r \mid P_G(\alpha_i)$ for $i \in \{0, \ldots, I\}$.

Let l be least such that $p^r \nmid c_{G,l}$. We claim that $I < l$. If not, then we would have the following:

(i) $l \leq I < p$.

(ii) $\alpha_l \equiv l \bmod p^r$.

(iii) $p^r \mid P_G(\alpha_l)$.

But this contradicts Lemma 3 with $f(x) = P_G(x)$ and $\alpha = \alpha_l$. (In applying the lemma, we use the fact that the numbers $c_{G,k}$ are the coefficients in the factorial representation of $P_G(x)$.) Therefore, $I < l$, so $p^r \mid c_{G,i}$ for all $i \leq I$.

4 Background on class field theory

The results in Section 5 concerning the splitting of chromatic polynomials over $\mathbb{Z}_p$ rely on some algebraic number theory.

4.1 Principal results from class field theory

We first collect together the main results we will use from class field theory. All we will need is class field theory over $\mathbb{Q}$.

Theorem 4 (Kronecker–Weber)**.** *Every finite abelian extension of $\mathbb{Q}$ is contained in a cyclotomic field, i.e., a field $\mathbb{Q}(\zeta)$ where ζ is a root of unity.*

We typically denote a primitive nth root of unity by ζ_n. The particular choice rarely matters. If $L/\mathbb{Q}$ is an abelian extension, the smallest n such that $L \subseteq \mathbb{Q}(\zeta_n)$ is called the *conductor* of $L/\mathbb{Q}$. A prime p ramifies in $L/\mathbb{Q}$ if and only if it divides the conductor.

For each prime residue class $\overline{a} \in (\mathbb{Z}/n\mathbb{Z})^\times$, there is a unique automorphism $\varphi_a \in \mathrm{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{Q})$ satisfying $\varphi_a(\zeta_n) = \zeta_n^a$, and the map

$$\begin{array}{ccc} (\mathbb{Z}/n\mathbb{Z})^\times & \to & \mathrm{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{Q}) \\ \overline{a} & \mapsto & \varphi_a \end{array}$$

is an isomorphism. Therefore, via Galois theory, the subfields of $\mathbb{Q}(\zeta_n)$ are in bijection with the subgroups of $(\mathbb{Z}/n\mathbb{Z})^\times$. If $L \subseteq \mathbb{Q}(\zeta_n)$, let H_L^n be the corresponding subgroup of $(\mathbb{Z}/n\mathbb{Z})^\times$, i.e., the subgroup consisting of prime residue classes a mod n such that φ_a is the identity on L.

A prime p is said to *split completely* in an extension $L/\mathbb{Q}$ of finite degree d if the ideal $p\mathcal{O}_L$ in the ring of integers $\mathcal{O}_L$ of L factorizes as a product of d distinct prime ideals, the maximum number possible in such a factorization. The following is a special case of [11, Chap. VI, Theorem 7.3].

Theorem 5. *Let $L/\mathbb{Q}$ be an abelian extension contained in $\mathbb{Q}(\zeta_n)$. If $p \nmid n$ is a prime, then p splits completely in $L/\mathbb{Q}$ if and only if the class of p mod n is in H_L^n. If n is divisible only by the ramified primes (for example, if n is the conductor), then the primes that split completely in $L/\mathbb{Q}$ are precisely those whose residue classes are in H_L^n.*

Example. Let $L = \mathbb{Q}(\alpha)$, where α is a root of $f(x) = x^3 - 3x + 1$. By considering the discriminant 9^2 of the polynomial $f(x)$, we find that $L/\mathbb{Q}$ is abelian with conductor 9 and is therefore contained in $\mathbb{Q}(\zeta_9)$. Because $(\mathbb{Z}/9\mathbb{Z})^\times$ is cyclic of order 6, it has a unique subgroup of index 3, namely, $\{\overline{1}, \overline{8}\} = \{\overline{1}, \overline{-1}\}$. Therefore, $H_L^9 = \{\overline{1}, \overline{-1}\}$, which is to say that L is the fixed field in $\mathbb{Q}(\zeta_9)$ of the automorphism $\zeta_9 \mapsto \zeta_9^{-1}$. By Theorem 5, a prime splits completely in $L/\mathbb{Q}$ if and only if it is congruent to ± 1 mod 9.

In the case where L is itself a cyclotomic field, Theorem 5 gives the following.

Proposition 6. *If $n \geq 3$, then a prime p splits completely in $\mathbb{Q}(\zeta_n)/\mathbb{Q}$ if and only if $p \equiv 1$ mod n.*

Definition 7. *If $f(x) \in \mathbb{Z}[x]$ is a monic polynomial and p a prime, we will say that $f(x)$ splits completely over $\mathbb{Z}_p$ if it is the product of linear factors $x - \alpha$ where each α is in $\mathbb{Z}_p$.*

A version of the following theorem holds for polynomials over the ring of integers of any number field. Since we need only the case of polynomials with coefficients in $\mathbb{Z}$, we give only this simplified version. The advantage is that not as much technical background is required to state the theorem in this form.

Theorem 8. *Let $f(x) \in \mathbb{Z}[x]$ be a monic irreducible polynomial, and L the extension of $\mathbb{Q}$ generated by a chosen root of $f(x)$. For a given prime p, the following are equivalent:*

(i) $f(x)$ splits completely over $\mathbb{Z}_p$.

