3-2011

Nonsolvable Polynomials with Field Discriminant 5^a

David P. Roberts
University of Minnesota - Morris, roberts@morris.umn.edu

Recommended Citation
David P. Roberts. Nonsolvable polynomials with field discriminant 5^a. *International Journal of Number Theory* 7 (2011), no. 2, 289-322.

NONSOLVABLE POLYNOMIALS WITH FIELD DISCRIMINANT 5^A

DAVID P. ROBERTS

Abstract. We present the first explicitly known polynomials in $\mathbf{Z}[x]$ with nonsolvable Galois group and field discriminant of the form $\pm p^A$ for $p \leq 7$ a prime. Our main polynomial has degree 25, Galois group of the form $PSL_2(5)^5.10$, and field discriminant 5^{69}. A closely related polynomial has degree 120, Galois group of the form $SL_2(5)^5.20$, and field discriminant 5^{311}. We completely describe 5-adic behavior, finding in particular that the root discriminant of both splitting fields is $125 \cdot 5^{-1/12500} \approx 124.984$ and the class number of the latter field is divisible by 5^4.

1. Introduction

1.1. **Background.** Two of the most important invariants of a Galois number field $L \subset \mathbf{C}$ are its Galois group $G = \mathrm{Gal}(L/\mathbf{Q})$ and the set S of primes dividing its field discriminant $\mathrm{disc}(L/\mathbf{Q})$. In the mid-1990s, Gross circulated the observation that no Galois number fields were known with G nonsolvable and S consisting of a single prime ≤ 7. In this connection, Gross [11] developed a remarkable conjectural theory of algebraic modular forms which predicts with great specificity that indeed such fields exist. An example pursued by Lansky and Pollack [17] is that there should exist a field with $(G, S) = (G_2(5), \{5\})$.

In 2008, Dembélé [6] proved the existence of the first field meeting Gross's specifications by means of computations with Hilbert modular forms. Dembélé's field has $G = SL_2(2^8)^2.8$ and $S = \{2\}$. In 2009, Dembélé, Greenberg, and Voight [7] similarly proved the existence of fields for $(G, S) = (PGL_2(3^k).9, \{3\})$ for $k = 18$, 27, and 36. They also proved the existence of fields for $(G, \{5\})$ with G involving one or more copies of the simple group $PSL_2(5^k)$ for $k = 1$, 2, 5, 10, 15, 25, 40.

Whenever one knows abstractly of the existence of an interesting Galois number field L, a natural problem is to produce a polynomial $g(x) \in \mathbf{Z}[x]$ with splitting field L. For all of the above cases but the pair $(PSL_2(5)^5.10, \{5\})$, the minimal degree of such a $g(x)$ is very large. Finding a defining polynomial in these cases seems well beyond current techniques. On the other hand, for the group $PSL_2(5)^5.10$ the minimal degree is twenty-five. In their 2009 preprint [7], Dembélé, Greenberg, and Voight specifically raised the problem of finding a defining polynomial for L in this relatively modest case. The field L embeds in a field $\tilde{L}$ with Galois group $SL_2(5)^5.20$, also ramifying at five only. One could also ask for a defining polynomial at this level, where the minimal degree is 120.

1.2. **The main results.** The first main result of this paper consists of explicit polynomials defining nonsolvable fields ramified at 5 only:

Theorem 1.1. A. *Let*

$$\begin{aligned} g_{25}(x) = \\ & x^{25} - 25x^{22} + 25x^{21} + 110x^{20} - 625x^{19} + 1250x^{18} - 3625x^{17} + 21750x^{16} \\ & -57200x^{15} + 112500x^{14} - 240625x^{13} + 448125x^{12} - 1126250x^{11} + 1744825x^{10} \\ & -1006875x^9 - 705000x^8 + 4269125x^7 - 3551000x^6 + 949625x^5 - 792500x^4 \\ & +1303750x^3 - 899750x^2 + 291625x - 36535. \end{aligned}$$

Then its splitting field $L \subset \mathbf{C}$ *has Galois group* $\mathrm{Gal}(L/\mathbf{Q}) = PSL_2(5)^5.10$ *and its root field* $K = \mathbf{Q}[x]/g_{25}(x)$ *has discriminant* $\mathrm{disc}(K/\mathbf{Q}) = 5^{69}$.

B. *Let* $g_{120}(x)$ *be the degree* 120 *polynomial given in Table 5. Then its splitting field* $\tilde{L} \subset \mathbf{C}$ *is an unramified extension of* L *of relative degree* $[\tilde{L} : L] = 2^6$ *and Galois group* $\mathrm{Gal}(\tilde{L}/\mathbf{Q}) = SL_2(5)^5.20$. *The root field* $\tilde{K} = \mathbf{Q}[x]/g_{120}(x)$ *has discriminant* $\mathrm{disc}(\tilde{K}/\mathbf{Q}) = 5^{311}$.

The polynomials $g_{25}(x)$ and $g_{120}(x)$ as well as some related polynomials are available in a form suitable for computer algebra systems on the author's homepage.

One would certainly expect from matching invariants, including Frobenius invariants as discussed below, that our fields L and $\tilde{L}$ coincide with the fields with the same Galois group proved to exist in 2009 in [7]. In the final 2010 version of [7], Dembélé, Greenberg, and Voight prove that this agreement does indeed hold, by applying results of Skinner and Wiles [29] and Jarvis [12].

An immediate consequence of Theorem 1.1 is that the degree $N = 7,776,000,000$ field L and the degree $\tilde{N} = 497,664,000,000$ field $\tilde{L}$ have discriminants $5^{\alpha N}$ and $5^{\alpha \tilde{N}}$ respectively, for some common rational number α. Our second main result, Theorem 8.1, is a general statement about a class of p-adic fields including the 5-adic completion of K. As a consequence, one finds that $\alpha = 3 - 1/12500$. The common root discriminant of L, $\tilde{L}$, and a similarly behaved solvable field L^s is then $5^\alpha \approx 124.984$. Furthermore, the compositum $\tilde{L}L^s$ is a very slightly ramified elementary abelian extension of $\tilde{L}$ of degree 5^5. It contains an unramified subextension of degree 5^4, proving that the class number of $\tilde{L}$ is divisible by 5^4.

1.3. **Organization of this paper.** Section 2 provides some optional context. An obvious principle is that while nonsolvable fields ramified at two small primes only may be hard to find, fields ramified at just one small prime are much harder to find. We present a quantitative version of this principle in our setting of relative quintics. Section 3 discusses the polynomial $g_{25}(x)$ and its factorization into five conjugate quintics over the cyclic field

$$F = \mathbf{Q}[\pi]/(\pi^5 + 5\pi^4 - 25\pi^2 - 25\pi - 5). \tag{1}$$

Section 3 proves Part A of Theorem 1.1 but does not address at all the more interesting issue of how we found $g_{25}(x)$.

Sections 4 and 5 describe how $g_{25}(x)$ was found. In brief, we worked with a one-parameter family of polynomials

$$f_5(j, x) = x^5 + 5x^4 + 40x^3 - 1728j \tag{2}$$

related to five-torsion points on elliptic curves. We looked at many specializations of this family, eventually finding a suitable $j_2 \in F$. The product of $f_5(j_2, x)$ and its four conjugates is a polynomial in $\mathbf{Q}[x]$ defining K. The polynomial $g_{25}(x)$ is then obtained by adjusting this product polynomial to get a monic polynomial with relatively small integral coefficients defining the same field. Section 4 focuses on why we worked with $f_5(j, x)$ and Section 5 explains how we found j_2. Our main goal in these two sections is to communicate a practical sense of

the search process. We aim to provide enough information to support similar computations aimed at finding different fields in the future.

Section 6 uses division polynomials to get a degree 24 polynomial $f_{24}(j_2, x)$. The product of $f_{24}(j_2, x)$ and its four conjugates is a polynomial in $\mathbf{Q}[x]$ and $g_{120}(x)$ of Part B of Theorem 1.1 is then obtained by reducing the size of coefficients as before. It is a simple fact that $\tilde{L}/L$ is unramified, and so Section 6 proves Part B of the theorem.

Section 7 computes Frobenius elements for our field $\tilde{L}$. We explain how complete Frobenius information for L/F can be deduced from $g_{25}(x)$ alone. Similarly, complete Frobenius information about an intermediate extension $L(e^{2\pi i/5})/F$ easily follows by considering also the class of primes modulo 4. Finally $g_{120}(x)$ resolves some but not all of the remaining two-fold ambiguities to give further information about Frobenius elements for $\tilde{L}/F$. The Frobenius elements we compute match the characteristic 5 Hecke eigenvalues tabulated in [7, Table 3.9]; this agreement continues for all primes, by the 2010 result of [7] alluded to above.

Section 8 analyzes a general class of p-adic fields which includes the 5-adic completion of K and summarizes the regularity found as Theorem 8.1. Section 9 applies this theorem to get Corollary 9.1, applying to L and related fields, as explained above. Our analysis in Sections 8 and 9 can be compared to Serre's calculation [25] that Dembélé's field for $(G, S) = (SL_2(2^8)^2.8, \{2\})$ has root discriminant ≤ 55.395.

1.4. **Previously known nonsolvable fields ramified at one prime.** For some further context, we should mention that from the theory of classical modular forms of level one it has long been known that for each prime $p \geq 11$ there exists a nonsolvable field with $G = PGL_2(p)$ and $S = \{p\}$; see e.g. [30]. For some recently computed defining equations, see [3]. For defining equations for some other nonsolvable fields ramified at one prime only, see [13]. It is interesting to note that the field with $G = PGL_2(11)$ and $S = \{11\}$ given by this theory also arises from a specialization of the j-line. The polynomial $f_5(j, x)$ is replaced by a degree 12 polynomial defining the modular curve $X_0(11)$ and the complicated $j_2 \in F$ above is replaced by $-64/297 \in \mathbf{Q}$. A degree 24 polynomial analogous to $g_{120}(x)$ with Galois group $SL_2^{\pm}(11)$ is given in [13, §7].

2. Mass Heuristics

2.1. **Local mass formulas.** In [20] we combined the Krasner-Serre mass formula [23] with generating function arguments to obtain the total mass $\lambda_{F,n}$ of isomorphism classes of degree n separable algebras over a given v-adic base field F. The contribution of an isomorphism class $[K/F]$ is its mass $1/a$, where a is the number of automorphisms of K which fix F.

One has $\lambda_{\mathbf{C},n} = 1/n!$, the mass all coming from the unique algebra $\mathbf{C}^n$ with its $n!$ automorphisms. Similarly $\lambda_{\mathbf{R},n} = i_n/n!$ where i_n is the number of elements of order at most two in the symmetric group S_n. The other easy case is when n is greater than the residual characteristic p of F. In this case, $\lambda_{F_n} = \lambda_n$, the number of partitions of n.

The remaining cases are all more complicated, but one of the results of [20] is that $\lambda_{F,n}$ depends on F only through p and the degree $n_0 = [F : \mathbf{Q}_p]$. Accordingly, we write write $\lambda_{F,n} = \lambda_{p,Q,n}$ where $Q = p^{n_0}$. The relevant quantities for quintics are

$$\lambda_{\mathbf{C},5} = \frac{1}{120}, \qquad \lambda_{2,Q,5} = 2Q + Q^2 + 4Q^3,$$
$$\lambda_{\mathbf{R},5} = \frac{26}{120}, \qquad \lambda_{3,Q,5} = 1 + 6Q,$$
$$\lambda_5 = 7, \qquad \lambda_{5,Q,5} = 1 + 5Q.$$

2.2. **Global mass heuristics.** Now let F be a number field. Let Σ be a finite set of places of F. Let U be the set of real places of F not in Σ. Let $\mathrm{Fields}^{\mathrm{big}}_{F,n,\Sigma}$ be the set of isomorphism classes of degree n field extensions K of F such that the corresponding Galois closure M over F satisfies $\mathrm{Gal}(M/F) = A_n$ or $\mathrm{Gal}(M/F) = S_n$ and all ramification is over Σ. Then, adapting [2] to a somewhat different context, we argued in [20, §11] for the heuristic

$$|\mathrm{Fields}^{\mathrm{big}}_{F,n,\Sigma}| \approx \frac{1}{2} \prod_{v \in U} \frac{1}{n!} \prod_{v \in \Sigma} \lambda_{F_v,n}. \tag{3}$$

Here the absolute values on the left are to be interpreted as total mass, but this agrees with cardinality when $n \neq 2, 3$. The heuristic is to be understood with some caveats [20, §11]. In particular, for very small Σ it seems that there are generally substantially fewer fields than predicted.

2.3. **Quintics.** For quintics over $\mathbf{Q}$ and quintics over our quintic F the numbers work out as follows.

	$F = \mathbf{Q}$				$F = \mathbf{Q}[\pi]/(\pi^5 + 5\pi^4 - 25\pi^2 - 25\pi - 5)$			
S	$\{5\}$	$\{3,5\}$	$\{2,5\}$	$\{2,3,5\}$	$\{5\}$	$\{3,5\}$	$\{2,5\}$	$\{2,3,5\}$
Predicted:	2.9	56	120	2,200	3.7	5,400	490,000	720,000,000
Actual:	0	28	43	1,415	≥ 1	$\gg 33$	$\gg 154$	$\gg 905$

Here $\Sigma = \{\infty\} \cup S$ in the case of ground field $\mathbf{Q}$ and $\Sigma = \nu^{-1}(\{\infty\} \cup S)$ in the case of the quintic ground field F, with ν being the natural map from places of F to places of $\mathbf{Q}$. Thus in the last column of the table, Σ has the form $\{\infty_1, \infty_2, \infty_3, \infty_4, \infty_5, 2, 3, \pi\}$.

The numbers in the predicted row are rounded to two significant digits. The numbers in the actual row for $\mathbf{Q}$ are drawn from [15]. The numbers in the actual row for the quintic F are the numbers of fields found in the modest search of Section 5. From searches in the context of §4.1, §4.2, and §4.4, we know for sure that there are indeed many more fields, as indicated. The main point of the numbers in the actual row for the quintic F is they faithfully capture the ratios encountered by searches: it is very easy to find $\{2,3,5\}$ relative quintics, much harder to find $\{2,5\}$ relative quintics, perceptibly harder still to find $\{3,5\}$ relative quintics, and very much harder still to find a $\{5\}$ relative quintic.

