1-2006

A Database of Local Fields

John W. Jones
Arizona State University

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

A DATABASE OF LOCAL FIELDS

JOHN W. JONES AND DAVID P. ROBERTS

Abstract. We describe our online database of finite extensions of $\mathbf{Q}_p$, and how it can be used to facilitate local analysis of number fields.

1. Introduction

1.1. **Overview.** Given a number field K, one has for each prime p its associated p-adic algebra,

$$K \otimes \mathbf{Q}_p \cong \prod_{i=1}^{g} K_{p,i}\,.$$

Here the $K_{p,i}$ are fields, each a finite extension of $\mathbf{Q}_p$. For investigating some problems about number fields, it suffices to know just basic invariants of the $K_{p,i}$, such as ramification index and residual degree. For other investigations, it is essential to have much more refined information, such as local Galois groups and slopes measuring wildness of ramification.

To facilitate refined analysis of number fields, we have constructed a database of p-adic fields, available at `http://math.asu.edu/~jj/localfields`. Let $\mathcal{K}(p,n)$ be the set of isomorphism classes of degree n extensions of $\mathbf{Q}_p$. The sets $\mathcal{K}(p,n)$ are finite, with general mass formulas which counting these fields with certain weights being known [Se2, Kr, PR]. Our database presents some of the sets $\mathcal{K}(p,n)$ in a complete and easy-to-use way. The philosophy behind the database is that the intricate local considerations needed to construct it should be done once and then recorded. Thereafter, a local result can be obtained by mechanical appeal to the database whenever it is needed in a global situation.

1.2. **Fields in the database.** When n is not divisible by p, all fields in $\mathcal{K}(p,n)$ are tame, and so $\mathcal{K}(p,n)$ is relatively easy to describe. Our database treats these fields dynamically, with restrictions on p and n limited only by computational feasibility. The first case involving wild fields is $n = p$. This case is also relatively easy to describe in a way uniform in p; for example, $|\mathcal{K}(p,p)| = p^2 + 1$ for p odd. Again, our database treats these fields essentially without restriction on p.

The backbone of our database consists of tables explicitly describing $\mathcal{K}(p,n)$ for small p and n. The numbers $|\mathcal{K}(p,n)|$ for $p < 30$ and $n < 10$ are listed in Table 1.1. The table for $\mathcal{K}(p,n)$ in the database has one line for each isomorphism class of p-adic field of degree n and gives a defining polynomial for the field and many invariants of the field. Our tables provide many illustrations of the relatively easy cases discussed in the previous paragraph. However their main function is to cover the five harder cases with $n < 10$, namely $(p,n) = (2,4)$, $(2,6)$, $(3,6)$, $(2,8)$, and $(3,9)$. The case of 2-adic quartics has received detailed attention previously, for example in [We] for the one A_4 and the three S_4 extensions and in [Na] for the

TABLE 1.1. The number $|\mathcal{K}(p,n)|$ of isomorphism classes of p-adic fields of degree n, for $p < 30$ and $n < 10$. The entries corresponding to the five cases which we treat individually are underlined.

n	2	3	5	7	11	13	17	19	23	29
1	1	1	1	1	1	1	1	1	1	1
2	7	3	3	3	3	3	3	3	3	3
3	2	10	2	4	2	4	2	4	2	2
4	59	5	7	5	5	7	7	5	5	7
5	2	2	26	2	6	2	2	2	2	2
6	47	75	7	12	7	12	7	12	7	7
7	2	2	2	50	2	2	2	2	2	8
8	1823	8	11	8	8	11	15	8	8	11
9	3	795	3	7	3	7	3	13	3	3

thirty-six D_4 extensions. Also the case of 2-adic octics with Galois group within $GL_2(3)$ was previously treated in [BR].

1.3. **Sections of this paper.** Section 2 discusses how we found our lists of defining polynomials. It treats first the tame and $n = p$ cases systematically, and then describes our *ad hoc* approach to the five harder cases. Section 3 discusses how we computed the invariants for each field K in the database. The most difficult invariants to compute in the five harder cases (p,n) are the local Galois groups G and the size of all the subquotients $Q^s = G^s/G^{s+}$ coming from the filtration of G by its ramification subgroups. Our general approach is to compute G and the Q^s simultaneously, by working within K as much as possible and, when necessary, also working inside suitable resolvents L.