(ii) p splits completely in $L/\mathbb{Q}$.

(iii) p splits completely in the splitting field $K_{f(x)}$ of $f(x)$.

If, in addition, $L \subseteq \mathbb{Q}(\zeta_n)$ where n is a positive integer divisible only by primes that ramify in $L/\mathbb{Q}$, then (i)–(iii) are equivalent to each of the following:

(iv) $f(x)$ *has a root in* $\mathbb{Z}_p$.

(v) p *is coprime to* n*, and its residue class mod* n *lies in* H_L^n.

Proof. The equivalence of (ii) and (iii) is simply a result of the fact that a prime that splits completely in each of two extensions $E/\mathbb{Q}$ and $F/\mathbb{Q}$ splits completely in the compositum [11, Chap. I, Sect. 8, Exercise 3]. For the equivalence of (i) and (ii), note that $f(x)$ splits completely over $\mathbb{Z}_p$ if and only if it splits completely over $\mathbb{Q}_p$, since it is monic with coefficients in $\mathbb{Z}$. Now use the fact that the irreducible factors in the factorization of $f(x)$ over $\mathbb{Q}_p$ correspond bijectively to the primes of L above p [11, Chap. II, Prop. 8.2].

Now assume that $L \subseteq \mathbb{Q}(\zeta_n)$ for n of the type specified in the second half of the theorem. (For example, n could be the conductor.) The equivalence of (v) and (ii) is Theorem 5. We will therefore be done once we show that, if $f(x)$ has a root in $\mathbb{Z}_p$, then it has all its roots in $\mathbb{Z}_p$. If α_0 is a root of $f(x)$ in $\mathbb{Z}_p$, then $\mathbb{Q}(\alpha_0)/\mathbb{Q}$ is abelian (because $L/\mathbb{Q}$ is), so $\mathbb{Q}(\alpha_0)$ contains all the roots of $f(x)$. Since $\mathbb{Q}(\alpha_0) \subseteq \mathbb{Q}_p$ and $f(x) \in \mathbb{Z}[x]$ is monic, we are done. □

Corollary 9. *If* $f(x) \in \mathbb{Z}[x]$ *is monic (but not necessarily irreducible), then* $f(x)$ *splits completely over* $\mathbb{Z}_p$ *if and only if* p *splits completely in the splitting field* $K_{f(x)}$ *of* $f(x)$.

Proof. Apply the theorem to each of the irreducible factors in $f(x)$. □

We will also use the next result, which is [11, Chap. VII, Prop. 13.9].

Proposition 10. *If* E/K *and* F/K *are extensions of number fields and* E/K *is Galois, then* $E \subseteq F$ *if and only if every prime that splits completely in* F/K *also splits completely in* E/K.

4.2 Additional class-field-theoretic results

We remind the reader that, if m is a positive integer, a Galois extension is said to have exponent m if its Galois group does, i.e., if $\sigma^m = 1$ for all σ in the Galois group and m is least with this property.

Lemma 11. *Let* $L/\mathbb{Q}$ *be an abelian extension of exponent* m *and conductor dividing* n*. If* $p \nmid n$ *is a prime congruent to an* m*th power mod* n*, then* p *splits completely in* $L/\mathbb{Q}$*. In particular, if* p *has prime-to-*m *order in* $(\mathbb{Z}/n\mathbb{Z})^\times$*, then* p *splits completely.*

Proof. Let $H = H_L^n$ be the subgroup of $G = (\mathbb{Z}/n\mathbb{Z})^\times$ corresponding to the subextension $L/\mathbb{Q}$ of $\mathbb{Q}(\zeta_n)/\mathbb{Q}$. Then $G/H \simeq \mathrm{Gal}(L/\mathbb{Q})$, so G/H has exponent m. Therefore, if $\overline{p}$ is an mth power in G, then $\overline{p} \in H$, so p splits completely by Theorem 5.

For the last assertion, just note that in any group G, if $x \in G$ has order t coprime to some natural number m, then writing $1 = am + bt$, we have $x = x^{am+bt} = (x^a)^m$, so x is an mth power in G. □

The following lemma is useful for Proposition 13.

Lemma 12. *Let G be a finite abelian group and H a subgroup of prime index ℓ. If J is a cyclic subgroup of G of order divisible by ℓ, then H contains the index-ℓ subgroup of J. Further, H contains every subgroup of G of order coprime to ℓ.*

Proof. If g generates J, then because $|G : H| = \ell$, we have $(gH)^\ell = H$, i.e., $g^\ell \in H$. But g^ℓ generates the unique index-ℓ subgroup of J.

The second statement is also clear: If g has order coprime to ℓ in G, then the order of gH in G/H is coprime to ℓ but also divides ℓ, so $g \in H$. □

If n is a positive integer, then we will denote by Z_n the cyclic group of order n.

Proposition 13. *Let ℓ be a prime and $L/\mathbb{Q}$ a Z_ℓ-extension. Then the conductor of $L/\mathbb{Q}$ is equal to $\ell^c r$ for some squarefree integer $r \geq 1$ divisible only by primes congruent to 1 mod ℓ, where $c \in \{0, 2, 3\}$ if $\ell = 2$ and $c \in \{0, 2\}$ otherwise.*

Proof. Choose n such that $L \subseteq \mathbb{Q}(\zeta_n)$, and write

$$n = \ell^s \left(\prod_{i=1}^{k} p_i^{a_i} \right) \left(\prod_{j=1}^{m} q_j^{b_j} \right),$$

where $p_i \equiv 1 \bmod \ell$, $q_j \not\equiv 1 \bmod \ell$, and $a_i, b_j \geq 1$. Let $G = \mathrm{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{Q})$, and let $H = \mathrm{Gal}(\mathbb{Q}(\zeta_n)/L)$, which has index ℓ in G.