2.4. **Behavior over R.** Note that in the language of this section, where $\mathbf{C}/\mathbf{R}$ is considered ramified, Gross's original question asks for nonsolvable number fields ramified within $\Sigma = \{\infty, p\}$ for some $p \leq 7$. The currently known constructional techniques are quite restrictive on the placement of complex conjugation in Galois groups. For example, the use of Hilbert modular forms as in [7] requires the field F to be totally real, but, in the case $p > 2$, yields only fields which are ramified above each real place of F. Reflecting these restrictions, real places of F are preferred over complex places in the specialization technique of Section 5, because two real places contribute two independent units while one complex place contributes only one such unit. Furthermore, specializing nonsolvable three-point covers can only give fields which have complex places over every infinite place of the specialization field F [24, §6].

One could of course ask about the existence of nonsolvable number fields ramified at exactly $\Sigma = \{p\}$. The smallest prime p for which it is known that there exists a nonsolvable number field for $\Sigma = \{p\}$ is $p = 1039$ [13, §4]. The field has Galois group A_5 and discriminant 1039^4. There are no other fields with $p \leq 1039$ and Galois group A_5, S_5, A_6, or S_6 [13, 15]. The heuristics of this section suggest that nonsolvable fields for $\Sigma = \{p\}$ should be much rarer still than fields for $\Sigma = \{\infty, p\}$. It is very plausible that for infinitely many primes p, they do not exist.

3. Discussion of $g_{25}(x)$

In this section we discuss various aspects of $g_{25}(x)$. The discussion both proves Theorem 1.1A and introduces the reader to some of the objects considered in subsequent sections. Here and throughout this paper, many of our assertions can only be confirmed with the assistance of a computer. However our presentation aims to emphasize various aspects of the situation that can be easily seen without a computer.

3.1. **Ramification at 5.** The fact that K is highly ramified at 5 can be seen directly from the coefficients of $g_{25}(x)$. Visibly, 5 divides the coefficient of each term except x^{25} and also 5 exactly divides the constant term -36535. Thus $g_{25}(x)$ is Eisenstein at 5. As 5 also divides the degree 25, one gets that K is wildly ramified at 5 and so 5^{25} divides $\mathrm{disc}(K/\mathbf{Q})$.

However one can easily go much further than simply $5^{25}|\mathrm{disc}(K/\mathbf{Q})$. Note that 5 divides many of the coefficients to quite high powers:

$$\begin{aligned} g_{25}(x) = x^{25} & \\ &+5\left(22x^{20} - 7307\right) \\ &+25\left(-x^{22} + x^{21} - 2288x^{15} + 69793x^{10}\right) \\ &+125\left(-29x^{17} + 174x^{16} + 34153x^7 - 28408x^6 + 7597x^5 - 7198x^2 + 2333x\right) \\ &+625\left(-x^{19} + 2x^{18} + 717x^{12} - 1802x^{11} - 1611x^9 - 1128x^8 - 1268x^4 + 2086x^3\right) \\ &+3125\left(36x^{14} - 77x^{13}\right). \end{aligned}$$

In general, if a polynomial $g(x) \in \mathbf{Z}[x]$ is Eisenstein at a prime p, then the contribution of p to the field and polynomial discriminants agree and this common number can be read off from congruential conditions on the coefficients of $g(x)$. In our case, writing the general term as $a_i x^i$, one has $5||a_0, a_{20}$ and $5^2|a_5, a_{10}, a_{15}, a_{21}, a_{22}, a_{23}, a_{24}$ while 5^3 divides the remaining a_i. The 5-Eisenstein polynomials satisfying these conditions are exactly the ones contributing 5^{69}. A standard reference on this topic is [22, III.6]; our [20, §8] also treats this issue.

3.2. **Lack of ramification away from 5.** Applying say *Pari*'s `nfdisc`, one gets that $g_{25}(x)$ has field discriminant exactly 5^{69} in under a second. To see this more directly, one can work with polynomial discriminants and factorization modulo primes. The polynomial discriminant of $g_{25}(x)$ factors into primes as

$$\begin{aligned} D \;=\; & 5^{69}\, 7^{40}\, 457^2\, 607^2\, 10193^2\, 33749^2\, 1433699^2 \\ & 9865993^2\, 47227393999^2\, 144256219620449^2\, 346858998100585793^2. \end{aligned}$$

For each of the nine factors p^2, one can apply a simple test: in general, suppose p^2 exactly divides the polynomial discriminant of a degree n monic polynomial $g(x) \in \mathbf{Z}[x]$; then p does not divide the field discriminant if and only if $g(x)$ has the form $g_{n-2}(x)(x-a)^2$ in $\mathbf{F}_p[x]$ with $g_{n-2}(x)(x-a)$ having distinct roots. Applying the test in our cases shows that indeed these p do not divide $\mathrm{disc}(K/\mathbf{Q})$. One can show directly that 7 does not divide $\mathrm{disc}(K/\mathbf{Q})$ by a similar but more involved argument involving Newton polygons. We omit this argument because it will be immediate conceptually from our construction in Sections 4 and 5 that in fact all primes besides 5 do not divide $\mathrm{disc}(K/\mathbf{Q})$.

3.3. **Notation for the ground field F.** To go further in the analysis of K, it is best to use a presentation of K more refined than $K = \mathbf{Q}[x]/g_{25}(x)$. Consider the field F defined in (1). Via $\pi \mapsto -c^4 - c^3 + 4c^2 + 3c - 3$ with $c = 2\cos(2\pi/25)$, the field F is identified with the unique quintic subfield of the degree twenty cyclotomic field $\mathbf{Q}(e^{2\pi i/25})$. The construction of Dembélé, Greenberg, and Voight [7] shows that the field K can be viewed as a quintic

extension of F, although these authors highlight the field element $b = \pi + 1$, rather than π. Let

$$\sigma(\pi) = 7^{-1}(-4\pi^4 - 18\pi^3 + 9\pi^2 + 92\pi + 40) \tag{4}$$

Then σ extends to an automorphism of F and $\mathrm{Gal}(F/\mathbf{Q}) = \{1, \sigma, \sigma^2, \sigma^3, \sigma^4\}$.

Let R be the ring of integers of F. The polynomial discriminant of the polynomial defining F in (1) is $5^8 7^2$ while the field discriminant is 5^8. Thus our standard basis 1, π, π^2, π^3, π^4 for F spans only an index seven lattice in R. This accounts for the ubiquity of inconsequential 7's in denominators throughout this paper.

To carry out our computations over F, it is essential to have good control over the ideal theory of R. Because $F/\mathbf{Q}$ is cyclic of prime order this ideal theory is particularly simple. First, in R one has $(5) = (\pi)^5$. Second, if p is congruent to 1, 7, 43, 49, 51, 57, 93 or 99 modulo 100, then (p) is the product of five conjugate ideals, all with residual field $\mathbf{F}_p$. Third and lastly, if p is otherwise then (p) is a prime ideal in R.

It is also essential for our purposes to have good control over the multiplicative group $F^\times$. Because F has class number one, the multiplicative group $F^\times$ is relatively easy to work with. Some important elements besides π are

$$u_i = \sigma^{i-1}(\pi) + 1, \qquad \omega_{7,i} = \sigma^{i-1}(\pi) + 2. \tag{5}$$

The elements u_1, u_2, u_3, u_4, u_5 are conjugate units. Any four of them together with -1 generate the unit group of F. We take $\omega_{7,i}$ for $i = 1, \ldots, 5$ as our standard generators for the corresponding five prime ideals $\Pi_{7,i}$ above 7. For split primes p larger than 7, the five primes Π above p are in natural bijection with the five roots $r \in \mathbf{F}_p$ of the polynomial defining F in (1), according to the image of π in $R/\Pi \cong \mathbf{F}_p$. Viewing these roots as in $\{0, \ldots, p-1\}$, we let r_1 be the smallest and let $\Pi_{p,1}$ be the corresponding ideal. Then we label the other ideals so that $\Pi_{p,i}^\sigma = \Pi_{p,i+1}$ always holds, and let r_i correspond to $\Pi_{p,i}$. This level of detail is necessary to fully match Frobenius elements to Hecke eigenvalues, and how things look explicitly can be seen in the left part of Table 7. When we need a generator $\omega_{p,1}$ of $\Pi_{p,1}$, we choose one arbitrarily. Then we get generators for the other ideals above p via $\omega_{p,i}^\sigma = \omega_{p,i+1}$. Note that here and in the sequel we often use exponential notation for Galois actions, as in $\sigma(\pi) = \pi^\sigma$.

3.4. **Factorization over F.** The needed notation having been set up, we can now give the promised refined presentation of K. Let

$$\alpha = -\frac{5}{7}\left(3\pi^4 + 10\pi^3 - 19\pi^2 - 62\pi + 5\right) = u_1^{-2}u_2^3u_3^{-1}u_4^{-3}\pi^6, \tag{6}$$

$$\omega_{7307,3} = \frac{1}{7}(-79\pi^4 - 331\pi^3 + 288\pi^2 + 1803\pi + 566), \tag{7}$$

and

$$f_5(x) = x^5 + \alpha x^2 - \alpha x + \pi\omega_{7307,3}. \tag{8}$$

Then

$$g_{25}(x) = \prod_{i=1}^{5} f_5^{\sigma^i}(x). \tag{9}$$

Thus $K = F[x]/f_5(x)$ together with (1) is a two-step presentation of K.

3.5. **Polynomial discriminant.** The polynomial discriminant of $f_5(x)$ is

$$\begin{aligned} D &= \frac{5^5}{7}\left(99432077\pi^4 + 407302465\pi^3 - 362208460\pi^2 - 2145278225\pi - 552808790\right) \\ &= \pi^{29}\omega_{7,1}^6\omega_{7,4}^4\omega_{10193,1}^2 u_1^{-8}u_2^{15}u_3^{-1}u_4^{-11}, \end{aligned}$$

with $\omega_{10193,1} = \pi^4 + 4\pi^3 - \pi^2 - 19\pi - 23$. One thus has $D \sim d = \pi u_2 u_3 u_4$, with $\sim$ indicating equality in $F^\times/F^{\times 2}$. One can check that $\pi^\sigma = \pi u_1 u_3 u_4$. Accordingly,

$$\frac{d^\sigma}{d} = \frac{(\pi u_1 u_3 u_4)u_3 u_4 u_5}{\pi u_2 u_3 u_4} = \frac{u_1 u_3 u_4 u_5}{u_2} \sim u_1 u_2 u_3 u_4 u_5 = 1.$$

Thus D is not itself a square, but it agrees with all its conjugates modulo squares.

3.6. **Galois group.** Because $g_{25}(x)$ has the factorization (9) and $\mathrm{Gal}(F/\mathbf{Q}) = C_5$, the Galois group G of $g_{25}(x)$ is a subgroup of the wreath product $S_5^5.C_5$. Because the polynomial discriminant of $f_5(x)$ is a nonsquare in F, but agrees with each of its conjugates up to a square, one has that G is a subgroup of $A_5^5.C_2.C_5 \cong A_5^5.10$. The Frobenius elements tabulated in Table 7 are then more than sufficient to force G to be all of $A_5^5.10$.

3.7. **T_2-reduction.** For a monic polynomial $h(x) = \prod_i (x - \alpha_i)$ in $\mathbf{Z}[x]$, define $T_2(h) = \sum_i |\alpha_i|^2$. If all roots of $h(x) = x^n + a_1 x^{n-1} + a_2 x^{n-2} + \cdots$ are real, then the absolute values are superfluous, and $T_2(h)$ is the integer $a_1^2 - 2a_2$. In general, $T_2(h)$ is an algebraic integer in the splitting field of h. It is conventional to present number fields as $\mathbf{Q}[x]/h(x)$ with h chosen to minimize $T_2(h)$, as typically coefficients are then fairly small as well. If $h(x)$ minimizes T_2 then $(-1)^n h(-x)$ also minimizes T_2 and typically there are no other minimizing polynomials. The command `polredabs` in *Pari* carries out this reduction. Our $g_{25}(x)$ and $g_{30}(x)$ just below are T_2-reduced with $T_2(g_{25}) \approx 110.92$ and $T_2(g_{30}) \approx 102.84$. On the other hand we prefer to define F in (1) via $\pi^5 + 5\pi^4 - 25\pi^2 - 25\pi - 5$ with its T_2 of 25 rather than via $b^5 - 10b^3 - 5b^2 + 10b - 1$ with its T_2 of 20 as in [7]. This is because using the uniformizer π rather than the unit $b = u_1 = \pi + 1$ makes 5-adic behavior more evident.

3.8. **Sextic analog.** One can work with the sextic polynomal (18) rather than the quintic polynomial (2). Proceeding as before, including T_2-reduction, one gets that

$$\begin{aligned} g_{30}(x) = {} & x^{30} - 5x^{29} + 10x^{28} + 15x^{27} - 170x^{26} + 429x^{25} + 550x^{24} - 8175x^{23} \\ & + 33350x^{22} - 83150x^{21} + 122955x^{20} - 27500x^{19} - 375050x^{18} + 1050375x^{17} \\ & - 1390025x^{16} + 309375x^{15} + 2499150x^{14} - 4752625x^{13} + 2829175x^{12} \\ & + 2859125x^{11} - 6266355x^{10} + 3272775x^9 + 1787275x^8 - 3243075x^7 \\ & + 1099450x^6 + 565746x^5 - 468930x^4 + 45160x^3 + 53915x^2 - 12845x - 2351 \end{aligned}$$

has the same splitting field as $g_{25}(x)$. The polynomial $g_{30}(x)$ factors into five sextics over F, namely

$$\begin{aligned} f_6(x) &= x^6 + 7^{-1}\left(-4\pi^4 - 11\pi^3 + 23\pi^2 + 50\pi - 2\right)x^5 \\ &\quad + 5x^4 - 5x^2 + \left(-3\pi^3 - 7\pi^2 + 20\pi + 24\right) \end{aligned} \tag{10}$$

and its four conjugates. The sextic analog f_6 will prove convenient in Sections 6 and 7, as the field $K_{30} = \mathbf{Q}[x]/g_{30}(x) = F[x]/f_6(x)$ is a subfield of the degree 120 field $\tilde{K}$ considered there, while $K = \mathbf{Q}[x]/g_{25}(x) = F[x]/f_5(x)$ is not. On the other hand, f_6 does not fit so conveniently into the p-adic considerations of Sections 8 and 9. In fact, $g_{30}(x)$ factors modulo 5 as $(x-4)^{25}(x-1)^5$. This factorization corresponds to a 5-adic factorization $(K_{30} \otimes \mathbf{Q}_5) \cong (K \otimes \mathbf{Q}_5) \times (F \otimes \mathbf{Q}_5)$.