Section 4 gives some details on the computation of G and the Q^s, these details naturally depending strongly on the field at hand. The cases $(p,n) = (2,4)$, $(2,6)$, and $(3,6)$ are roughly equal in complexity, and we treat them all systematically here, giving a table for each summarizing the much larger table on our database. These low degree cases are too simple to provide good illustrations of our general technique: very few resolvents are needed and all the "hidden" slopes s are easy to find. So we give also one representative example each from $(2,8)$ and $(3,9)$. These two cases are very much more intricate than the previous three, and we treat them systematically in the companion papers [JR3] and [JR2].

Section 5 begins by describing the two interactive features of our database, what we call the p-adic identifier and the Galois root discriminant calculator. These are designed to maximize the utility of our database for applications. Section 5 concludes by briefly discussing three applications of the sort we have in mind, [APSo], [APSi], and [JR4].

2. A complete irredundant list of defining polynomials

In this section, we describe how we chose the polynomials defining the fields in the database. Sections 2.1–2.3 deal with unramified, tamely ramified, and degree p extensions of $\mathbf{Q}_p$, respectively. Section 2.4 deals with the remaining cases — wildly ramified extensions of composite degree.

2.1. **Unramified extensions.** Unramified extensions of $\mathbf{Q}_p$ are very simple, there being a unique one for each degree n, up to isomorphism. The only task is to choose a defining polynomial for each. In the sequel, we will usually drop qualifiers like "up to isomorphism," as they are always present and our meaning is clear.

Since the unramified extension of degree n of $\mathbf{Q}_p$ corresponds to the unique degree n extension of the residue field, one option is to use Conway polynomials [HL] for these extensions since they are a standard choice for defining $\mathbf{F}_{p^n}$ over $\mathbf{F}_p$ (e.g., they are used in the computer systems `magma` and `gap`). However, Conway polynomials can be expensive to compute, primarily because they are required to satisfy a compatibility condition which is not used here. Instead, our selection of defining polynomials described below is in the same spirit, but with fewer restrictions.

We pick the "first" polynomial over $\mathbf{F}_p$ which has roots which are primitive, i.e., of multiplicative order $p^n - 1$. Here we use the same lexicographic ordering as for Conway polynomials. Namely, we write polynomials in the form $f(x) = x^n - a_{n-1}x^{n-1} + a_{n-2}x^{n-2} - \cdots$ and $g(x) = x^n - b_{n-1}x^{n-1} + b_{n-2}x^{n-2} - \cdots$ with a_i and b_i between 0 and $p-1$ inclusive. Then we define $f < g$ iff there exists k with $a_i = b_i$ for all $i > k$ and $a_k < b_k$. This normalization also defines how we will represent the polynomials in $\mathbf{Z}[x] \subset \mathbf{Q}_p[x]$. To compute these polynomials, we simply step through them in the given ordering until an irreducible primitive polynomial is found. Note that for defining $\mathbf{Q}_p$ itself, our choice leads to the "degree one Conway polynomial" $x - r$, where r is the first primitive root modulo p.

2.2. **Tame extensions.** Our starting point is the following standard result on totally ramified tame extensions, whose statement is based on [PR, Theorem 7.2].

Proposition 2.2.1. *Let K^u be an unramified extension of $\mathbf{Q}_p$ with degree f. Let $\zeta \in K^u$ be a primitive $(p^f-1)^{\text{st}}$ root of unity. Let e be a positive integer with $p \nmid e$.*

1. *The totally ramified degree e extensions of K^u, are given by roots of polynomials $h_{e,r}(x) = x^e - \zeta^r p$.*
2. *Two such polynomials $h_{e,r}$ and $h_{e,r'}$ yield K^u-isomorphic extensions iff $r \equiv r' \pmod{\gcd(e, p^f-1)}$.*
3. *If a monic polynomial g satisfies $g \equiv h_{e,r} \pmod{p^2}$, then g defines the same extension as $h_{e,r}$.*

Proof: The first part is stated in [PR, Theorem 7.2]. Moreover, the backward implication of Part (2) follows from the proof given there, and the forward direction then follows from the statement in [PR] that the $h_{e,r}$ give mutually non-isomorphic fields for $0 \le r < g$.