First take $p = p_i$ and $a = a_i$ for some i, and let $J = \mathrm{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{Q}(\zeta_{n'}))$, where $n' = n/p^a$. Then $J \simeq \mathrm{Gal}(\mathbb{Q}(\zeta_{p^a})/\mathbb{Q})$ and is therefore cyclic of order $(p-1)p^{a-1}$. Further, by assumption, $\ell \,|\, p-1$ so ℓ divides $|J|$. Hence, by Lemma 12, H contains the subgroup of J of index ℓ. But then H also contains the subgroup of J of index $p-1$, which is $\mathrm{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{Q}(\zeta_{n'p}))$ because $[\mathbb{Q}(\zeta_{n'p}) : \mathbb{Q}(\zeta_{n'})] = [\mathbb{Q}(\zeta_p) : \mathbb{Q}] = p - 1$. Thus, $L \subseteq \mathbb{Q}(\zeta_{n'p})$.

Next, if $q = q_j$, $b = b_j$, and $n' = n/q_j^{b_j}$, then $\mathrm{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{Q}(\zeta_{n'})) \simeq \mathrm{Gal}(\mathbb{Q}(\zeta_{q^b})/\mathbb{Q})$, which has order coprime to ℓ, so H contains $\mathrm{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{Q}(\zeta_{n'}))$ by Lemma 12 again, i.e., $L \subseteq \mathbb{Q}(\zeta_{n'})$.

We now turn to the subgroup $J = \mathrm{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{Q}(\zeta_{n'}))$ where $n' = n/\ell^s$. First assume that $\ell \neq 2$. If $s \leq 1$, then J has order coprime to ℓ (specifically, order 1 or $\ell - 1$), so H contains J, i.e., $L \subseteq \mathbb{Q}(\zeta_{n'})$. Assume now that $s \geq 2$. Then $J \simeq \mathrm{Gal}(\mathbb{Q}(\zeta_{\ell^s})/\mathbb{Q})$, which is cyclic of order $(\ell-1)\ell^{s-1}$ because $\ell \neq 2$. By Lemma 12, H contains the subgroup of J of index ℓ. Therefore, H also contains the subgroup of J of index $(\ell-1)\ell$, which is $\mathrm{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{Q}(\zeta_{n'\ell^2}))$ because $[\mathbb{Q}(\zeta_{n'\ell^2}) : \mathbb{Q}(\zeta_{n'})] = [\mathbb{Q}(\zeta_{\ell^2}) : \mathbb{Q}] = (\ell-1)\ell$. Thus, $L \subseteq \mathbb{Q}(\zeta_{n'\ell^2})$.

To deal with the case $\ell = 2$, we make some observations on the structure of groups of the form $X = \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2^d\mathbb{Z}$ with $d \geq 1$. Such a group has more than one subgroup of index 4 (if $d \geq 2$), but there is a unique one X' that is contained in three subgroups of index 2. Equivalently, by the third and fourth isomorphism theorems, X' is the unique subgroup of X such that $X/X' \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$.

Importantly, X' is also characterized by the fact that it is generated by $2g$ (writing X additively) where g is any element of X of order 2^d.

Let $J = \mathrm{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{Q}(\zeta_{n'}))$ where $n' = n/2^s$. Everything in the case $\ell = 2$ is the same as in the general case except when $s \geq 3$. We therefore assume $s \geq 3$. Note that $J \simeq \mathrm{Gal}(\mathbb{Q}(\zeta_{2^s})/\mathbb{Q})$, which takes the form of the group X in the previous paragraph. Choose $g \in J$ of order 2^{s-2}. Because H has index 2 in G, it follows that $(gH)^2 = H$ in G/H, so H contains the element g^2 and therefore contains the subgroup $\langle g^2 \rangle$ of J. By the general remarks we have just made, $\langle g^2 \rangle$ is the unique subgroup J' of J such that $J/J' \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$. But $J/\mathrm{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{Q}(\zeta_{8n'})) \simeq \mathrm{Gal}(\mathbb{Q}(\zeta_{8n'})/\mathbb{Q}(\zeta_{n'})) \simeq \mathrm{Gal}(\mathbb{Q}(\zeta_8)/\mathbb{Q}) \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$, so $\langle g^2 \rangle = \mathrm{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{Q}(\zeta_{8n'}))$. Thus, because H contains $\langle g^2 \rangle$, we see that $L \subseteq \mathbb{Q}(\zeta_{8n'})$.

Putting all of the above together, and using the fact that the conductor divides all N such that $L \subseteq \mathbb{Q}(\zeta_N)$, we are done. □

Proposition 14. *Assume that $f(x) = x^3 + a_2x^2 + a_1x + a_0 \in \mathbb{Z}[x]$ is irreducible and has square discriminant. If a prime p satisfies $p \mid a_0, a_1, a_2$ and $p^3 \nmid a_0$, then p ramifies in the extension generated by a root of $f(x)$.*

Proof. Let the roots of $f(x)$ be α, β, γ, and let L be the extension generated by any one of these. In fact, $L/\mathbb{Q}$ is an A_3-extension because $f(x)$ has square discriminant, so L contains all the roots of $f(x)$.