4. Choosing a Family to Specialize

In this section, we explain why we chose the family (2) of quintic polynomials to exhaustively specialize. In the process, we discuss two larger families that we rejected in favor of (2), and also three other families which have just one parameter like (2). Any one of these other families could be the best choice in similar searches for different relative quintics.

The main point in this section, appearing at the end of §4.3, is that the family (2) is guaranteed to contain a specialization point corresponding to the field K sought, by a theorem of Shepherd-Barron and Taylor [27]. This theorem is very particular to our exact situation here, and the rest of our discussion gives some feel for how one might go about choosing the most promising family in other situations.

4.1. **All quintics.** A natural place to start our considerations is the family

$$f(a,b,c,d,e,x) = x^5 + ax^4 + bx^3 + cx^2 + dx + e \tag{11}$$

of all quintics. Driver and Jones [8] have successfully specialized this family to get complete lists of quintics with certain prescribed ramification behavior over quadratic fields F.

Our search is for a single field only, and so the complications of ensuring that a list is complete are not present. On the other hand, our base is quintic and this adds enormous computational complexity in comparison with the quadratic case.

The discriminant $D(a,b,c,d,e)$ has 59 terms each of which has weighted degree 20 when a, b, c, d, e are respectively given weights 1, 2, 3, 4, 5. Standard searches take a, b, c, d, and e in the ring of integers R of F, with a very small. The case $a = 0$ is representative of the others, and for it we have

$$\begin{aligned} D(0,b,c,d,e) = & \\ & 108b^5e^2 - 72b^4cde + 16b^4d^3 + 16b^3c^3e - 4b^3c^2d^2 - 900b^3de^2 + 825b^2c^2e^2 \\ & +560b^2cd^2e - 128b^2d^4 - 630bc^3de + 144bc^2d^3 - 3750bce^3 + 2000bd^2e^2 \\ & +108c^5e - 27c^4d^2 + 2250c^2de^2 - 1600cd^3e + 256d^5 + 3125e^4. \end{aligned} \tag{12}$$

The search process involves plugging in $(b,c,d,e) \in R^4$ and, in our case, immediately rejecting those (b,c,d,e) for which the integer $\mathrm{Norm}_{F/\mathbf{Q}}(D(0,b,c,d,e))$ is not of the form $5f^2$. Even for (b,c,d,e) very small, the integer $|\mathrm{Norm}_{F/\mathbf{Q}}(D(0,b,c,d,e))|$ tends to be larger than 10^{15} and so it is very difficult for (b,c,d,e) to pass even this very first test.

4.2. **Dodecahedral quintics.** The degrees of the irreducible complex characters of A_5 are 1, 3, 3, 4, and 5. The two three-dimensional characters have character field $\mathbf{Q}(\sqrt{5})$ and are conjugate; each corresponds to rotating a dodecahedron in real three space. Extended to the group $A_5 \times \{\pm 1\}$, these representations are reflection representations, in fact number twenty-three on the Shephard-Todd list [26]. Since the quotient space $\mathbf{R}^3/(A_5 \times \{\pm 1\})$ is just another copy of $\mathbf{R}^3$, one can construct a corresponding family of polynomials for the original group A_5:

$$\begin{aligned} f(a,b,c,x) \quad = \quad & x^5 + (-10ab)x^3 + (5ac + 40b^2)x^2 + (-15a^3c - 55a^2b^2 + 5bc)x \\ & +(8a^5c + 40a^4b^2 + 5a^2bc + c^2). \end{aligned} \tag{13}$$

The polynomial discriminant of $f(a,b,c,x)$ is

$$D(a,b,c) = 5^5 \left(a^5 - 5a^2b - c\right)^2 \Delta(a,b,c)^2 \tag{14}$$

where

$$\Delta(a,b,c) = 64a^5c^2 + 640a^4b^2c + 1600a^3b^4 - 80a^2bc^2 - 720ab^3c - 1728b^5 - c^3. \tag{15}$$

Here, when one gives a, b, and c weights 1, 3, and 5 respectively, $\Delta(a,b,c)$ has weighted degree 15. Very promisingly for finding our K, the discriminant can only be of the form $5f^2$. Not relevant for us, but perhaps worth mentioning, is that $\Delta(a,b,c)$ is also involved in another discriminant formula: $\mathrm{disc}(x^5+5ax^4-20bx^2-4c) = 2^8 5^5 c\Delta(a,b,c)$.

In principle, the situation here should be similar to the case of general quintics, although it has not been worked out in the literature. Namely any quintic field K over any number field F with $\mathrm{disc}(K/F) = 5 \in F^\times/F^{\times 2}$ should have infinitely many defining polynomials $f(a,b,c,x) \in R[x]$. Moreover at least one defining polynomial should have a, b, c satisfying certain bounds depending only on the signature of F and the size of the field discriminant $\mathrm{disc}(K/F)$.

Even though the full theory is not set up, one can carry out exploratory searches over small parts of R^3. The factor $\left(a^5-5a^2b-c\right)^2$ in (14) does not contribute to field discriminants and is irrelevant for us. The factor $\Delta(a,b,c)$ is crucial for immediately eliminating polynomials, for if a prime p exactly divides the integer $\mathrm{Norm}_{F/\mathbf{Q}}(\Delta(a,b,c))$ then p is necessarily ramified in $F[x]/f(a,b,c,x)$.

In terms of finding a defining polynomial for our particular K/F, searching via (13)–(15) seems much more promising than searching via (11)–(12). However again one has the fundamental problem that $|\mathrm{Norm}_{F/\mathbf{Q}}(\Delta(a,b,c))|$ tends to be larger than 10^{15}. Note however that our choice of coordinates (a,b,c) in (13)–(15) has been made so that the numeric factor in (14) is a power of 5. One could change coordinates in a number of natural ways to get much smaller coefficients in (15) at the expense of getting factors of 2 and/or 3 in (14).

4.3. **Modular quintics.** When carrying our modest searches using (13)–(15) as just sketched, it happened that almost all of the least ramified fields found had a equal to zero. To pursue this, note first that $\Delta(0,b,c) = -1728b^5 - c^3$. Carrying out the substitution $(b,c,x) \to (j,-12j^2,-12j/x)$, the polynomial $f(0,b,c,x)$ becomes the polynomial of (2),

$$f_5(j,x) = x^5+5x^4+40x^3-1728j = x^5+5x^4+40x^3-J, \tag{16}$$

with discriminant

$$D(j) = 2^{24}3^{12}5^5 j^2(j-1)^2 = 5^5 J^2(J-1728)^2. \tag{17}$$

Here j is the coordinate we will use in the sequel, to keep within the standard conventions of three point covers, where $j = 0$, 1, and ∞ are the special values. The alternative coordinate $J = 1728j$ is more natural in the setting of elliptic curves.

In fact, $f_5(j,x)$ is a familiar polynomial from the theory of elliptic curves as follows. The projective line with coordinate j is naturally identified with the j-line $X_0(1)$ parametrizing elliptic curves. One can view $f_5(j,x)$ as defining a degree 5 map from a curve X with function field $\mathbf{Q}(x)$ to $X_0(1)$ with Galois group S_5. This cover is the quintic version of the standard cover $X_0(5)$ with defining polynomial

$$f_6(j,x) = \left(x^2-10x+5\right)^3 + 1728jx \tag{18}$$

and Galois group $PGL_2(5)$.

The simplicity of the discriminant formula (17) is very promising, and accounts for the experimental phenomenon of a commonly being 0 for the least ramified fields. However a new fundamental concern arises. Certainly, not all quintic field extensions of a given number field F with $d = 5 \in F^\times/F^{\times 2}$ arise as specializations of (16). For (16) to be useful for us, we need our K/F to so arise. If it does arise, then it arises infinitely often; see [9] for some related explicit formulas in the case $F = \mathbf{Q}$.

Theorem 1.2 of [27] answers our fundamental concern. It says that for any ground field F of characteristic zero, a $PGL_2(5)$ extension arises as a specialization of (16) if and only if it lifts to a $GL_2(5)$ extension having cyclotomic determinant. This is the case for the $PGL_2(5)$ extension of [7].

4.4. **Other quintic three-point covers.** Family (2) is a quintic cover of the j-line with Galois group S_5, ramified at the three points 0, 1, and ∞ only. There are other such covers, all of them being base changes of four possibilities:

χ	λ_0	λ_1	λ_∞	$f(j,x)$	$D(j)$
$1/30 = 0.0\overline{3}$	311	221	5	$x^3\left(x^2+5x+40\right)-1728j$	$2^{24}3^{12}5^5j^2(j-1)^2$
$-1/20 = -0.05$	41	2111	5	$x^4(x-5)\quad+256j$	$2^{32}5^5j^3(j-1)$
$-1/12 = -0.08\overline{3}$	32	221	41	$x^3(x-10)^2\ -108(5x+4)j$	$-2^{18}3^{15}5^5j^3(j-1)^2$
$-2/15 = -0.1\overline{3}$	32	2111	5	$x^3(x-5)^2\quad-108j$	$2^83^{12}5^5j^3(j-1)$

Here (2) is reproduced on the first line, for easy comparison. In general, the partitions λ_0, λ_1, and λ_∞ measure ramification of the cover above $\tau = 0$, 1, and ∞, respectively. Table 1 describes ramification in specializations of (2) and one can construct analogs of this table for the remaining three covers. Just as for (2), for the last three covers also there are 2-adic regions where 2 does not ramify and 3-adic regions where 3 does not ramify. Thus the last three covers are *a priori* possibilities for finding the field K sought.

Even if one did not have Theorem 1.2 of [27], Cover (2) would seem the most promising of these four covers. One reason is that only for (2) is the discriminant restricted to be $5 \in F^\times/F^{\times 2}$. Another reason concerns the Euler characteristic $\chi = \frac{1}{e_0} + \frac{1}{e_1} + \frac{1}{e_\infty} - 1$, with e_τ the least common multiple of the parts of λ_τ. As this quantity becomes more negative, the harder it becomes to find specialization points keeping ramification within a fixed set of primes, as the exponents on x, y, and z in the analogs of (20), (21) become larger. Only in the first case can there be infinitely many specialization points keeping ramification within a given set of primes. See e.g. [5] for this finiteness statement and general background on considerations involving Euler characteristics. An opposing argument in favor of the second-listed cover is that only for it is 3 generically unramified.

4.5. **Discussion.** One should note that it is not the degree, five in our case, which directly governs computational complexity. For example, we are emphasizing $f_5(j,x)$ from (2) throughout this paper, but this section and the next would change only trivially if we had used $f_6(j,x)$ from (18). It is instead the nature of the discriminant formula which is the central concern. Some three-point covers of large degree are possibilities to get fields ramified at one prime only for other nonsolvable groups. The specialization considerations of the next section would then serve as a model.

On the other hand, for three-point covers with larger groups it seems that most commonly there are at least two primes at which all specializations ramify. Also, one expects no analogs of Theorem 1.2 of [27] for larger groups, since this theorem is connected to the Euler characteristic χ being positive. Thus it seems very possible that fields ramified at one prime will arise naturally only in families with more than one parameter, such as those of §4.1 and §4.2. Finding a correct specialization point would then remain a very difficult problem.

5. Specialization

Specializing three-point covers has both local and global aspects. We explain these aspects in turn with reference to the modular family (2). We follow the notation of [21], where specialization over the field $\mathbf{Q}$ was considered systematically. In particular we denote the

affine curve $\mathbf{P}^1 - \{0, 1, \infty\}$ by T. In terms of finding $g_{25}(x)$ and $g_{120}(x)$, Eq. (23) identifying j_2 is the main point.

5.1. **Local aspects.** For this paragraph, let F be a p-adic field with ring of integers R, prime ideal Π, and residue field R/Π having q elements. Consider the F-algebras $K_j = F[x]/f_5(j, x)$ as j varies over $T(F) = F - \{0, 1\}$. By Krasner's Lemma the isomorphism type of K_j is locally constant in j.

It is convenient to start the local analysis by focusing on a decomposition into open sets:

$$T(F) = T(F)^{\mathrm{gen}} \coprod \left(\coprod_{i=1}^{\infty} T(F)^{0,i} \right) \coprod \left(\coprod_{i=1}^{\infty} T(F)^{1,i} \right) \coprod \left(\coprod_{i=1}^{\infty} T(F)^{\infty,i} \right). \tag{19}$$

Here $T(F)^{\mathrm{gen}} = R - \Pi$ and

$$T(F)^{0,i} = \Pi^i - \Pi^{i+1}, \quad T(F)^{1,i} = (1 + \Pi^i) - (1 + \Pi^{i+1}), \quad T(F)^{\infty,i} = \Pi^{-i} - \Pi^{-i-1}.$$

The natural measure μ on $T(F)$ gives $T(F)^{\mathrm{gen}}$ mass $q - 2$ and each $T(F)^{\tau,i}$ mass $(q-1)/q^i$ so that all of $T(F)$ has mass $q + 1$.

Table 1 has been normalized to facilitate applications to our global quintic F. Let $j \in F - \{0, 1\}$ so that the discriminant $\mathrm{disc}(K_j/\mathbf{Q})$ is a positive integer. Let p be a prime and consider the local discriminant-exponent $c = \mathrm{ord}_p(\mathrm{disc}(K_j/\mathbf{Q}))$. Suppose that $p \geq 7$ is inert in F. Then the last of the five blocks is relevant. If $j \in T^{\mathrm{gen}}(F)$, then $c = 0$, as indicated in the first column. If $j \in T^{\tau,i}(F)$ then c is given in the (τ, i) slot of the block to the right, with blank slots being determined by repeating the parenthesized segment. Thus, for example, $c = 0$ if and only if (τ, i) has the form $(0, 3k)$, $(1, 2k)$, or $(\infty, 5k)$. If $p \geq 7$ is a split prime then the situation is similar, except one has five independent contributions to c, all computed from the fourth of the five blocks on Table 1.