The final part follows from a standard Krasner's Lemma argument, or from the construction used in [PR, Theorem 7.1–7.2] to produce defining polynomials; the coefficients are picked from a set which is only well-defined modulo p^2. □

To apply the proposition, we take $K^u = \mathbf{Q}_p[\alpha]/h(\alpha)$ where h is the degree f polynomial chosen in the previous subsection. We consider $x^e - \alpha^r p$, as the third part of Proposition 2.2.1 lets us replace ζ by α.

To move from an irreducible polynomial $k(x)$ over K^u to a polynomial over $\mathbf{Q}_p$, we take norms, in the sense of the product of conjugates under $\mathrm{Gal}(K^u/\mathbf{Q}_p)$. The norm of $k(x)$ is irreducible over $\mathbf{Q}_p$ iff the conjugates of $k(x)$ are distinct. Since $\mathrm{Gal}(K^u/\mathbf{Q}_p)$ is generated by Frobenius σ, with

$$\sigma(\alpha) \equiv \alpha^p \pmod{p},$$

the polynomials $x^e - \alpha^r p$ give conjugate extensions for r which differ multiplicatively by a power of p. Thus, taking the norm of $x^e - \alpha^r p$ to $\mathbf{Q}_p[x]$, we get an irreducible polynomial iff the orbit of r in $\mathbf{Z}/(p^f-1)\mathbf{Z}$ under multiplication by p has length f.

Our recipe for picking defining polynomials of tamely ramified extensions with given e and f is as follows. Let $g = \gcd(e, p^f - 1)$ and partition $\mathbf{Z}/g\mathbf{Z}$ into orbits under multiplication by p. These orbits correspond to the desired extensions of $\mathbf{Q}_p$. For each orbit $\mathcal{O} \subseteq \mathbf{Z}/g\mathbf{Z}$, we lift its elements to $\mathbf{Z}/(p^f-1)\mathbf{Z}$ and consider them under multiplication by p.

Now, there are two cases. If there is an orbit of length f, take the smallest $r \geq 0$ contained in such an orbit. Then the norm of $x^e - \alpha^r p$ to $\mathbf{Q}_p[x]$ will be irreducible. Otherwise, if there are no lifts to an orbit of length f for our orbit $\mathcal{O}$, we take the smallest $r \geq 0$ representing an element of the orbit and use the norm of the polynomial $k(x) = (x+\alpha)^e - \alpha^r p$ to $\mathbf{Q}_p[x]$. This fallback polynomial is guaranteed to give a defining polynomial for our extension by the following proposition.

Proposition 2.2.2. *Let $K^u = \mathbf{Q}_p(\alpha)$ be the unramified extension of $\mathbf{Q}_p$ of degree f, where α generates the multiplicative group modulo p. If $r \in \mathbf{Z}$ and e is a positive integer, then the norm of $k(x) = (x+\alpha)^e - \alpha^r p$ to $\mathbf{Q}_p[x]$ is irreducible over $\mathbf{Q}_p$.*

Proof: If the norm of $k(x)$ is reducible, then two conjugates of $k(x)$ would be equal. Letting $\sigma \in \mathrm{Gal}(K^u/\mathbf{Q}_p)$ denote the Frobenius automorphism, we get equality of the degree $e-1$ terms of these conjugates: $e\sigma^a(\alpha)x^{e-1} = e\sigma^b(\alpha)x^{e-1}$ with $1 \leq a, b < f$. But this implies $\alpha^{p^a} \equiv \alpha^{p^b} \pmod{p}$. Since α reduces modulo p to an element of order $p^f - 1$, this implies $a = b$. □

To illustrate the procedure, suppose we want to generate the sextic tame extensions of $\mathbf{Q}_5$ with residue degree 2. We first construct the unramified quadratic extension of $\mathbf{Q}_5$ by the procedure described in §2.1, giving $K^u = \mathbf{Q}_5[\alpha]/(\alpha^2 - \alpha + 2)$. Here $g = \gcd(e, p^f - 1) = \gcd(3, 5^2 - 1) = 3$. Multiplication by 5 on $\mathbf{Z}/3\mathbf{Z}$ has two orbits, $\{1, 2\}$ and $\{0\}$, so there will be two extensions. In the first case, $\{1, 5\} \subset \mathbf{Z}/24\mathbf{Z}$ is the prescribed lift, so we take the norm of $x^3 - 5\alpha$ to get $x^6 - 5x^3 + 50$. For the other orbit, the first orbit modulo 24 of length $f = 2$ reducing to $\{0\}$ is $\{3, 15\}$. Thus, we take the norm of $x^3 - 5\alpha^3$ to get $x^6 + 25x^3 + 200$.