Assume that p is unramified in $L/\mathbb{Q}$. If $\mathfrak{p}$ is a prime of L above p, and v is the $\mathfrak{p}$-adic valuation of L, then $v(p) = 1$ by assumption. Therefore, $1 \leq v(a_0) \leq 2$, which is to say

$$1 \leq v(\alpha) + v(\beta) + v(\gamma) \leq 2.$$

Hence, at least one of α, β, γ is a $\mathfrak{p}$-adic unit, γ say, and at least one is not, α say.

Next,

$$1 \leq v(a_1) = v(\alpha\beta + \beta\gamma + \gamma\alpha) = v(\beta\gamma + \alpha(\beta + \gamma)).$$

From here, we deduce that $v(\beta) \geq 1$, for if not, we would have $v(\beta\gamma + \alpha(\beta + \gamma)) = 0$ because $v(\alpha) \geq 1$.

Since we now have $v(\alpha), v(\beta) \geq 1$ and $v(\gamma) = 0$, it follows that $v(\alpha + \beta + \gamma) = 0$. But this contradicts that $v(a_2) \geq 1$. Thus, p ramifies in $L/\mathbb{Q}$. □

5 Splitting of $P_G(x)$ over $\mathbb{Z}_p$

In Section 3, we related the existence of certain p-adic roots of $P_G(x)$ to the divisibility by p of the numbers $c_{G,k}$ associated to G.

Of especial interest is the situation where $P_G(x)$ has as many roots in $\mathbb{Z}_p$ as possible for a polynomial of its degree, i.e., the situation where $P_G(x)$ splits completely over $\mathbb{Z}_p$. This is the situation we now turn to, considering conditions under which this complete splitting occurs.

Definition 15. *Let G be a graph.*

(i) *We denote by L_G the splitting field of $P_G(x)$, i.e., the field generated by the roots of $P_G(x)$ in $\mathbb{C}$.*

(ii) *We will say that a graph H is chromatically contained in G if $L_H \subseteq L_G$.*

There is nothing special about the choice of field $\mathbb{C}$ in this definition. We could replace it by any algebraically closed field Ω containing $\mathbb{Q}$, so long as Ω remains fixed throughout the whole discussion.

The significance of the notion of chromatic containment for the p-adic roots of a chromatic polynomial will become clear throughout the remainder of the paper.

The new results, where we analyze a certain infinite family of graphs introduced by Morgan [10], will be presented in Section 5.2. But first, in Section 5.1, we provide some generalities that are reformulations, into the language of graphs, of some of the class-field-theoretic results above. Although it is interesting to see what these results say for graphs, and although we are not aware of them having been considered in this graph-theoretic context elsewhere, we take no credit for the statements in Section 5.1, as they are, at their core, long-standing number-theoretic results.

5.1 Generalities

Proposition 16. *If G and H are graphs, then the following are equivalent:*

(i) *H is chromatically contained in G.*

(ii) *For every prime p such that $P_G(x)$ splits completely over $\mathbb{Z}_p$, $P_H(x)$ also splits completely over $\mathbb{Z}_p$.*

Proof. This is Theorem 8 together with Proposition 10. □

The following result is a restatement in graph-theoretic language of the Kronecker–Weber Theorem, i.e., that every finite abelian extension of $\mathbb{Q}$ is contained in a cyclotomic field.

Proposition 17. *If G is a graph for which $L_G/\mathbb{Q}$ is an abelian extension, then G is chromatically contained in a cycle graph.*

The graph-theoretic input in the proof of this is the well-known fact that L_{C_n} is the cyclotomic field $\mathbb{Q}(\zeta_{n-1})$ generated by a root of unity ζ_{n-1} of order $n-1$. The rest is the Kronecker–Weber Theorem.

When $L_G/\mathbb{Q}$ is abelian, the question of precisely which cycle graphs chromatically contain G is related to the p-adic roots of $P_G(x)$ via the following fact.

Proposition 18. *If $L_G/\mathbb{Q}$ is an abelian extension and $n \geq 4$ is an integer, then the following are equivalent:*

(i) *G is chromatically contained in the cycle graph C_n.*

(ii) $P_G(x)$ splits completely over $\mathbb{Z}_p$ for every prime $p \equiv 1 \bmod n-1$.

Proof. Use Proposition 16 together with Proposition 6 and the fact that $L_{C_n} = \mathbb{Q}(\zeta_{n-1})$. □

5.2 Results on Morgan's Z_n-families of graphs

We now turn to some new results concerning an infinite family of graphs $G_{3,q,r+q}$ studied by Morgan [10], where $q \geq 0$ and $r = d^2 + d + 8$ for an integer d. Equivalently, $r = \frac{1}{4}(s^2 + 27) + 1$ for some odd integer s. This description of r will be more convenient for our calculations later. The graph $G_{3,q,r+q}$ is defined as follows: Take a copy of the complete graph K_{r+q-1}, and add three new vertices v_1, v_2, v_3, joining each v_i to each of the $r+q-1$ vertices in K_{r+q-1}. Then add a final vertex w and join it to v_1, v_2, v_3, as well as to q of the vertices in K_{r+q-1}. The family of such graphs $G_{3,q,r+q}$ (with r of the form d^2+d+8) will be called *Morgan's Z_3-family*, because the Galois group of each chromatic polynomial is the cyclic group Z_3 of order 3; see [10, Theorem 4].