TABLE 1. The possibilities for the contribution of a p-adic prime ideal Π to the discriminant-exponent of the local field $K_j/\mathbf{Q}_p$. Here and in the next three tables, boldface indicates no ramification at 2 and italics indicate no ramification at 3.

gen	τ	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
$\Pi = (2)$	0	40	20,10	30	20	20	(**0**	10	10)								
	1	30	(30	40)													
30,20	∞	40	20,10	30	20	20	(**0**	20	20	20	20)						
$\Pi = (3)$	0	(30	20	20)													
	1	20	20	(*0*	10)												
20,10	∞	20	20	(*0*	20	20	20	20)									
$\Pi = \pi$	0	67	65	63	61	55,47	57	55	53	51	45,43	47	45	(43	41	43)	
	1	67	65	63	61	55,47	57	55	53	51	45,43	47	45	47	45	(43	43)
65*	∞	(69	69	69	69	65*)											
Π split	0	(2	2	0)													
	1	(2	0)														
0	∞	(4	4	4	4	0)											
Π inert	0	(10	10	0)													
	1	(10	0)														
0	∞	(20	20	20	20	0)											

The blocks for the three wild primes 2, 3, and 5 have been computed non-rigorously by interpolation. The most important point here is the presence of zeros in the 2-adic and 3-adic blocks, some of these zeros following immediately from the polynomial discriminant formula (17). The other numbers are included for a more complete picture. They shed light on the distribution of global discriminants in Table 4 below, and also the local analysis of the final two sections. Occasionally, there are two possibilities for c for j in a given region. In all cases, the larger possibility is the more common, often by far. In one repeated situation, there are actually six possibilities for c. Namely, a printed 65^* indicates that the possibilities are 65, 61, 57, 53, 45, and 43. With respect to the measure μ, in each region these possibilities occur with relative frequency $4/5$, $4/5^2$, $4/5^3$, $4/5^4$, $4/5^5$, and $1/5^5$ respectively.

Table 1 gives one a first feel for the difficulty of choosing j so that only 5 ramifies in K_j. In terms of the measure μ, the fractions of $F_p - \{0,1\}$ yielding no ramification at p are respectively

$$p = 2: \qquad 2(64-1)/(64+1)(64^6-1) \approx 2.8 \times 10^{-11},$$
$$p = 3: \qquad 2(27-1)/(27+1)(27^3-1) \approx 9.4 \times 10^{-5}.$$

As we have to avoid ramification at both 2 and 3, this measure calculation suggests finding the appropriate j may be difficult.

5.2. **Specialization points.** Let F be our quintic field (1) with ring of integers R and consider the F-algebras $K_j = F[x]/f_5(j,x)$ indexed by $j \in F - \{0,1\}$. The discriminant $\mathrm{disc}(K_j/\mathbf{Q})$ is divisible only by the primes 2, 3, and 5 if and only if the following conditions are satisfied. First, one must be able to express j in the form

$$j = -\frac{ax^3}{cz^5}, \tag{20}$$

with a, c invertible in $R[1/30]$ and x, z in R. Second, there must likewise be $b \in R[1/30]^\times$ and $y \in R$ such that

$$ax^3 + by^2 + cz^5 = 0. \tag{21}$$

Here the equations (20),(21) together are exactly what is needed to ensure that for each prime Π different from 2, 3, and π, one has $c = 0$ from Table 1.

If j lies in $\mathbf{Q} - \{0,1\}$, then $K_j \cong \mathbf{Q}[x]/f_5(j,x) \otimes F$ and so the associated Galois group is within the subgroup $S_5 \times C_5$ of the the desired group $A_5^5.10$. We exclude these j from consideration. Conjugate j yield K_j which are isomorphic as extensions of $\mathbf{Q}$, and so in our discussion below we always take only one j from each conjugacy class $\{j, \sigma(j), \sigma^2(j), \sigma^3(j), \sigma^4(j)\}$.

We find solutions $j \in F - \mathbf{Q}$ by a modest computer search. Note first, however, that the j-line also parametrizes elliptic curves, and one may ask if the field we seek comes from the mod 5 representation associated to an elliptic curve over F with good reduction outside of 5. We expect the answer is no, because the field of coefficients in [7] is larger than $\mathbf{Q}$. Accordingly, the solution we seek should only come from ABC triples with $z \in R$ not a unit.

Our computer search is designed to not only find the field sought, but also to get some general perspective on the situation. We look at a great many j of the form (20) and select those for which the sum $ax^3 + cz^5$ has the right form $-by^2$. Our search is modest because for x and z we take either 1 or one of the five $\omega_{7,i}$. These are very low cutoffs and increasing the number possibilities for x and z would likely be the easiest way to get more fields. For a/c we take numbers of the form $2^\alpha 3^\beta \pi^\gamma u$ with $\alpha \in [-6,6]$, $\beta \in [-3,3]$, $\gamma \in [-6,6]$ and u running over more than a thousand units. When $x = z = 1$ then a solution j yields another one $f_2(j) = 4j(1-j)$ [21, §4]. Using this base change operator together with the direct search gives a total of 647 different j.

TABLE 2. Ordered pairs $(\mathrm{ord}_2(j), \mathrm{ord}_3(j-1))$ for 647 j-invariants found by the computer search of §5.2. Each of these j corresponds to a different K_j and the splitting fields all have Galois group $A_5^5.10$.

		$\mathrm{ord}_2(j)$											
		-5	-4	-3	-2	-1	0	1	2	3	4	5	6
	1					5	5	4					
	0	1	2	4	67	63	248	74	66	12	4		**1**
$\mathrm{ord}_3(j-1)$	-1			1		16	35	12				1	
	-2						5	9	8	3			
	-3						*1*						

The distribution of the pair $(\mathrm{ord}_2(j), \mathrm{ord}_3(j-1))$ is presented in Table 2. Note that these pairs cluster about the mode at $(0,0)$. Some of the horizontal spread comes from the use of the base change operator f_2.

According to Table 1, the field K_j is not ramified at 2 if and only if $\mathrm{ord}_2(j)$ is a non-zero multiple of 6. Similarly, K_j is not ramified at 3 if and only if $\mathrm{ord}_3(j-1)$ is a non-zero multiple of 3. Table 2 says that the search finds one field of each type. The field corresponding to the bold 1 comes from the ABC triple

$$2^6 - (\omega_{7,1}\omega_{2399,4})^2 - u_1 u_4^{-1} \pi^2 \omega_{7,4}^5 = 0.$$

Explicitly,

$$j_1 = \frac{u_1 \pi^2 \omega_{7,4}^5}{2^6 u_4} = \frac{-2^6}{5 \cdot 7^6}(68155\pi^4 + 288368\pi^3 - 125935\pi^2 - 1495535\pi - 1089160).$$

The field K_{j_1} has discriminant $3^{20}5^{69}$. The field coming from the italicized 1 has discriminant $2^{40}5^{67}$. A Frobenius computation reveals that the 647 fields are pairwise non-isomorphic, despite the repetition in field discriminants evident in Table 4 below. The lack of any repetition in fields whatsoever strongly suggests that longer searches would find many more fields. The same Frobenius computation also shows that all 647 fields have associated Galois group all of $A_5^5.10$.

5.3. **Base change.** Besides f_2, there are two more simple base change operators which allow one to pass from ABC triples of low height to ABC triples of larger height under certain conditions [21, §4]:

$$f_3(j) = \frac{(4j-1)^3}{27j}, \qquad f_4(j) = \frac{(9j-1)^3(1-j)}{64j}.$$

If K_j has discriminant of the form $2^a 3^b 5^c$ then so does $K_{f_3(j)}$ as long as one can take $x = 1$ in an ABC triple determining j. Similarly, if K_j has discriminant of the form $2^a 3^b 5^c$ then so does $K_{f_4(1-j)}$ as long as one can take $y = 1$ in an ABC triple determining j. Applying f_3 and f_4 to the appropriate j's discussed in the previous subsection gives 409 and 99 new j's respectively. However now there is some repetition of fields, mostly because $f_3(j) \neq f_3(1/j)$ and $f_4(1-j) \neq f_4(1-1/j)$ but in each case both sides define the same fields. One gets 205 distinct fields from f_3 and 53 distinct fields from f_4. The original list of 647 fields and the two new lists are pairwise disjoint giving a total of 905 fields. The associated Galois group in all cases is all of $A_5^5.10$.

TABLE 3. Ordered pairs $(\mathrm{ord}_2(j), \mathrm{ord}_3(j-1))$ for 409 j-invariants of the form $f_3(t)$ and 99 j-invariants of the form $f_4(1-t)$ with t one of the j-invariants contributing to Table 2. Underlining, italics, and boldface respectively indicate j's which come as $f_4(1-t)$, which yield a field unramified at 3, and which yield a field unramified at 2.

	−12	−11	−10	−9	−8	−7	−6	−5	−4	−3	−2	−1	0	1	2	3	4	5
1						$\underline{3}$	$\underline{\mathbf{4}}$				$\underline{1}$							
0	$\underline{4}$			$\underline{8}$	$\underline{3}$	$\underline{7}$	$\underline{\mathbf{50}}$				$\underline{7}$	4	2	3	$\underline{4}$			
−1				$\underline{3}$			$\underline{\mathbf{4}}$				$\underline{1}$							
−2																		
$\mathrm{ord}_3(j-1)$ −3							***1***		*3*	*5*	*55*	*31*	*146*	*30*	*45*			*2*
−4										1	2	9	19	5				
−5												5	22	10	6			
−6																		
−7										1	6	2	3					

In particular, our desired specialization point is $j_2 = f_3(j_1)$. An ABC triple corresponding to j_2 is

$$x^3 + u_4 y^2 + 2^6 3^3 u_1^2 u_4 \pi^4 z^5 = 0, \tag{22}$$

with

$$\begin{aligned} x = \omega_{7,1}\omega_{7,2}^2\omega_{3982743607} &= -51\pi^4 - 255\pi^3 + 176\pi^2 + 1549\pi + 379, \\ y = \omega_{7,3}\omega_{7,5}\omega_{257}\omega_{349} & \\ \omega_{2399}\omega_{2693}\omega_{14249} &= 7^{-1}(-5142\pi^4 - 26212\pi^3 + 11706\pi^2 + 138482\pi + 33507), \\ z = \omega_{7,4}^2 &= 7^{-1}(13\pi^4 + 55\pi^3 - 45\pi^2 - 292\pi - 67). \end{aligned}$$

Explicitly,

$$\begin{aligned} j_2 &= \frac{-x^3}{2^6 3^3 u_1^5 u_4 \pi^4 z^5} \\ &= \frac{-1}{2^6 3^3 5^1 7^{11}} \left(16863524372777476\pi^4 + 8854036993798358 8\pi^3 \right. \\ &\quad \left. -11247914660553215\pi^2 - 464399360515483572\pi - 353505866738383680\right). \end{aligned} \tag{23}$$

Note that each one of the five $\omega_{7,i}$ appears in the expression for either x, y, or z. On the other hand, for $p > 7$ it is not necessary here to distinguish between the different $\omega_{p,i}$ and so we have just written ω_p instead.

It is fortunate that j_2 arises via base change, as its large height makes it unlikely one could find it via a direct computer search that did not use the base change operators. Note also the factors of π^2 and π^4 in the denominator of j_1 and j_2 respectively. Via Table 1, these factors explain why K_{j_1} and K_{j_2} both have the maximum possible 5-adic discriminant, namely 5^{69}.

Table 4 gives a summary of the fields found by our search. All fields are wildly ramified at 5 since even F is wildly ramified at 5. Of the 153 fields ramified exactly at 2 and 5, all are wildly ramified at 2. Of the 32 fields ramified exactly at 3 and 5, all are wildly ramified at 3.

Thus among the fields found by our modest search, the unique field ramified at 5 only is an extreme outlier.

TABLE 4. The 905 fields K found by the search of §5.2 together with the base change operators of §5.3, sorted by discriminant $2^a3^b5^c$. Fields with $b = 0$ are emphasized by italics and fields with $a = 0$ are emphasized by boldface.

	3^0						3^{10}			3^{20}								3^{30}						
	5^{51}	5^{61}	5^{63}	5^{65}	5^{67}	5^{69}	5^{65}	5^{67}	5^{69}	5^{51}	5^{55}	5^{57}	5^{61}	5^{63}	5^{65}	5^{67}	5^{69}	5^{55}	5^{57}	5^{61}	5^{63}	5^{65}	5^{67}	5^{69}
2^0						***1***							**1**	**3**	**4**	**4**	**19**							**1**	
2^{10}														1		2	4								1
2^{20}		*2*	*1*	*3*	*5*	*29*				2	3		5	15	30	43	56				1	4	10	6
2^{30}		*1*	*1*	*3*	*6*	*61*		2			1	2	15	17	62	60	95	1		2	4	15	11	12
2^{40}	*1*	*1*	*4*	*8*	*4*	*23*	2		3		2	4	7	19	54	44	75		1	2	2	6	3	13

6. LIFTING TO $SL_2(5)^5.20$

In this section, we work with five-torsion points on an elliptic curve to produce the polynomial $g_{120}(x)$ appearing in Theorem 1.1B, so that $\tilde{K} = \mathbf{Q}[x]/g_{120}(x)$ has discriminant 5^{311}. We explain in the last subsection how suitably twisting $\tilde{K}$ gives three other degree 120 fields with the same splitting field $\tilde{L}$.

6.1. **Torsion points on elliptic curves.** Let F be a field of characteristic zero, let $j \in F - \{0, 1\}$, and let $d \in F^\times$. The elliptic curve with affine equation

$$d\frac{j}{288(j-1)^2}y^2 = x^3 - \frac{j}{48(j-1)}x + \frac{j}{864(j-1)} \tag{24}$$

has j-invariant j; see e.g. [28, III.1]. Our coefficients are chosen to keep coefficients in (25) relatively small. As one varies the twist factor d, the curve (24) represents all isomorphism classes of elliptic curves with j-invariant j. The isomorphism class of (24) depends exactly on $d \in F^\times/F^{\times 2}$.

The theory of division polynomials as very explicitly presented in [18] lets one pass from a given elliptic curve (24) and any prime $\ell > 2$ to a polynomial $f_{j,\ell}(x) \in F[x]$ of degree $(\ell^2-1)/2$ whose roots in an algebraic closure $\overline{F}$ are exactly the x-coordinates of the primitive ℓ-torsion points of the elliptic curve. Taking the resultant of this polynomial with the difference of the two sides of (24) gives a degree $\ell^2 - 1$ polynomial $f_{j,d,\ell}(y) \in F[y]$ whose roots are exactly the y-coordinates of the same torsion points. The dependence on d is simple as $f_{j,d,\ell}(y)$ has the form $\phi_{j,d,\ell}(dy^2)$.