As an example where the last phase of the procedure is necessary, consider degree 12 extensions of $\mathbf{Q}_5$ with $e = 6$ and $f = 2$ so that $g = \gcd(6, 24) = 6$. The orbit $\{0\} \subset \mathbf{Z}/6\mathbf{Z}$ has only lifts of size 1 in $\mathbf{Z}/24\mathbf{Z}$. So, we take the norm of $(x+\alpha)^6 - 5$, which is the irreducible polynomial $x^{12} + 6x^{11} + 27x^{10} + 80x^9 + 195x^8 + 366x^7 + 571x^6 + 702x^5 + 1005x^4 + 1140x^3 + 357x^2 - 138x + 44$.

2.3. **Degree p ramified extensions of $\mathbf{Q}_p$.** The six ramified quadratic extensions of $\mathbf{Q}_2$ are given by $x^2 - D$ for $D = -4$, 12, ± 8, and ± 24, with $\mathrm{ord}_2(D)$ being the discriminant exponent c. Each of these six extensions has two automorphisms. The rest of this subsection treats the case of p odd, which is different as the generic degree p extension of $\mathbf{Q}_p$ has just the identity automorphism.

Most of the information we need can then be extracted from [Am]. These fields come in three families as shown in Table 2.1, which gives our preferred defining polynomials.

Proposition 2.3.1. *If p is an odd prime, Table 2.1 gives exactly one polynomial for each isomorphism class of ramified degree p extension of $\mathbf{Q}_p$, where the degree p field K has ramification exponent c, and the Galois closure K^g has Galois groups*

TABLE 2.1. Degree p ramified extensions of $\mathbf{Q}_p$, for p odd.

Family	Parameters	c	G	I
$x^p + apx^\lambda + p$	$1 \le a \le p-1$ $1 \le \lambda \le p-1$ $(\lambda, a) \ne (p-1, p-1)$	$p + \lambda - 1$	$C_p : C_{d_2}$	$C_p : C_{d_1}$
$x^p - px^{p-1} + p(1+ap)$	$0 \le a \le p-1$	$2p-2$	C_p	C_p
$x^p + p(1+ap)$	$0 \le a \le p-1$	$2p-1$	$C_p : C_{p-1}$	$C_p : C_{p-1}$

and inertia groups as shown. In Table 2.1, $d_1 = (p-1)/g$ *where* $g = \gcd(p-1, c)$. *Also* $d_2 = (p-1)/(\gcd((p-1)/m, g))$ *where* m *is the order of* $a\lambda$ *in* $\mathbf{F}_p^*$.

Proof: Theorems 6 and 7 of [Am] show that the families given in Table 2.1 give each ramified degree p extension of $\mathbf{Q}_p$ exactly once. Computing the value of c from an Eisenstein polynomial is well-known (see e.g., [Se1, §III.6]). This leaves the determination of the Galois and inertia groups.

Let π be a root of one of the polynomials in Table 2.1. Then Section 2 of [Am] gives an explicit description of the Galois closure of $\mathbf{Q}_p(\pi)$ as $K^g = \mathbf{Q}_p(\pi, \gamma)$ where $\gamma^{p-1} \in \mathbf{Q}_p$. Since $\mathbf{Q}_p$ contains a primitive $(p-1)^{\text{st}}$ root of unity, $\mathbf{Q}_p(\gamma)/\mathbf{Q}_p$ is Galois with cyclic Galois group and $K^g/\mathbf{Q}_p(\gamma)$ is Galois of degree p, hence also cyclic. Since the orders of these cyclic groups are relatively prime, the Galois and inertia groups are semi-direct products of the form $C_p : C_d$ for some d. All that remains is to determine d in each case. For our second (resp. third) family, [Am] shows one can take γ to be 1 (resp. a primitive p-th root of unity). In both of these cases, $K^g/\mathbf{Q}_p$ is clearly totally ramified, and $d = 1$ (resp. $p-1$) for the Galois and inertia groups.