The key results in this section are Theorem 19 and its cousin, Proposition 24.

Theorem 19. *Let $G_{3,q,r+q}$ be one of the graphs in Morgan's Z_3-family. Then $G_{3,q,r+q}$ is chromatically contained in the cycle graph C_r.*

We begin our proof by reminding the reader that, because $L_{C_r} = \mathbb{Q}(\zeta_{r-1})$, the aim is to show that $L_G \subseteq \mathbb{Q}(\zeta_{r-1})$ where $G = G_{3,q,r+q}$. The numbers $r = d^2 + d + 8$ that appear in Morgan's Z_3-family are exactly those of the form $t+1$, where $t = \frac{1}{4}(s^2 + 27)$ with s an odd integer. We will find the numbers s and t easier to work with than r and d, so we will shift to this notation for the rest of the proof. Also, for any $q \geq 0$, $G_{3,q,r+q}$ is the join of $G_{3,0,r}$ and K_q, so $P_{G_{3,q,r+q}}(x) = (x)_q P_{G_{3,0,r}}(x-q)$. As a result, $L_{G_{3,q,r+q}} = L_{G_{3,0,r}}$, so we may assume that $q = 0$.

By [10, Theorem 1],

$$P_{G_{3,0,t+1}}(x) = (x)_{t+1}((x-t-1)^3 + t(x-t)^2),$$

so $L_{G_{3,0,t+1}}$ is the field generated by the roots of the cubic polynomial

$$f_t(x) = (x-t-1)^3 + t(x-t)^2.$$

Consider the following changes of variable:

$$\begin{aligned} g_t(x) &= f_t(x+t) = (x-1)^3 + tx^2, \\ h_t(x) &= -x^3 g_t(1/x) = (x-1)^3 - tx, \\ j_t(x) &= h_t(x+1) = x^3 - tx - t. \end{aligned} \tag{3}$$

Each change of variable produces a polynomial with the same splitting field as the previous one, so $L_{G_{3,0,r}} = L_t$, the splitting field of $j_t(x)$. Now, we see from the equality $t = \frac{1}{4}(s^2 + 27)$ in terms of the odd number s that t also is odd. Therefore, the polynomial $x^3 - tx - t$ is irreducible over $\mathbb{Q}$, because its reduction

mod 2 is the irreducible cubic $x^3 + x + 1$. Further, the discriminant of $j_t(x)$ is $t^2(4t - 27) = t^2 s^2$, which is square, so $L_t/\mathbb{Q}$ is cyclic of degree 3. (Morgan uses the same argument on $f_t(x)$ itself, but we feel $j_t(x)$ is easier to work with than $f_t(x)$.)

Our goal is to show that the conductor of $L_t/\mathbb{Q}$ divides $t = r-1$. Equivalently, we need to show that the discriminant Δ_t of L_t divides t^2, since the discriminant of a cubic abelian extension of $\mathbb{Q}$ is the square of its conductor.

However, the foregoing calculations only give us $\Delta_t \mid t^2 s^2$. The key difficulty is obtaining $\Delta_t \mid t^2$, for which we have to work a bit harder.

Proposition 20. *If $t = \frac{1}{4}(s^2+27)$, where s is an odd integer, then the discriminant of the splitting field L_t of $j_t(x) = x^3 - tx - t$ divides t^2. Equivalently, the conductor of the abelian extension $L_t/\mathbb{Q}$ divides t.*

Proof. Let α be a root of $x^3 - tx - t$, and let

$$\beta = \frac{1}{s}\left(\alpha^2 + \frac{1}{2}(s-3)\alpha + \frac{1}{2}(s-9)\right).$$

Explicit computation shows that β is a root of the polynomial

$$\hat{\jmath}_s(x) = x^3 - \frac{1}{2}(3+s)x^2 - \frac{1}{2}(3-s)x + 1, \tag{4}$$

which has integral coefficients because s is odd. The polynomial $\hat{\jmath}_s(x)$ must in fact be the minimal polynomial of β over $\mathbb{Q}$, because $\beta \notin \mathbb{Q}$. Alternatively, it is irreducible because its reduction mod 2 is either $x^3 + x + 1$ or $x^3 + x^2 + 1$, depending on the residue class of s mod 4, and both these polynomials are irreducible over $\mathbb{F}_2$. Hence, β is an algebraic integer in L_t such that the powers $1, \beta, \beta^2$ are linearly independent. Therefore, the discriminant of L_t divides the discriminant of the order $\mathbb{Z}[\beta]$, which is the discriminant of the polynomial $\hat{\jmath}_s(x)$, which is easily computed to be t^2. □

The proof of Theorem 19 is now complete, because L_t has conductor dividing t by Proposition 20 and is therefore contained in $\mathbb{Q}(\zeta_t)$, i.e., $L_G \subseteq \mathbb{Q}(\zeta_{r-1})$.