In the case $\ell = 5$, this procedure gives

$$\begin{aligned}\phi_{j,d,5}(u) \;=\; & 125u^{12} - 9000ku^{11} + 5184k^2u^{10} + 199566ku^{10} - 1188000k^2u^9 \\ & +622080k^3u^8 - 6763905k^2u^8 - 8132400k^3u^7 + 1166400k^4u^6 \\ & -4193100k^3u^6 + 3359232k^5u^5 - 2387232k^4u^5 + 1399680k^5u^4 \\ & -790965k^4u^4 - 29160k^5u^3 - 36450k^5u^2 + 729k^6.\end{aligned} \tag{25}$$

On the right, we have used the abbreviation $k = 1-j$ to keep the expression relatively concise.

TABLE 5. Polynomials defining $\tilde{K}$ and its splitting field $\tilde{L}$. The polynomial $g_{120}(x) \in \mathbf{Q}[x]$ is the product of $f_{24}(x)$ and its four other conjugates in $F[x]$

$$
\begin{aligned}
7f_{24}(x) = {} & 7x^{24} \\
& -52045\pi^4x^{22} \\
& -243670\pi^3x^{22} \\
& +68355\pi^2x^{22} \\
& +1259160\pi x^{22} \\
& +928935x^{22} \\
& -3098395696\pi^4x^{20} \\
& -14645353797\pi^3x^{20} \\
& +4009956421\pi^2x^{20} \\
& +76372306067\pi x^{20} \\
& +56546420285x^{20} \\
& +2773874326655\pi^4x^{18} \\
& +13108010975190\pi^3x^{18} \\
& -3593706901525\pi^2x^{18} \\
& -68355532760945\pi x^{18} \\
& -506074908333355x^{18} \\
& +3445327389646550\pi^4x^{16} \\
& +16282532224913110\pi^3x^{16} \\
& -4461790749743685\pi^2x^{16} \\
& -849105148530245 15\pi x^{16} \\
& -62865746554585540x^{16} \\
& -649153319122415 73\pi^4x^{14} \\
& -3067884115365627 39\pi^3x^{14} \\
& +840669036982353 88\pi^2x^{14} \\
& +159984715351285 7137\pi x^{14} \\
& +1184489339956417922x^{14} \\
& +16395684334962892080\pi^4x^{12} \\
& +77485635988243413765\pi^3x^{12} \\
& -21232804266959253340\pi^2x^{12} \\
& -40407384319789846956 5\pi x^{12} \\
& -299166801483805686500x^{12} \\
& -80620840119403359737 3\pi^4x^{10} \\
& -38101227998989732120 93\pi^3x^{10} \\
& +10440592069955307023 18\pi^2x^{10} \\
& +19869114361884763910602\pi x^{10} \\
& +14710626515374478523745x^{10} \\
& +49914114653987435346555\pi^4x^8 \\
& +23589298498695331182724 0\pi^3x^8 \\
& -64639975082428982610600\pi^2x^8 \\
& -12301400616264305604891 50\pi x^8 \\
& -91076686552678190337880 0x^8 \\
& +25916844503989928321047 5\pi^4x^6 \\
& +12248242513904985126361 75\pi^3x^6 \\
& -33562934944678672950635 0\pi^2x^6 \\
& -63872411473803999975230 75\pi x^6 \\
& -47289636201848594883618 00x^6 \\
& -37470318567407566093108 0\pi^4x^4 \\
& -17703838411877422830911 40\pi^3x^4 \\
& +48524960831581141585332 5\pi^2x^4 \\
& +92346103524428594953443 50\pi x^4 \\
& +68370890335329196766566 00x^4 \\
& -40155900972025536030175\pi^4x^2 \\
& -18977588625575234117362 5\pi^3x^2 \\
& +52002854427805448365000\pi^2x^2 \\
& +98964757441503994249481 25\pi x^2 \\
& +73271186545576461890237 5x^2 \\
& -25316729772828532653 40\pi^4 \\
& -11964629639571447753400\pi^3 \\
& +32785771981100735044 75\pi^2 \\
& +62393420656294097744100\pi \\
& +46194626070054783641000
\end{aligned}
$$

$$
\begin{aligned}
g_{120}(x) = {} & x^{120} \\
& +75875x^{118} \\
& +4433249820x^{116} \\
& -49201372899625x^{114} \\
& +1388752994012323 25x^{112} \\
& -1016307308112854928 75x^{110} \\
& -2481244410863037821 96575x^{108} \\
& +3563480680137799249 2993875x^{106} \\
& +3184089744155137288 69132030700x^{104} \\
& +2521264748202114139368 29970728725x^{102} \\
& +5061589753038564871 31302139455510 20x^{100} \\
& -1547671302312365597 28901535775715 9050x^{98} \\
& -1547594397259918649082443176514981 68250x^{96} \\
& +4867821035798662923292789878435380731275x^{94} \\
& -1825744840675958747234460076428409907877000x^{92} \\
& +1833556350454921262734558471442093275701756 30x^{90} \\
& -1254541093719392365818274089643042368724683405 0x^{88} \\
& +4592613101582725772274476597325078565429822187 00x^{86} \\
& -1350008069215520575166273091783119405121344359 0350x^{84} \\
& +2239984471900934328269583806397532562105487046335 25x^{82} \\
& +8579732748368022156383811605492709480260120302317960x^{80} \\
& +1236161960862240781218201894498308969084770850475 00525x^{78} \\
& +3022556554362539911741796392500720116840988719162863550x^{76} \\
& +5299260624752744656622715292119987639535610121159476880 0x^{74} \\
& +7096740514976271283408638781136703274491901200268723907 5x^{72} \\
& -6109996456957007827028243367304714554649555705815343241 99x^{70} \\
& +6884138417860041391100099478847832963036373563732897532875x^{68} \\
& +2778249567565101440595304205079797125905561943150775565770x^{66} \\
& -3921669517788320293732131355968163731003255888538098003775 0x^{64} \\
& -7573189072073147661613369218032918011021787577693882021472 5x^{62} \\
& +2497161426468089815714964563447193787346707052460991712258 00x^{60} \\
& -2959504831911991703722842969209133187347362566442011318058 50x^{58} \\
& +2086565180547593025573935122359346565181100006086556269503 75x^{56} \\
& -7003037808658056887005760694135133337332027512460244668360 0x^{54} \\
& -8430811254921054772706888159791528649933354690181608663587 5x^{52} \\
& +9926642618922720746083119647987480044231324011742347252713 0x^{50} \\
& -1478722019240514954406629647934813611965239765931721343943 75x^{48} \\
& +6988068811100905459033405600746933783676854803470805120437 5x^{46} \\
& -9833945613688517799337910282039965659143927742952406072500x^{44} \\
& +2284941239738993839775112265389393114644048651746550609375x^{42} \\
& -2661438765488132691494838375140724457363987359711995520625x^{40} \\
& -1309200438172791546382244498663483683291550449885873150000x^{38} \\
& +3487789668535358976042160201279382631592746320670134843 75x^{36} \\
& +1786979943361501521409227759707409033301038854754390625 0x^{34} \\
& +3979122628910045305502862922166159126436358282173879687 5x^{32} \\
& +2832734472839931933240266147328146992179352403486228125x^{30} \\
& -3000021530697883715015667845051363549415692595292656250x^{28} \\
& -2644821674482262883021225956446665378854871721815625 00x^{26} \\
& +4031075217941431852314120821413607521069052026515625 0x^{24} \\
& +5829819867309054032004971974393116491059610206640625x^{22} \\
& +2799348057459198113299002320167172720042750547656 25x^{20} \\
& -4601229911030288915962388240493379793569199609375x^{18} \\
& -2126400711689549978969708393854142334173652343 75x^{16} \\
& +3452840068185293658743184347789640485082031250x^{14} \\
& +9185656210180316707958328085359926464843750x^{12} \\
& -1149103081879362395091139879854000976562 5x^{10} \\
& -4373796021206535202788567018173828125 0x^8 \\
& +2461738901861270226326789218750000x^6 \\
& +5449354415044950377676700195312 5x^4 \\
& +1338936922930656633212890625 0x^2 \\
& +1558442701125234934531 25
\end{aligned}
$$

6.2. **Specialization.** Applying this theory with j the specialization point j_2 from (23) and

$$d = -\frac{yu_1u_4}{24\omega_{7,4}^6\pi^2} \tag{26}$$

gives an even degree 24 polynomial $f_{j,d,5}(y)$ in $F[y]$ with Galois group $GL_2(5)$. Here in (26), y is the complicated quantity appearing in (22). The fact that z is a square in (22) plays an important role in d being the right choice. Also only $-u_1u_4$ is the only element out of the 32-element group of units modulo squares that works in (26). All the other choices would introduce ramification at 2.

The polynomial $f_{j,d,5}(y)$ is non-monic with large coefficients. We adjusted this polynomial in an *ad hoc* fashion to obtain a polynomial $f_{24}(x) = f_{12}(x^2)$ with considerably smaller coefficients defining the same field. The left column of Table 5 gives this better polynomial $f_{24}(x) \in F[x]$. The right column of Table 5 gives the product $g_{120}(x) = g_{60}(x^2)$ of the five conjugates of $f_{24}(x)$.

The degrees of the polynomials are large enough that not all standard operations with *Pari* are feasible. For example, a several-day computation trying to find the T_2-reduction of $g_{60}(x)$ did not reach a result. However *Pari* does succeed in computing the discriminant of $\tilde{K} = \mathbf{Q}[x]/g_{120}(x)$ to be 5^{311} in well under a second.

The Galois group of $f_{12}(x)$ is the fiber product $PGL_2(5) \times_2 4$, with the subscript 2 corresponding to the extension $F(\sqrt{5})/F$ and the second factor 4 corresponding to the extension $F(e^{2\pi i/5})/F$. The Galois groups of $g_{60}(x)$ and $g_{120}(x)$ respectively have the form $PSL_2(5).20$ and $SL_2(5)^5.20$, there being group-theoretically no other possibilities.

6.3. **Twisting and 5-adic behavior.** The field $\tilde{K} = \mathbf{Q}[x]/g_{120}(x)$ has an order four automorphism $a : \tilde{K} \to \tilde{K}$. Also the ground field $\mathbf{Q}$ has a unique extension with Galois group C_4 ramified at 5 only, namely the standard cyclotomic field $\mathbf{Q}(e^{2\pi i/5})$. This is a standard set-up for twisting. One gets that the field $\tilde{K} = \mathbf{Q}[x]/g_{120}(x)$ is one of four similar fields as follows.

For $i = 0, 1, 2, 3$, the map $t_i : GL_2(5) \to GL_2(5)$ given by $t_i(g) = \det(g)^i g$ is an automorphism. As a special case of the definition one has

$$t_i \begin{pmatrix} a & b \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} a^{i+1} & a^i b \\ 0 & a^i \end{pmatrix}. \tag{27}$$

Let D_i be the group of matrices of the form on the right of (27), with $a \in \mathbf{F}_5^\times$ and $b \in \mathbf{F}_5$. The orbit sizes of D_i on the four column vectors of the form $\begin{pmatrix} * \\ 0 \end{pmatrix}$ are given in the column λ_4 of Table 6. Similarly the orbit sizes of D_i on the remaining twenty column vectors are given in

TABLE 6. 5-adic behavior in the four fields $\tilde{K}_i$.

	λ_{24}		λ_{120}		
i	λ_{20}	λ_4	λ_{100}	λ_{20}	c
0	$5,5,5,5$	4	$25_{69}, 25_{69}, 25_{69}, 25_{69}$	20_{35}	311
1	20	$2,2$	100_{279}	$10_{17}, 10_{17}$	313
2	$10,10$	4	$50_{139}, 50_{139}$	20_{35}	313
3	20	$1,1,1,1$	100_{279}	$5_8, 5_8, 5_8, 5_8$	311

the column λ_{20} on the left. The partitions in the two columns under λ_{120} are obtained from the partitions in the two columns under λ_{24} by multiplying all parts by 5.

The i^{th} row corresponds to a field $\tilde{K}_i$, with D_i identified with the π-decomposition group. Our field $\tilde{K}$ is the field $\tilde{K}_0$, because $\tilde{K}$ factors 5-adically into four fields of degree 25 and one field of degree 20. As indicated by the subscripts, the four fields of degree 25 all have

discriminant 5^{69}, while the one field of degree 20 has discriminant 5^{35}. All together the sum of the subscripts is 311, so that the the discriminant of $\tilde{K}_0$ itself is 5^{311}. Table 6 describes the 5-adic behavior of each of the four fields in this way.

The field $\tilde{K}_2$ is a quadratic twist of $\tilde{K}_0$ and has $g_{60}(5x^2)$ as defining polynomial. The fields $\tilde{K}_1$ and $\tilde{K}_3$ are likewise quadratic twists of each other. However to obtain say $\tilde{K}_1$ from $\tilde{K}_0$ one has to use an explicit expression for the order four automorphism a. We do not enter into this complication here, as our main focus is on the common splitting field $\tilde{L}$ of the four $\tilde{K}_i$.

7. Frobenius Computations

In this section, we work mainly over the quintic field F, rather than over $\mathbf{Q}$. The focus is on $f_5(x)$, $f_6(x)$, $f_{12}(x)$, and $f_{24}(x) \in F[x]$ from (8), (10), Table 5, and Table 5 respectively. The corresponding Galois groups are respectively

$$S_5 \;\cong\; PGL_2(5) \leftarrow GL_2(5)/\{\pm 1\} \leftarrow GL_2(5). \tag{28}$$

Here the two covering maps indicated by arrows each have degree two. We consider the three groups G in turn, and discuss computing Frobenius elements in the correspond set $G^\natural$ of conjugacy classes. These sets have 7, 14, and 24 elements respectively. The calculations of this section are designed to be compared with Table 3.9 of [7] and we make the comparison in the last two subsections.

7.1. **Frobenius elements at the projective level.** To begin as naively as possible, we first work over $\mathbf{Q}$. For each prime $p \neq 5$, the degrees of the irreducible factors of $g_{25}(x)$ over the p-adic integers $\mathbf{Z}_p$ give a partition Λ_p of 25. To describe the possibilities for Λ_p, note first that there are seven partitions of 5, namely the elements of $S_5^\natural = \{5,\ 311,\ 221,\ 11111,\ 41,\ 32,\ 2111\}$. The four partitions listed first are even, meaning that they are realized as cycle partitions of elements of A_5. The three partitions listed last are odd, hence realized as cycle partitions of elements of $S_5 - A_5$.