For the first family, let $d_2 = [\mathbf{Q}_p(\gamma) : \mathbf{Q}_p]$ and let d_1 be the tame degree. We need to show that these are given by the formulas stated in the theorem. Note $g = \gcd(p-1, c) = \gcd(p-1, \lambda + p - 1) = \gcd(p-1, \lambda)$. Then [Am] gives the unramified subextension of K^g as $\mathbf{Q}_p(\theta)$ where $\theta^g = \lambda a$, and γ above satisfies $\gamma^{(p-1)/g} = \theta p^{\lambda/g}$. Clearly, the tame degree $d_1 = [\mathbf{Q}_p(\gamma) : \mathbf{Q}_p(\theta)] = (p-1)/g$. Since λa is prime to p, modulo p is it a $(p-1)/m$ power of a generator of $\mathbf{F}_p^*$, hence $[\mathbf{Q}_p(\theta) : \mathbf{Q}_p] = g/\gcd((p-1)/m, g)$. Thus,

$$d_2 = d_1 \cdot [\mathbf{Q}_p(\theta) : \mathbf{Q}_p] = \frac{p-1}{g} \frac{g}{\gcd((p-1)/m, g)} = \frac{p-1}{\gcd((p-1)/m, g)}. \qquad \square$$

2.4. **Wild extensions of composite degree.** The complexity of the unramified, tamely ramified, and degree p cases just treated suggests that analogous recipes for the remaining cases would have to be quite complex indeed. So instead, we treat the five cases $(p, n) = (2, 4)$, $(2, 6)$, $(3, 6)$, $(2, 8)$, and $(3, 9)$ individually. The problem then becomes simply to find a defining polynomial for each degree n extension of $\mathbf{Q}_p$ for the given (p, n).

Pauli and Roblot give a general algorithm for solving this problem. One key ingredient is Panayi's p-adic root finding algorithm [Pa], [PR, Section 8] which lets one determine whether two degree n fields $\mathbf{Q}_p[x]/f_1(x)$ and $\mathbf{Q}_p[x]/f_2(x)$ are isomorphic and similarly lets one compute the number of automorphisms of a given field $\mathbf{Q}_p[x]/f(x)$. Another key ingredient is the mass formula [PR, Theorem 6.1] which lets one determine when all fields have been found.

We used Pauli and Roblot's approach for generating polynomials as needed. However, in some special cases, we generated the polynomials instead by utilizing complete lists of lower degree fields. We did this in two situations, fields which contain an index 2 subfield, and degree 6 fields.

When computing degree n fields K with n even, one can take each field E of degree $n/2$ and find its quadratic extensions by taking square roots of representatives of E^* modulo squares. This approach was helpful in generating many, although certainly not all, of the 2-adic octic fields.

For degree 6 fields, most extensions are old fields in the terminology of [JR1, §3.2], and can be computed by sextic twinning from lower degree fields. This approach is illustrated in [JR1] for certain extensions of $\mathbf{Q}$. Computing old fields by twinning produces all 2-adic sextics and most of the 3-adic sextics. For all remaining cases we used [PR].

3. Invariants associated to a given p-adic field

Let $f(x) \in \mathbf{Z}[x]$ be a degree n polynomial on one of our p-adic tables. In this section, we discuss the invariants the tables present for the corresponding field $K = \mathbf{Q}_p[x]/f(x)$. Table 3.1 serves as a guide to the discussion, with the top line indicating the subsection in which the corresponding invariant is discussed.

Table 3.1. The first six lines of the 2-adic quartic table, corresponding to the fields with $c \leq 4$.