Corollary 21. *Let $G = G_{3,q,r+q}$ be one of the graphs in Morgan's Z_3-family. If $p \nmid r-1$ is a cube mod $r-1$, then $P_G(x)$ splits completely over $\mathbb{Z}_p$.*

Proof. By Corollary 9, $P_{G_{3,q,r+q}}(x)$ splits completely over $\mathbb{Z}_p$ if and only if p splits completely in $L_{G_{3,q,r+q}} = L_{G_{3,0,r}} = L_t$, where $t = r-1$ and L_t is the splitting field of $x^3 - tx - t$. The conductor of $L_t/\mathbb{Q}$ divides t by Proposition 20, so we may apply Lemma 11 with $m = 3$ to get the result. □

Example. Consider the graph $G_{3,0,20}$ (here, $r = d^2 + d + 8$ with $d = 3$). According to the corollary, the chromatic polynomial $P_{G_{3,0,20}}(x)$ splits completely over $\mathbb{Z}_p$ for any prime congruent mod 19 to

$$1, \quad 7, \quad 8, \quad 11, \quad 12, \quad 18,$$

because these are the cubes mod 19. In fact, this list is complete: If p is a prime such that $P_{G_{3,0,20}}(x)$ splits completely over $\mathbb{Z}_p$, then p is congruent mod 19 to one of the numbers in this list.

The list that Corollary 21 generates may not always be complete for other graphs $G_{3,q,r+q}$. For example, the list of residue classes mod 63 arising from the corollary in the case of the graph $G_{3,0,64}$ is

$$1, \quad 8, \quad 55, \quad 62,$$

telling us that $P_{G_{3,0,64}}(x)$ splits completely over $\mathbb{Z}_p$ for any prime congruent to one of these four numbers mod 63. But the full list of residue classes of the primes p such that $P_{G_{3,0,64}}(x)$ splits completely over $\mathbb{Z}_p$ is

$$1, \quad 5, \quad 8, \quad 11, \quad 23, \quad 25, \quad 38, \quad 40, \quad 52, \quad 55, \quad 58, \quad 62.$$

We now provide a result that tells us under what circumstances Corollary 21 gives us the full set of primes p such that $P_{G_{3,q,r+q}}(x)$ splits completely over $\mathbb{Z}_p$.

Proposition 22. *Let $G = G_{3,q,r+q}$ be one of the graphs in Morgan's Z_3-family. If $r-1$ is a power of a prime, then the primes p appearing in Corollary 21 are all of the primes such that $P_G(x)$ splits completely over $\mathbb{Z}_p$. Otherwise, there are infinitely many more primes for which this happens.*

Proof. Let $t = r-1$ again, and suppose $t = \ell^k$ is a prime power. Then the 3-rank of $(\mathbb{Z}/t\mathbb{Z})^\times$ is at most one, but in fact it has to be exactly one because $(\mathbb{Z}/t\mathbb{Z})^\times$ contains the subgroup H of index 3 corresponding to the cubic extension L_t, the field generated by a root of $x^3 - tx - t$. Hence, the subgroup J of $(\mathbb{Z}/t\mathbb{Z})^\times$ consisting of the cubes has index 3 and is therefore equal to H.

Now, Proposition 20 tells us that the conductor f of the extension $L_t/\mathbb{Q}$ divides $t = \ell^k$, so f and t have the same support $\{\ell\}$. Therefore, any prime p that splits completely in L_t is necessarily coprime to t, and then by Theorem 5 its class in $(\mathbb{Z}/t\mathbb{Z})^\times$ lies in H. But as we said above, $H = J$, the subgroup of cubes.

Conversely, suppose t is not a power of a prime, so that t has at least two distinct prime divisors. By Lemma 23 below, the prime divisors of t are congruent to 0 or 1 mod 3. If two of them, ℓ_1 and ℓ_2 say, are congruent to 1 mod 3, then $(\mathbb{Z}/t\mathbb{Z})^\times$ contains a subgroup isomorphic to $\mathbb{Z}/(\ell_1 - 1)\mathbb{Z} \times \mathbb{Z}/(\ell_2 - 1)\mathbb{Z}$ and therefore has 3-rank at least two. Otherwise, t is divisible by 3 and at least one prime $\ell \equiv 1 \bmod 3$. But then $3 \,|\, s$, where s and t are related as above by the equation $s^2 = 4t - 27$, so in fact $9 \,|\, t$. Therefore, $(\mathbb{Z}/t\mathbb{Z})^\times$ contains a subgroup isomorphic to $\mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/(\ell - 1)\mathbb{Z}$ so again has 3-rank at least two. Thus, in the case where t is not a prime power, the subgroup J of cubes in $(\mathbb{Z}/t\mathbb{Z})^\times$ has index divisible by 9 and therefore is a proper subgroup of H. □

Lemma 23. *Suppose $t = \frac{1}{4}(s^2 + 27)$, where s is an odd integer. Then every prime divisor of t is congruent to 0 or 1 mod 3.*

Proof. Let $p \neq 3$ be a prime divisor of t. Then $p \nmid s$, so letting $\left(\frac{\cdot}{p}\right)$ denote the Legendre symbol, we have

$$\begin{aligned} 1 &= \left(\frac{s^2}{p}\right) \\ &= \left(\frac{4t-27}{p}\right) \\ &= \left(\frac{-27}{p}\right) \\ &= \left(\frac{-3}{p}\right) \\ &= \left(\frac{p}{3}\right), \end{aligned}$$

the last equality by quadratic reciprocity. Thus, $p \equiv 1 \bmod 3$. □

Before stating the next proposition, we remind the reader that if $P_G(x)$ has abelian Galois group, then the conductor f of the abelian extension $L_G/\mathbb{Q}$ tells us the smallest cycle graph in which G is chromatically contained: G is chromatically contained in C_{f+1} but no smaller cycle graph.