Suppose first that p is inert. Then all parts of Λ_p are multiples of 5. If $p \equiv 1, 4$ modulo 5 then the possibilities for Λ_p are 5(5), 5(311), 5(221), and 5(11111). If $p \equiv 2, 3$ modulo 5 then the possibilities are 5(41), 5(32), and 5(2111).

Table 7. Frobenius data for the extensions K/F and $\tilde{K}/F$ and small primes p.

Split Primes												Other Primes		
p	$r_{p,1}$	$r_{p,2}$	$r_{p,3}$	$r_{p,4}$	$r_{p,5}$	$[p]$	$\lambda_{p,1}$	$\lambda_{p,2}$	$\lambda_{p,3}$	$\lambda_{p,4}$	$\lambda_{p,5}$	p	$[p]$	λ_p
∞	−3.5	−0.3	2.3	−2.6	−0.9	1	221	221	221	221	221	2	2	$41B$
7	26	32	3	31	1	2	221	32	32	221	$41B$	3	3	2111
43	2	6	23	18	32	3	$41B$	$41B$	$41B$	32	32	5	–	–
101	23	96	35	82	62	1	221	$311B$	$5B$	221	$311B$	11	1	221
107	17	20	79	39	54	2	$41A$	32	$41B$	$41A$	$41B$	13	3	32
149	15	90	103	99	135	4	5	311	5	5	221	17	2	2111
151	14	37	85	102	59	1	$5A$	$311A$	221	$5B$	221	19	4	5
157	5	87	113	51	53	2	2111	32	$41A$	32	$41A$	23	2	32
193	15	167	95	163	134	3	$41A$	32	32	$41B$	2111	29	4	5
199	26	137	154	117	158	4	5	221	5	5	5	31	1	$5B$

TABLE 8. Different viewpoints on the 24-element set of conjugacy classes in $GL_2(5)$.

#	λ_5	λ_6	λ_{12}	det	L	min poly	λ_{24}	L	min poly	λ_{24}
1	1^5	1^6	1^{12}	1	A	$(x-1)$	1^{24}	B	$(x-4)$	2^{12}
			2^6	4	$+$	$(x-3)$	4^6	$-$	$(x-2)$	4^6
15	221	2211	2^6	1		$(x-3)(x-2)$	4^6			
			$2^4 1^4$	4		$(x-4)(x-1)$	$2^{10}1^4$			
20	311	33	3^4	1	A	x^2-4x+1	3^8	B	x^2-x+1	6^4
			6^2	4	$+$	x^2-2x+4	12^2	$-$	x^2-3x+4	12^2
24	5	51	$5^2 1^2$	1	A	$(x-1)^2$	$5^4 1^4$	B	$(x-4)^2$	$10^2 2^2$
			$10^1 2^1$	4	$+$	$(x-3)^2$	$20^1 4^1$	$-$	$(x-2)^2$	$20^1 4^1$
10	2111	222	4^3	2		x^2+2	8^3			
			4^3	3		x^2+3	8^3			
30	41	411	$4^2 2^1 1^2$	2	A	$(x-2)(x-1)$	$4^5 1^4$	B	$(x-4)(x-3)$	$4^5 2^2$
			$4^2 2^1 1^2$	3	A	$(x-3)(x-1)$	$4^5 1^4$	B	$(x-4)(x-2)$	$4^5 2^2$
20	32	6	12	2	$+$	x^2-x+2	24	$-$	x^2-4x+2	24
			12	3	$+$	x^2-2x+3	24	$-$	x^2-3x+3	24

Now suppose that p is split. The invariant Λ_p can be refined into five partitions of five. Making use of the notations set up in §3.3, one gets one partition $\lambda_{p,i}$ for each of the ideals $\Pi_{p,i}$ above p. For $p > 7$, one computes $\lambda_{p,i}$ by first reducing $f_5(x)$ in (8) to a quintic in $\mathbf{F}_p[x]$ by sending π to the residue class $r_{p,i} \in \mathbf{F}_p$; then one factors the reduced polynomial and $\lambda_{p,i}$ is the partition giving the degrees of the factors. This refinement is exactly what is meant in the split case by "working over F." In the inert case, working over F is just a change in viewpoint: one divides all parts of the above partitions Λ_p by 5 to get λ_p. Thus Frobenius elements Fr_Π lie in $S_5^\natural$ for both split and inert primes.

Table 7 presents Frobenius data for the field K and small primes p. It gives analogous information for $p = \infty$ for the sake of comparison. Thus $r_{\infty,1}$ is an approximation to the least root of the polynomial in (1) and the other $r_{\infty,i}$ are obtained by successively applying σ. As always $p = 7$ needs some modification: one factors over $\mathbf{Z}_7$ rather than $\mathbf{F}_7$, and $r_{7,i}$ is the image of π in $R/\Pi_{7,i}^2 = \mathbf{Z}/49$.

7.2. **Frobenius information at the intermediate level.** To move past the projective level, it is best to first restate the projective level using the sextic polynomial (10) rather than the quintic polynomial (8). Just as each Fr_Π is completely determined by a partition in $S_5^\natural$ which we now call $\lambda_{5,\Pi}$, so too each Fr_Π is completely determined by a partition of six $\lambda_{6,\Pi}$. The bijection between all partitions of five and the relevant partitions of six is given in Table 8.

The intermediate level does not present new calculational challenges. The class of a Frobenius element Fr_Π is given by the pair $(\lambda_{6,\Pi}, [p])$ with $[p] \in \mathbf{F}_p^\times$ the class of p modulo 5. As indicated by Table 8, one has $[p] \in \{1,4\}$ if $\lambda_{6,\Pi}$ is even and $[p] \in \{2,3\}$ if $\lambda_{6,\Pi}$ is odd. Table 8 also gives the possibilities for $\lambda_{12,\Pi}$, obtained by factoring $f_{12}(x)$ modulo Π. Note that in the even case $p \equiv 1, 4\ (5)$, the partition $\lambda_{12,\Pi}$ does not fully capture Fr_Π, as one has the ambiguity of 2^6 appearing in two places. In the odd case, $\lambda_{12,\Pi}$ alone is even weaker, as it gives just the information contained in $\lambda_{5,\Pi}$ or $\lambda_{6,\Pi}$.

7.3. **Frobenius information at the linear level.** Frobenius information at the linear level is much more subtle. Conjugacy classes in $GL_2(5)$ are indexed by minimal polynomials of matrices. Thus a scalar class $\begin{pmatrix} a & 0 \\ 0 & a \end{pmatrix}$ is indexed by the linear polynomial $x-a$. Non-scalar classes are indexed by polynomials $x^2 - tx + d$ with t being the trace of the matrix and d the determinant.

Table 8 indicates the map $GL_2(5)^\natural \to (GL_2(5)/\{\pm 1\})^\natural$. Four classes in $(GL_2(5)/\{\pm 1\})^\natural$ have only one preimage. Five classes have two preimages labeled by A and B. Five more classes have two preimages labeled by $+$ and $-$. The classes labeled by A and B are distinguished from each other by factoring $f_{24}(x)$ as indicated by the table; notation is chosen so that λ_{24} has more parts in Class A then it does in Class B. The classes labeled by $+$ have trace in $\{1, 2\}$ while the classes labeled by $-$ have trace in $\{-2, -1\}$. They are not distinguished by factoring $f_{24}(x)$. One could make use of the order four automorphism a of $\tilde{K}/F$ to distinguish $+$ from $-$ in all but the last two cases, by computing fixed points of $a^i\phi^j$ in positive characteristic, with ϕ the Frobenius operator; however we have not pursued our computations to this level of refinement.

Note that the Frobenius elements considered in this section are all calculated with reference to $\tilde{K}$. If we replaced $\tilde{K} = \tilde{K}_0$ by another one of the $\tilde{K}_i$ from §6.3, then Frobenius elements would change accordingly. For example, suppose we replaced $\tilde{K}$ with its quadratic twist $\tilde{K}_2$; then characteristic polynomials $x^2 - tx + d$ would change to $x^2 + tx + d$ for all Π with $p \equiv 2, 3\ (5)$. The only part of this switch visible to our calculations occurs for primes Π with $\lambda_{5,\Pi} = 41$. In this case, Π contributes $4^5 1^4$ to the factorization pattern of one of $g_{60}(x^2)$ and $g_{60}(5x^2)$, and $4^5 2^2$ to the factorization of the other.

7.4. **Matching Hecke eigenvalues.** Table 3.9 of [7] presents Hecke eigenvalues in $GL_2(5)^{20}$. Here $GL_2(5)^{20}$ is the twenty-element quotient of $GL_2(5)^\natural$ where one no longer distinguishes between the scalar class with minimal polynomial $(x-a)$ and the nonscalar class with minimal polynomial $(x-a)^2$. Our Frobenius computations see the nineteen-element quotient $GL_2(5)^{19}$ where the five ambiguities associated to $+$ versus $-$ have not been resolved.

Table 3.9 of [7] and our Table 7 agree where there is overlap, as they must since our fields coincide with those of [7]. The two computations together let one in principle see Frobenius elements where they live, meaning $GL_2(5)^\natural$. In practice, however, Hecke eigenvalue computations can only be done for Π of quite small residual cardinality. Instead one can count points on the elliptic curve (23), (24), (26) and use $f_{24}(x)$ to resolve the scalar/nonscalar ambiguity. This alternative method also lets one see Frobenius elements in $GL_2(5)^\natural$.

7.5. **Use of Frobenius elements in finding polynomials.** In principle, we could have used the Frobenius information in Table 3.9 of [7] to target our search for a numerically matching polynomial. Indeed, it would have been easy to simultaneously impose the behavior at say 2 and 3, to cut down search times by a factor of about five. However there does not seem to be a practical way to use Frobenius information at many primes simultaneously to find the desired specialization point. The method [10] used by Bosman to find the polynomials in [3] presents a sharp contrast: it does not involve specializing families at all and does make use of Hecke eigenvalues through Fourier expansions of modular forms.

8. Totally Ramified Binomial-over-Abelian p-adic Fields of Degree p^2

This section describes the class of p-adic fields given in the section title, as made precise in (29) below. The main statement, Theorem 8.1, immediately applies to our main Galois field L and a solvable analog L^s to give Corollary 9.1 of the next section.

Our framework in this section is similar to the framework of [14], as follows. For each prime p, fix an algebraic closure $\overline{\mathbf{Q}}_p$ of the field of p-adic numbers $\mathbf{Q}_p$. Given an irreducible polynomial $g(x) \in \mathbf{Q}_p[x]$, one has its root field $K = \mathbf{Q}_p[x]/g(x)$ and its splitting field $L \subset \overline{\mathbf{Q}}_p$. So one views K as an abstract field and L as an embedded field, with in fact L being the composita of all the embeddings of K into $\overline{\mathbf{Q}}_p$. We are interested in classifying fields K up to isomorphism and for each K describing the Galois group $\mathrm{Gal}(L/\mathbf{Q}_p)$ and its filtration by ramification subgroups. One of the principles of [14] is that standard invariants of K often need to be supplemented substantially before one gets the desired description of L. The class of p-adic fields here is well-behaved in that the passage from a description of K to one of L is unusually straightforward, as will be clear from Theorem 8.1.

With weaker hypotheses one could get statements similar to Theorem 8.1 with more complicated conclusions. We isolate Theorem 8.1 because it is just enough to obtain Corollary 9.1 with no extra work. In particular, one of our several simplifying hypotheses is that p is odd.

8.1. **Some Kummer theory.** Given now an odd prime p, our class of p-adic fields consists of those fields of the form

$$K = F[x]/(x^p - a) \tag{29}$$

with F a totally ramified degree p cyclic extension of $\mathbf{Q}_p$ and $a \in F^\times - F^{\times p}$. It is simple to establish that there are p possible isomorphism classes for F, and they all have discriminant $p^{2(p-1)}$. In fact, for i in $\mathbf{Z}_p$ write

$$f_i(\pi) = \pi^p - p\pi^{p-1} + (p + ip^2). \tag{30}$$

Then the isomorphism class of $F_i = \mathbf{Q}_p[\pi]/f_i(\pi)$ depends only on $i \in \mathbf{F}_p$ and these classes represent all possibilities. As a generator for $\mathrm{Gal}(F_i/\mathbf{Q}_p)$, we take the automorphism satisfying $\sigma(\pi) \equiv \pi + \pi^2 \pmod{\pi^3}$. Then $\sigma^j(\pi) \equiv \pi + j\pi^2 \pmod{\pi^3}$.

Fix now an F as above and consider the set of all possible isomorphism classes for K. Here, for the moment, we are requiring that isomorphisms from K_1 to K_2 fix F. The elementary parts of Kummer theory say that, up to F-isomorphism, K in (29) depends exactly on the subgroup generated by a in the quotient group $F^\times/F^{\times p}$.

8.2. **Generators.** To go further, it is convenient to have an explicit description of $F^\times/F^{\times p}$. To begin, we use some structure which is present for arbitrary ground fields Q of characteristic different from p, not just $Q = \mathbf{Q}_p$. Let σ be a generator of the p-element group $\mathrm{Gal}(F/Q)$. Then the field automorphism $f \mapsto f^\sigma$ of F descends to a group automorphism of $F^\times/F^{\times p}$. In fact, consider the group ring $\mathbf{F}_p[\mathrm{Gal}(F/Q)] = \mathbf{F}_p[\sigma]/(\sigma^p - 1)$. Any element of this group ring induces a group endomorphism of $F^\times/F^{\times p}$. As before, we will use exponential notation, as in $f^{\sigma-1} = f^\sigma/f$.

Now we will use facts particular to our ground field $Q = \mathbf{Q}_p$. In general, suppose F is any degree m field extension of $\mathbf{Q}_p$. Then $F^\times/F^{\times p}$ has rank $m+2$ or $m+1$ according to whether F contains a primitive p^{th} root of unity or not. We are in the latter case with $m = p$, so a minimal generating set of $F^\times/F^{\times p}$ has $p+1$ elements.