Proposition 24. *Let $G = G_{3,q,r+q}$ be one of the graphs in Morgan's Z_3-family, so that $r - 1 = \frac{1}{4}(s^2 + 27)$ for some odd integer s. Then the conductor of the extension $L_G/\mathbb{Q}$ is equal to km, where m is the product of the primes $p \neq 3$ such that $3 \nmid v_p(r-1)$, and*

$$k = \begin{cases} 9 & \text{if } v_3(s) \in \{1, 2\} \\ 1 & \text{otherwise.} \end{cases}$$

Before proving Proposition 24, let us consider how one may use it.

Example. If $G = G_{3,0,64}$, then from the factorizations $r - 1 = 63 = 3^2 \cdot 7$ and $s = 15 = 3 \cdot 5$, we see that the conductor of $L_G/\mathbb{Q}$ is $9 \cdot 7 = 63$. Thus, G is chromatically contained in C_{64} but no smaller cycle graph.

Example. We contrast the previous example with the following, in which $G = G_{3,0,4564}$. Here, we have the factorizations $r - 1 = 4563 = 3^3 \cdot 13^2$ and $s = 135 = 3^3 \cdot 5$, showing that the conductor is 13. Therefore, G is chromatically contained in C_{14} but no smaller cycle graph.

Proof. (Proposition 24) Let $t = r - 1 = \frac{1}{4}(s^2 + 27)$. We remind the reader of the polynomials $j_t(x)$ and $\hat{j}_s(x)$, defined in (3) and (4) respectively, as both reappear in this proof. As in the proof of Theorem 19, the field L_G is equal to L_t, the splitting field of $j_t(x)$. By Proposition 13, the conductor of $L_t/\mathbb{Q}$ takes the form km, where $k \in \{1, 9\}$ and m is a squarefree natural number not divisible by 3. It therefore remains to determine which primes ramify in $L_t/\mathbb{Q}$.

We first consider primes $p \neq 3$. Our claim is that p ramifies in $L_t/\mathbb{Q}$ if and only if $3 \nmid v_p(t)$. Write $t = p^{3k+l}a$, where a, k, and l are non-negative integers with p not dividing a and with $l \in \{0, 1, 2\}$. We then consider the polynomial

$$\frac{1}{p^{3k}} j_t(p^k x) = x^3 - p^{k+l}ax - p^l a. \tag{5}$$

If $3 \nmid v_p(t)$, so that $l \in \{1, 2\}$, then p ramifies by Proposition 14 applied to this polynomial. Suppose instead that $3 \mid v_p(t)$. In this case, $l = 0$ and the polynomial in (5) is $x^3 - p^k ax - a$, which has discriminant $a^2(4p^{3k}a - 27)$. If $k = 0$, then $p \nmid t$ so p is unramified by Proposition 20, and if $k > 0$, then p does not divide the discriminant $a^2(4p^{3k}a - 27)$, so again p is unramified.

Now we consider the prime 3. We transition between t and s via the equality $t = \frac{1}{4}(s^2 + 27)$. If $v_3(s) = 0$, then $v_3(t) = 0$ also, so 3 is unramified by Proposition 20. Next, if $v_3(s) = 1$, then $v_3(t) = 2$, so 3 ramifies by Proposition 14 applied to $j_t(x)$.

For the remaining cases, where $v_3(s) \geq 2$, observe that $v_3(t) = 3$, so $t = 27c$ for some integer c not divisible by 3. Consider the polynomial

$$\hat{j}_s(x) = j_s(x + \tfrac{1}{6}(3 + s)) = x^3 - \frac{t}{3}x - \frac{st}{27} = x^3 - 9cx - sc.$$

If $v_3(s) = 2$, then Proposition 14 shows that 3 ramifies. If instead $v_3(s) \geq 3$, so that $s = 27d$ for some integer d, then we pass finally to the polynomial

$$\frac{1}{27}\hat{j}_s(3x) = x^3 - cx - cd.$$

Its discriminant is $c^2(4c - 27d^2)$, not divisible by 3, so 3 is unramified. □

Remark. *The fields $L_{G_{3,0,r}}$ arising from Morgan's Z_3-family may occasionally share a conductor. However, we point out that, for a given f, there can be at most finitely many graphs of the form $G_{3,0,r}$ in Morgan's family such that the conductor of $L_{G_{3,0,r}}$ is equal to f. This is essentially because of the fact that, for each $a \in \mathbb{N}$, the equation $y^2 = 4ax^3 - 27$ has at most finitely many integral solutions (x, y). See [13, Chap. IX, Theorem 4.3], for example.*

It seems especially rare for two of the fields $L_{G_{3,0,r}}$ to be the same. Some of the fields agree for very small r, and after that there is a notable exception in the pair of graphs $G_{3,0,14}$ and $G_{3,0,4564}$, whose chromatic polynomials both have the same splitting field, namely, the unique cubic subfield of $\mathbb{Q}(\zeta_{13})$. Such examples are very likely the result of pure coincidence.

Morgan also found, in the same article [10], a second infinite family of graphs in which each chromatic polynomial has cyclic splitting field, this time cyclic of degree 4. The graphs are denoted $G_{4,q,6+q}$, the definition being the same as that for $G_{3,q,r+q}$ above except that now the three vertices denoted v_1, v_2, v_3 become v_1, v_2, v_3, v_4.

Proposition 25. *For all $q \geq 0$, $G_{4,q,6+q}$ is chromatically contained in C_6. In fact, $L_{G_{4,q,6+q}} = L_{C_6}$.*

Proof. As in the case of the Z_3-family, we have $L_{G_{4,q,6+q}} = L_{G_{4,0,6}}$ for all $q \geq 0$, because $G_{4,q,6+q}$ is the join of $G_{4,0,6}$ and K_q. Now, as Morgan shows, the splitting field L is cyclic of degree 4 over $\mathbb{Q}$ and generated by a root of the irreducible quartic

$$g(x) = x^4 - 19x^3 + 141x^2 - 489x + 671,$$

which has discriminant $5^3 \cdot 11^2$. There are only two Z_4-extensions of $\mathbb{Q}$ of discriminant dividing $5^3 \cdot 11^2$, and they can be distinguished by the splitting of the prime 19. Indeed, in one of the fields, 19 splits completely, while in the other, $\mathbb{Q}(\zeta_5)$, it does not. Since $g(x)$ has no roots mod 19, we see that the former does not occur, so $L = \mathbb{Q}(\zeta_5) = L_{C_6}$. □

6 Concluding remarks

While the study of p-adic roots of chromatic polynomials should by no means be limited to the case of abelian extensions of $\mathbb{Q}$, this case is nonetheless a good starting point because of the simple way in which primes split under the abelian assumption.

That said, graphs whose chromatic roots generate abelian extensions of $\mathbb{Q}$ appear to be rare, and a challenge in this direction is to find new families of such graphs. The algorithm of Delbourgo and Morgan [5] mentioned earlier may lead to new families yielding quartic abelian extensions, since any quartic polynomial may be taken as input to the algorithm. One might hope that, if the algorithm is given a natural family of polynomials with quartic splitting fields, the graphs it outputs would also form some natural family, although there is no guarantee of this.

Approaching the problem from the opposite direction, one could instead consider families of graphs defined in terms of parameters, compute the chromatic polynomials, and see how to choose the parameters such that the extensions generated are all abelian over $\mathbb{Q}$. For example, among all the graphs $G_{3,q,r+q}$ discussed in Section 5.2, the ones where $r = d^2 + d + 8$ with $d \in \mathbb{Z}$ have abelian splitting fields—this is Morgan's family.

We make a final comment, concerning why it might be appropriate to view chromatic polynomials in a p-adic context, and therefore why it might seem reasonable to pursue the connection further. The natural numbers, being those numbers that we use to count, are central to graph theory (and to combinatorics more generally). The chromatic polynomial is defined purely in terms of counting, namely, the counting of proper colourings by a given number of colours. It is perhaps significant, then, that $\mathbb{Z}_p$ stands in special relationship to the set $\mathbb{N}$ of natural numbers: $\mathbb{Z}_p$ is a compact ring in which $\mathbb{N}$ is dense. By contrast, $\mathbb{C}$, where chromatic roots have historically been considered, has no such relationship with $\mathbb{N}$.

We hope that the relevance of p-adic roots of chromatic polynomials will become better understood in the future.

Acknowledgements

The author would like to thank the referee for having made suggestions for improvement.

References

[1] Adam Bohn. Chromatic polynomials of complements of bipartite graphs. *Graphs Combin.*, 30(2):287–301, 2014.

[2] Jason I. Brown, Carl Hickman, Alan D. Sokal, and David G. Wagner. On the chromatic roots of generalized theta graphs. *J. Combin. Theory Ser. B*, 83(2):272–297, 2001.

[3] Peter J. Cameron and Kerri Morgan. Algebraic properties of chromatic roots. *Electron. J. Combin.*, 24(1):Paper 1.21, 14, 2017.

[4] Daniel Delbourgo and Kerri Morgan. Algebraic invariants arising from the chromatic polynomials of theta graphs. *Australas. J. Combin.*, 59:293–310, 2014.

[5] Daniel Delbourgo and Kerri Morgan. An algorithm which outputs a graph with a specified chromatic factor. *Discrete Appl. Math.*, 257:128–150, 2019.

[6] Phil Hanlon. A Hodge decomposition interpretation for the coefficients of the chromatic polynomial. *Proc. Amer. Math. Soc.*, 136(11):3741–3749, 2008.

[7] Laure Helme-Guizon and Yongwu Rong. A categorification for the chromatic polynomial. *Algebr. Geom. Topol.*, 5:1365–1388, 2005.

[8] Neal Koblitz. *p-adic numbers, p-adic analysis, and zeta-functions*, volume 58 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, second edition, 1984.

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

[10] Kerri Morgan. Galois groups of chromatic polynomials. *LMS J. Comput. Math.*, 15:281–307, 2012.

[11] Jürgen Neukirch. *Algebraic number theory*, volume 322 of *Grundlehren der Mathematischen Wissenschaften [Fundamental Principles of Mathematical Sciences]*. Springer-Verlag, Berlin, 1999. Translated from the 1992 German original and with a note by Norbert Schappacher, With a foreword by G. Harder.

[12] Ronald C. Read. An introduction to chromatic polynomials. *J. Combinatorial Theory*, 4:52–71, 1968.

[13] Joseph H. Silverman. *The arithmetic of elliptic curves*, volume 106 of *Graduate Texts in Mathematics*. Springer, Dordrecht, second edition, 2009.

[14] Alan D. Sokal. Chromatic roots are dense in the whole complex plane. *Combin. Probab. Comput.*, 13(2):221–261, 2004.