To be maximally explicit, we choose a uniformizer π of F. For example, π in F_i from (30) works, although we will be working with other choices in the next section. Rather than emphasize the element $\sigma \in \mathbf{F}_p[\mathrm{Gal}(F/\mathbf{Q})]$, we focus on $q = \sigma - 1$ so that $\mathbf{F}_p[\mathrm{Gal}(F/\mathbf{Q})] = \mathbf{F}_p[q]/q^p$. Define $p+1$ elements $a_j \in F^\times/F^{\times p}$ by

$$a_j = \begin{cases} \pi^{q^j} & \text{if } j \in \{0, \dots, p-1\}, \\ 1+p & \text{if } j = p. \end{cases} \tag{31}$$

The a_j form a generating set, so that any class in $F^\times/F^{\times p}$ can be represented by an element

$$a = \pi^{m(q)}(1+p)^w$$

for a unique pair $(m(q), w)$ with $m(q) \in \mathbf{F}_p[q]/q^p$ and $w \in \mathbf{F}_p = \mathbf{F}_p[q]/q$. We write

$$K_{m(q),w} = F[x]/(x - \pi^{m(q)}(1+p)^w). \tag{32}$$

The a_j sit nicely with respect to the unit filtration of $F^\times/F^{\times p}$ as follows. Let R be the ring of integers of F and $\Pi = (\pi)$ the maximal ideal, so that the residue field R/Π is identified with $\mathbf{F}_p$. Let $U = U^0$ be the group of units and for $j \geq 1$ let $U^j = 1 + \Pi^j$ be the group of j-units. Then the quotient group U^0/U^1 is $\mathbf{F}_p^\times$ while the higher quotients U^j/U^{j+1} are naturally rank one modules over $\mathbf{F}_p$, in fact canonically isomorphic to Π^j/Π^{j+1}. Let V^j be the image of U^j in $V^{-1} = F^\times/F^{\times p}$. One can check that V^0 has index p in V^{-1} with $a_0 = \pi$ generating V^{-1}/V^0. One has $V^0 = V^1$ but for $j \in \{1, \ldots, p\}$ one has that V^j/V^{j+1} has p elements with generator a_j.

8.3. **Ramification.** The unit filtration is exactly what is needed to identify discriminants. Let $\delta_0 = 0$ and $\delta_\ell = 1$ for $\ell \geq 1$. Then one has

$$\mathrm{disc}(K_{m(q),w}/\mathbf{Q}_p) = p^{2(p-1)p + (p-1)(\ell+\delta_\ell)} \tag{33}$$

where $m(q)$ vanishes to order $p - \ell$ at 0.

To go further, we bring in the formalism of slopes, using the conventions of [14]. Thus 0 corresponds to no ramification, 1 to tame ramification, and slopes > 1 to wild ramification, this being a shift upwards by 1 from the upper numbering system of [22]. One part of the formalism says that a degree p^2 totally ramified extension K of $\mathbf{Q}_p$ has two wild slopes $s_a \leq s_b$. The case of concern here is the case where K contains subfields of degree p. Let K_1 be the subfield of degree p with smallest discriminant. Then s_a is calculated by $\mathrm{disc}(K_1/\mathbf{Q}_p) = p^{s_a(p-1)}$. The larger slope s_b is calculated by requiring $\mathrm{disc}(K/\mathbf{Q}_p) = p^c$ with

$$\frac{c}{p^2} = \frac{p-1}{p} s_b + \frac{p-1}{p^2} s_a. \tag{34}$$

Similarly, suppose L is a totally ramified field with degree $p^{\ell+1}t$ with t not divisible by p. Then L has the tame slope 1 and wild slopes $s_0 \leq \cdots \leq s_\ell$, likewise calculated via discriminants of distinguished (minimally ramified) subfields [14]. One has $\mathrm{disc}(L/\mathbf{Q}_p) = p^c$ with

$$\frac{c}{p^{\ell+1}t} = \frac{1}{p^{\ell+1}} \frac{t-1}{t} + \sum_{j=0}^{\ell} \frac{p-1}{p^{\ell+1-j}} s_j. \tag{35}$$

In general, the mean slope c/N of a degree N field is a weighted average of all the slopes appearing, with larger slopes being weighted more. A feature of the formalism of slopes is that it facilitates the transfer of information from one field to another. For example, suppose K has splitting field L. Then the slopes of K are all also slopes of L.

8.4. **Level and type.** Say a non-zero index $(m(q), w)$ has *level* $\ell \in \{0, \ldots, p\}$ if $m(q)$ vanishes to order $p - \ell$ at 0. If $(m(q), w)$ has level $\ell > 0$ with $m(q) = b_{p-\ell}q^{p-\ell} + \cdots$ say it has *type* $w/b_{p-\ell} \in \mathbf{F}_p$.

The indices of level 0, namely $(0, w)$ for $w \in \mathbf{F}_p^\times$, play a special role as follows. The associated fields $K_{0,w}$ are all isomorphic, in fact to $F \otimes \mathbf{Q}_p[x]/(x^p - (1+p))$. The wild slopes of $K_{0,w}$ are $s_a = 1 + \frac{1}{p-1}$, from the second factor $\mathbf{Q}_p[x]/(x^p - (1+p))$, and $s_b = 2$, coming from the first factor F. The splitting field $L_{0,w}$ has degree $(p-1)p^2$ and mean slope $2 + 1/(p-1) - 2/p^2$.

The indices of level 1 are also somewhat special. Analogously with (30), put

$$h_k(x) = x^p + (p + kp^2) \tag{36}$$

and put $M_k = \mathbf{Q}_p[x]/h_k(x)$. Then $F \otimes M_k$ is a field in our class, of level 1. In fact, if $F = F_i$ and π and σ are defined as in §8.1, then $F \otimes M_k$ is the field $K_{q^{p-1},k-j}$. Our explicit descriptions show that fields $K_{m(q),w}$ of level 0 or 1 have two degree p subfields. Fields $K_{m(q),w}$ of level > 1 have only one degree p subfield, namely F.

8.5. **Summarizing theorem.** The following theorem describes ramification in our class of fields K and their splitting fields L.

Theorem 8.1. *Fix $F/\mathbf{Q}_p$ a totally ramified degree p abelian extension. Fix also a generator $\sigma \in \mathrm{Gal}(F/\mathbf{Q}_p)$ and a uniformizer π so that the fields $K_{m(q),w}$ and $L_{m(q),w}$ as well as the notions of level and type are well-defined. Then degree p binomial extensions K of F are classified up to F-isomorphism by the p-dimensional projective space*

$$P = \left((\mathbf{F}_p[q]/q^p \oplus \mathbf{F}_p[q]/q) - \{0\}\right)/\mathbf{F}_p^\times. \tag{37}$$

The same fields are classified up to $\mathbf{Q}_p$-isomorphism by the orbits of σ on P. The fixed points of σ are exactly the p points of level 1 and the 1 point of level 0, implying that there are $p^{p-1} + \cdots + p^2 + 2p + 1$ different $\mathbf{Q}_p$-isomorphism classes.

For indices $(m(q), w)$ of level $\ell \in \{1, \ldots, p\}$, ramification is as follows:

- **A::** *The slopes of $K_{m(q),w}$ are $s_0 = 2$ and $s_\ell = 2 + \frac{1}{(p-1)p} + \frac{\ell}{p}$.*
- **B::** *Let $(m_1(q), w_1)$ have the same level as $(m(q), w)$. If their types $t, t_1 \in \mathbf{F}_p$ coincide then so do the corresponding splitting fields: $L_{\ell,t} := L_{m(q),w} = L_{m_1(q),w_1}$. If their types are different than $L_{\ell,t}$ and L_{ℓ,t_1} are disjoint degree p extensions of their intersection $L_{\ell-1,0}$.*
- **C::** *The tower of distinguished subfields of $L_{\ell,t}$ is*

$$\mathbf{Q}_p \overset{1}{\subset} \mathbf{Q}_p(\mu_p) \overset{2}{\subset} L_{0,0} \overset{s_1}{\subset} L_{1,0} \overset{s_2}{\subset} \cdots \overset{s_{\ell-1}}{\subset} L_{\ell-1,0} \overset{s_\ell}{\subset} L_{\ell,t}$$

The slope associated to each step is indicated. The mean slope (35) of $L_{\ell,t}$ is $2 + \frac{\ell}{p} - \frac{1}{(p-1)p^\ell}$.

Thus for K in this class of fields containing F, the discriminant-exponent c of K determines the degree and all the slopes of L. Up to a p-fold ambiguity, the single number c determines L itself. Theorem 8.1 can be seen very explicitly in the next subsection for $p = 3$. For $p = 5$ it can be seen more briefly in Table 10 of the next section.

8.6. **The case $p = 3$.** It is clarifying to compare Theorem 8.1 for the case $p = 3$ with the explicit classification of nonic 3-adic fields in [16]. Table 9 summarizes this comparison, which is somewhat subtle. The block of four columns on the top of this table repeats five lines of Table 5.1-2 in [16]. The lines correspond to the possible levels 3, 2, 1, and 0, except that there is an extra line 2^t. This extra line corresponds to a twinning phenomenon described in [16]: the Galois closure $L_{m(q),w}$ of the nonic field $K_{m(q),w}$ is also the Galois closure of a second nonic field $K^t_{m(q),w}$.

On a given line in the top block of Table 9, the number in the $\mathbf{Q}_3$ column gives the number of nonic 3-adic fields K with wild slopes the numbers printed in bold, such that $\mathrm{Gal}(L/\mathbf{Q}_p)$ has the given Galois group with the given wild slopes. The last number in the $\mathbf{Q}_3$ column is starred to indicated that only three of these six fields in [16] are binomial-over-abelian; the other three are nonbinomial-over-abelian.

TABLE 9. Nonic 3-adic fields illustrating Theorem 8.1

level	c	Gal($L/\mathbf{Q}_p$)	wild slopes	# of $K/\mathbf{Q}_3$'s	# of K/F's	# of K/F's by type: -1	0	1
3	23	$9T22$	$\mathbf{2}, 2.5, 2.8\overline{3}, \mathbf{3.1\overline{6}}$	27	81	27	27	27
						$\searrow$	$\downarrow$	$\swarrow$
2	21	$9T13$	$\mathbf{2}, 2.5, \mathbf{2.8\overline{3}}$	9	27	9	9	9
2^t	22	$9T11$	$2, \mathbf{2.5}, \mathbf{2.8\overline{3}}$	9		$\searrow$	$\downarrow$	$\swarrow$
1	19	$9T4$	$\mathbf{2}, \mathbf{2.5}$	9	9	3	3	3
0	15	$9T4$	$\mathbf{1.5}, \mathbf{2}$	^{*6}	3		(3)	

level	c	Gal($L/\mathbf{Q}_p$)	Fields
3	23	$9T22$	$K_{i;1+cq^2;w} = \mathbf{Q}_3[x]/(x^9 + (3+9w)x^6 + 2cx^3 + (3+9i))$
2	21	$9T13$	$K_{i;q;w} = \mathbf{Q}_3[x]/(x^9 + (6-9i-9w)x^6 + 9x^4 + (3+9i))$
2^t	22	$9T11$	$K^t_{i;q;w} = \mathbf{Q}_3[x]/(x^9 - (9w+9)x^6 - 9x^5 + (3+9i))$
1	19	$9T4$	$K_{i;1;w} = \mathbf{Q}_3[x]/(x^9 + 3x^6 - (9w+9)x^4 + 9x^2 - (3+9i))$
0	15	$9T4$	$K_{i;0;1} = \mathbf{Q}_3[x]/(x^9 + 6x^8 + 6x^7 + 3x^3 + (3+9i))$

The columns "# of $K/\mathbf{Q}_3$'s" and "# of K/F's" count $\mathbf{Q}_3$- and F-isomorphism classes of fields K respectively. In these counts, F is allowed to vary over all three possibilities. The columns contain multiples of 3 only, corresponding to the fact that the three F's contribute equally to all entries. The inflations $9 \to 27$ and $27 \to 81$ in the first two rows correspond to the fact that σ acting freely at levels ≥ 2, while it acts with fixed points only in levels 0 and 1. The information in "# of K/F's by type" refines the previous column, sorting F-isomorphism classes by type. The downward arrows indicate the behavior of the nilpotent operator q; it is visually clear that type 0 plays a special role, at least for levels $< p$. The parentheses in the bottom row indicate that fields of level 0 should be regarded as having type ∞, not 0.

The lower block in Table 9 classifies field K over $\mathbf{Q}_3$. For cubic fields F it takes F_i as in (30), and uses also the uniformizer π and generator σ given there. It incorporates the choice of F explicitly into the notation, so that $K_{i;m(q);w}$ means what was previously denoted $K_{m(q);w}$. In general, at the level of $\mathbf{Q}_p$-isomorphism classes, one has $K_{i;m(q);w} \cong K_{i,(1+q)m(q);w}$ because $\sigma = 1+q$. This identity, together with projective equivalence $K_{i;m(q);w} \cong K_{i,sm(q),sw}$, means that every $\mathbf{Q}_p$-isomorphism class appears exactly once if we restrict attention to $m(q) \in \mathbf{F}_p[q]/q^p$ of the form $q^{p-\ell} + cq^{p-\ell+2} + \cdots$. Table 9 then presents an Eisenstein polynomial for each field $K_{i;m(q);w}$ in a uniform way. Here i, w and c on the left are in $\mathbf{F}_3$; arbitrary representatives in $\mathbf{Z}_3$ can be taken on the right. The polynomials here sometimes agree with those in the database associated to [14], but usually do not. Nonetheless the database assisted essentially in obtaining the Eisenstein polynomials in Table 9.

9. Ramification in L and other Number Fields Ramified at One Prime

In this section, we apply Theorem 8.1 to obtain ramification information for L and a natural sequence of solvable fields ramified at one prime only. Corollary 9.1 summarizes the results obtained in the case $p = 5$.

9.1. **Application to L.** Every degree p extension K/F of p-adic fields with the largest possible relative discriminant is given by a binomial [1]. In our case, the polynomial $f_5(x)$ in (8) is not a binomial and to apply the theory of the previous section, we need to replace $f_5(x)$ by a binomial.

Let $\phi_5(x) = x^5 - \pi\omega_{7307,3}$ be the polynomial obtained from $f_5(x)$ in (8) by simply dropping the intermediate terms $\alpha x^2 - \alpha x$. Since α is divisible by π^6, one might suspect that the 5-adic completions of $F[x]/f_5(x)$ and $F[x]/\phi_5(x)$ are isomorphic. However this is not at all the case; one needs the intermediate terms to be considerably smaller before one can simply drop them.

To find a suitable binomial we proceed methodically as follows. Without changing notation, we work 5-adically with $K = F[v]/f_5(v)$. The element v, previously called x, is a uniformizer of K. The general uniformizer has the form $u = \pi c_0 + c_1 v + c_2 v^2 + c_3 v^3 + c_4 v^4$ with all c_i in the ring of integers R and c_1 invertible. Consider the characteristic polynomial $f_u(x) \in R[x]$. We work step-by-step, imposing congruence conditions on the interior coefficients of the undetermined quintic polynomial $f_u(x)$. For example, the coefficient a_4 of x^4 is determined by

$$\begin{aligned} 7a_4 &= 5\left(-9c_3\pi^4 + 12c_4\pi^4 + 57c_3\pi^2 - 76c_4\pi^2 - 7c_0\pi + 186c_3\pi - 248c_4\pi\right) \\ &\quad +5^2\left(-6c_3\pi^3 + 8c_4\pi^3 - 3c_3 + 4c_4\right). \end{aligned}$$

No matter what the c_i are, the π-adic valuation of a_4 is at least six. The three terms with valuation six are collected on the right in reduced form:

$$7a_4 \equiv 5\pi(3c_0 + c_3 + 2c_4) \pmod{\pi^7}.$$

We change variables, replacing c_3 by c_3' via

$$c_3 = -3c_0 - 2c_4 + \pi c_3'.$$

We continue in this way, always solving linear equations over $\mathbf{F}_5$, and correspondingly replacing one variable $c_i^{(k)}$ with a new variable $c_i^{(k+1)}$. We never change c_1, to ensure that the constant coefficient a_0 keeps its original π-valuation of 1. After thirteen steps we specialize the five remaining variables to 1. The intermediate coefficients all have π-valuation nine. Expecting this suffices, we drop them. We identify the constant term as $\pi^{1+q-q^2-q^3}6^{-1}$ in $F^\times/F^{\times 5}$, in the notation of the previous section.

As a final step, we compute a defining polynomial for the degree 125 algebra $K \otimes_F K_{1+q-q^2-q^3;-1}$. Its irreducible factors over $\mathbf{Q}_5$ have degrees 25 and 100. This factorization confirms that indeed K and $K_{1+q-q^2-q^3;-1}$ are 5-adically isomorphic. In contrast, $K \otimes_F K_{m(q);w}$ is a field for all $(m(q), w)$ not of the form $s(1+q-q^2-q^3, -1)$ for $s \in \mathbf{F}_5^\times$.

9.2. **Applications to solvable fields.** Let p be an odd prime number. The unique degree p subfield F of $\mathbf{Q}(e^{2\pi i/p^2})$ then represents the unique isomorphism class of degree p abelian extensions of $\mathbf{Q}$ ramified at p only. Let Π be the unique prime ideal above p in the ring of integers R. Let j be the smallest positive integer such that Π^j is principal. For all p for which calculations have been done [4], j is not divisible by p. Vandiver's conjecture implies that j is in fact never divisible by p [31, Corollary 10.6]. Assuming this is the case for our given p, let π be a generator of Π^j.

Under these conditions one can repeat many of the considerations of the previous section. In particular (31) still makes sense, with the a_j now lying in the number ring R. The element $a_0 = \pi$ is a p-unit and $a_1, \ldots, a_{p-1}$ are all units. On the other hand $a_p = 1 + p$ is not a p-unit.

The polynomials $x^p - \pi^{m(q)}(1+p)^w$ are now in $R[x]$ and their norms $g_{m(q),w}(x)$ are in $\mathbf{Z}[x]$. One thus has number fields $K_{m(q);w} = F[x]/(x^p - \pi^{m(p)}(1+p)^w) = \mathbf{Q}[x]/g_{m(q),w}(x)$ and their

splitting fields $L_{m(q);w} \subset \mathbf{C}$. We restrict attention to the case $w = 0$ so that the number fields are ramified at p only, and suppress $w = 0$ from the notation. As extensions of F, the set of fields $K_{m(q)}$ forms a projective space of dimension $p-1$ over $\mathbf{F}_p$. The automorphism σ acts with a single fixed point, so as extensions of $\mathbf{Q}$ the $K_{m(q)}$ define $p^{p-2} + \cdots + p + 2$ different isomorphism classes of number fields.

Let L^s be the joint splitting field of all the $K_{m(q)}$ in $\mathbf{C}$. The Galois group $\mathrm{Gal}(L^s/\mathbf{Q})$ coincides with its p-decomposition group, which in turn coincides with the p-inertia group. These groups all have the structure $p^p.p.(p-1)$.

Table 6.2 of [16] includes all five nonic fields appearing in the case $p = 3$. Table 10 presents five of the 157 fields appearing in the case $p = 5$. Here the discriminant of $K_{q^{5-\ell}}$ is 5^c and the

TABLE 10. Five polynomial defining Galois subfields L^s_ℓ of L^s for $p = 5$. The degree of $L^s_\ell/\mathbf{Q}_5$ is $5^{\ell+1}4$.

ℓ	Defining polynomial for $K_{q^{5-\ell}}$	c	s_ℓ	GMS	GRD	T_2
5	$x^{25} + 5x^{20} - 25x^{10} - 25x^5 - 5$	69	3.05	2.99992	124.98	30.25
4	$x^{25} + 5x^{20} - 30x^{15} - 25x^{10} + 15x^5 - 1$	65	2.85	2.7996	90.54	30.63
3	$x^{25} - 30x^{20} - 65x^{15} + 640x^{10} - 720x^5 - 1$	61	2.65	2.598	65.45	43.53
2	$x^{25} - 45x^{20} + 235x^{15} - 390x^{10} + 205x^5 + 1$	57	2.45	2.39	46.83	41.30
1	$x^{25} - 120x^{20} + 885x^{15} + 28385x^{10} - 3245x^5 + 1$	53	2.25	2.15	31.83	65.66

top 5-adic slope is given in the column s_ℓ. The Galois mean slope $\alpha \in \mathbf{Q}$, meaning the mean slope of $L_{q^{5-\ell}}$, is given exactly in the column GMS. Likewise the Galois root discriminant $5^\alpha \in \mathbf{R}$ is given approximately in the column GRD. The entries in the defining polynomial column for levels 5 and 4 are exactly the polynomials $g_{q^{5-\ell}}(x)$. The column T_2 then gives approximately the sum of the absolute squares of their roots, as in §3.7. For $\ell = 3$, 2, and 1 these numbers for $g_{q^{5-\ell}}(x)$ are approximately 51.94, 184.45 and 2094.02. Table 10 gives T_2-reduced polynomials instead.

9.3. **A compositum.** Let L and $\tilde{L}$ be our usual nonsolvable fields and let L^s be the solvable field for $p = 5$ from §9.2. The intersection of $\tilde{L}$ and L^s in $\mathbf{C}$ is exactly the degree twenty cyclotomic field $\mathbf{Q}(e^{2\pi i/25})$. The compositum $\tilde{L}L^s$ is a degree 5^5 elementary abelian extension of $\tilde{L}$.

The type of L^s is $0 \in \mathbf{F}_5$ while the type of L is 4, by the calculation of §9.1. Thus the types disagree and $\tilde{L}L^s/\tilde{L}$ is ramified, by Theorem 8.1. From Theorem 8.1 one can deduce two further things. First, $\tilde{L}L^s$ has just one 5-adic slope beyond the slopes of $\tilde{L}$. It is 5/4, the slope associated with $K_{0,1}$. Second, for $\ell = 1, \ldots, 5$, let L^s_ℓ be the level ℓ-subfield of L^s, as in the previous section. Then $\tilde{L}L^s_\ell/\tilde{L}$ is an extension of degree $[L^s_\ell : \mathbf{Q}(e^{2\pi i/25})] = 5^\ell$, and $\tilde{L}L^s_\ell$ is Galois over $\mathbf{Q}$, While $\tilde{L}L^s_5/\tilde{L}$ is ramified, as above, $\tilde{L}L^s_4/\tilde{L}$ is not.

9.4. **Concluding corollary.** The Galois number fields attracting most of our attention form a single chain, with relative Galois groups as indicated:

$$\mathbf{Q} \overset{PSL_2(5)^5.10}{\subset} L \overset{2^5.2}{\subset} \tilde{L} \overset{5^4}{\subset} \tilde{L}L^s_4 \overset{5}{\subset} \tilde{L}L^s. \tag{38}$$

Applying (35) again to compute the root discriminant of $\tilde{L}L^s$, we conclude by giving all the root discriminants:

Corollary 9.1. *The root discriminants of L, $\tilde{L}$, and $\tilde{L}L_4^s$ are all $125 \cdot 5^{-1/12500} \approx 124.984$. The root discriminant of $\tilde{L}L^s$ is $125 \cdot 5^{-17/312500} \approx 124.989$. Since $\tilde{L}L_4^s/\tilde{L}$ is an unramified elementary abelian extension of degree 5^4, the class number of $\tilde{L}$ is divisible by 5^4.*

References

[1] S. Amano, Eisenstein equations of degree p in a $\mathfrak{p}$-adic field, *J. Fac. Sci. Univ. Tokyo Sect. IA Math.*, **18** (1971), 1–21.

[2] M. Bhargava, Mass Formulae for Extensions of Local Fields, and Conjectures on the Density of Number Field Discriminants, *Internat. Math Res Notices*, 2007(rnm052):rnm052–20, 2007.

[3] J. Bosman, On the computation of Galois representations associated to level one modular forms, preprint, ArXiv:0710.1237 (2007), 15 pages.

[4] J. Buhler, C. Pomerance, and L. Robertson, Heuristics for class numbers of prime-power real cyclotomic fields, in *High primes and misdemeanours: lectures in honour of the 60th birthday of Hugh Cowie Williams*, Fields Inst. Commun., 41 (Amer. Math. Soc., Providence, RI, 2004) 149–157.

[5] H. Darmon and A. Granville, On the equations $z^m = F(x, y)$ and $Ax^p + By^q = Cz^r$, *Bull. London Math. Soc.* **27** (1995), no. 6, 513–543.

[6] L. Dembélé, A non-solvable Galois extension of $\mathbf{Q}$ ramified at 2 only, *C. R. Acad. Sci. Paris*, Ser I **347** (2009) 111–116.

[7] L. Dembélé, M. Greenberg, and J. Voight, Nonsolvable number fields ramified only at 3 and 5, preprint, arXiv:0906.4374 (v1, Jun 24, 2009 and v2, March 30, 2010).

[8] E. D. Driver and J. W. Jones, A targeted Martinet search, Math. Comp. **78** (2009), no. 266, 1109–1117.

[9] J. Edwards, A complete solution to $X^2 + Y^3 + Z^5 = 0$, *J. Reine Angew. Math.* **571** (2004), 213–236.

[10] B. Edixhoven, in collaboration with J.-M. Couveignes, R. de Jong, F. Merkl, and J. Bosman, On the computation of coefficients of a modular form, preprint, ArXiv:math/0605244 (2006,2009), 164 pages, revised version to appear in Annals of Mathematics Studies (Princeton University Press).

[11] B. H. Gross, Modular forms (mod p) and Galois representations, *Internat. Math. Res. Notices* 1998, **16**, 865–875.

[12] F. Jarvis, Mazur's principle for totally real fields of odd degree. *Compositio Math.* **116** (1999), no. 1, 39-79.

[13] J. W. Jones and D. P. Roberts, Number fields ramified at one prime, in *Algorithmic Number Theory*, Lecture Notes in Comput. Sci., 5011, (Springer, Berlin, 2008) 226–239.

[14] J. W. Jones and D. P. Roberts, A database of local fields, *J. Symbolic Comput.*, **41**, no. 1, (2006), 80–97. Database at `http://math.la.asu.edu/~jj/localfields/`

[15] J. W. Jones and D. P. Roberts, A database of number fields, in preparation.

[16] J. W. Jones and D. P. Roberts, Nonic 3-adic fields, in *Algorithmic number theory*, Lecture Notes in Comput. Sci., 3076, (Springer, Berlin, 2004) 293–308.

[17] J. Lansky and D. Pollack, Hecke algebras and automorphic forms, *Compositio Math.* **130** (2002), no. 1, 21–48.

[18] J. McKee, Computing division polynomials, *Math. Comp.* **63** (1994), no. 208, 767–771.

[19] The PARI Group, Bordeaux. PARI/GP, Version 2.3.4, 2009.

[20] D. P. Roberts, Wild partitions and number theory, *J. Integer Seq.* **10** (2007), no. 6, Article 07.6.6, 34 pages.

[21] D. P. Roberts, An *ABC* construction of number fields, in *Number Theory*, CRM Proc. Lecture Notes, 36, (Amer. Math. Soc., Providence, RI, 2004) 237–267.

[22] J.-P. Serre, *Local Fields*, Graduate Texts in Mathematics, 67 (Springer-Verlag, New York-Berlin, 1979).

[23] J.-P. Serre, Une "formule de masse" pour les extensions totalement ramifiées de degré donné d'un corps local, *C. R. Acad. Sci. Paris Sér. A-B* **286** (1978), no. 22, A1031–A1036.

[24] J.-P. Serre, Groupes de Galois sur $\mathbf{Q}$, in *Séminaire Bourbaki, Vol. 1987/88*, Astérisque No. 161-162, Exp. No. 689, 3 (1989), 73–85.

[25] J.-P. Serre, Un complément à la Note de Lassina Dembélé "A non-solvable Galois extension of $\mathbf{Q}$ ramified at 2 only," *C. R. Acad. Sci. Paris, Ser I* **347** (2009) 117-118.

[26] G. C. Shephard and J. A. Todd, Finite unitary reflection groups, *Canadian J. Math* **6**, (1954). 274–304.

[27] N. I. Shepherd-Barron and R. Taylor, Mod 2 and mod 5 icosahedral representations, *J. Amer. Math. Soc.* **10** (1997), no. 2, 283–298.

[28] J. H. Silverman, *The Arithmetic of Elliptic Curves,* 2nd ed., Graduate Texts in Mathematics, 106 (Springer, Dordrecht, 2009).

[29] C. M. Skinner and A. J. Wiles, Nearly ordinary deformations of irreducible residual representations, *Ann. Fac. Sci. Toulouse Math. (6)* **10** (2001), no. 1, 185-215.
[30] H. P. F. Swinnerton-Dyer, On l-adic representations and congruences for coefficients of modular forms, in *Modular functions of one variable, III (Proc. Internat. Summer School, Univ. Antwerp, 1972)*, Lecture Notes in Math., Vol. 350, (Springer, Berlin, 1973) 1–55.
[31] L. C. Washington, *Introduction to Cyclotomic Fields,* 2nd ed., Graduate Texts in Mathematics, 83 (Springer-Verlag, New York, 1997).

Division of Science and Mathematics, University of Minnesota, Morris, Morris, Minnesota, 56267, USA