3.1	3.1	3.1	3.1	3.3		3.5	3.5	3.4, 3.6 Galois Slope Content	3.7 GMS	3.2 Deg 2 Subs
c	e	f	d	ϵ	Polynomial	G	I			
0	1	4	$*$	1	$x^4 - x + 1$	C_4	$\langle e \rangle$	$[\,]^4$	0	$*$
4	2	2	1	-1	$x^4 + 8x^2 + 4$	V_4	C_2	$[2]^2$	1	$*, -1, -*$
4	2	2	$*$	-1	$x^4 - x^2 + 5$	C_4	C_2	$[2]^2$	1	$*$
4	2	2	-1	$-i$	$x^4 + 2x^2 + 4x + 4$	D_4	V_4	$[2,2]^2$	3/2	$*$
4	2	2	$-*$	$-i$	$x^4 - 5$	D_4	V_4	$[2,2]^2$	3/2	$*$
4	4	1	$*$	1	$x^4 + 2x + 2$	S_4	A_4	$[4/3, 4/3]_3^2$	7/6	

It is important to note that our numbering system for slopes differs from the standard reference [Se1] by a shift of 1, in the sense that our ramification group G^s is G^{s-1} in this reference. With our convention, slopes s arise literally as slopes $\Delta c/\Delta n$, as we explain in §3.4. In our convention, 0 corresponds to no ramification, 1 to tame ramification, and slopes $s > 1$ to wild ramification, and this is a useful normalization in global contexts. Note also that our computations require only a small part of [Se1]. For example, we don't use the lower numbering system at all, and thus we have no need of the transition functions between the lower and upper numbering systems.

3.1. **Basic Data.** The field discriminant of K as an ideal is $(p^c) \subseteq \mathbf{Z}_p$. The largest unramified subfield of K^u of K has degree the residual degree $f = [K^u : \mathbf{Q}_p]$. The ramification index is $e = n/f = [K : K^u]$. The entry d in the fifth

column is the field discriminant considered as an element of $\mathbf{Q}_p^\times/\mathbf{Q}_p^{\times 2}$. Here and elsewhere, $* \in \mathbf{Q}_p^\times/\mathbf{Q}_p^{\times 2}$ stands for the class of elements $a \in \mathbf{Q}_p^\times$ such that $\mathbf{Q}_p(\sqrt{a})$ is the unramified quadratic field extension of $\mathbf{Q}_p$. With this notational convention, $\mathbf{Q}_2^\times/\mathbf{Q}_2^{\times 2} = \{1, *, -1, -*, 2, 2*, -2, -2*\}$ and otherwise $\mathbf{Q}_p^\times/\mathbf{Q}_p^{\times 2} = \{1, *, p, p*\}$. We use number field commands in the computer program `gp` [PARI2] to compute c, e, and f. The discriminant class d is also easy to compute with `gp` from polynomial or number field discriminants.

3.2. **Subfields and automorphisms.** Our database gives all subfields of K of degrees $2, \ldots, n-1$, with each subfield hyperlinked to its entry in the database. Quadratic subfields are listed by the codes described in the previous subsection. An unramified subfield of degree $d > 2$ is listed as simply U_d. All other subfields are listed by their chosen defining polynomial. To determine if one field is a subfield of another, we make use of Panayi's p-adic root finding algorithm mentioned in §2.4, and apply it to each candidate subfield from the database with compatible degree, discriminant exponent, and residual degree.

Similarly, we use Panayi's root finding algorithm to find the number of automorphisms of K. Note that the automorphism group $\mathrm{Aut}(K/\mathbf{Q}_p)$ has order dividing $n = [K : \mathbf{Q}_p]$. Often, especially when $p > 2$, $|\mathrm{Aut}(K/\mathbf{Q}_p)| = 1$. Then the Galois group $\mathrm{Gal}(K^g/\mathbf{Q}_p)$ introduced below tends to be large, having order at least $2n$. At the other extreme, if $|\mathrm{Aut}(K/\mathbf{Q}_p)| = n$ then we can take $K^g = K$ and so $\mathrm{Gal}(K^g/\mathbf{Q}_p) = \mathrm{Aut}(K/\mathbf{Q}_p)$.

3.3. **Local root numbers.** Our database gives the local root number $\epsilon(K) \in \{1, i, -1, -i\}$. In this subsection, we sketch the context set up by the standard reference [T] and then completely describe our method of calculation. In this subsection only, we allow p also to be ∞, writing $\mathbf{Q}_\infty = \mathbf{R}$.

Local root numbers, $\epsilon(\rho) \in \mathbf{C}^\times$, are defined for representations $\rho : \mathrm{Gal}(\overline{\mathbf{Q}}_p/\mathbf{Q}_p) \to GL_n(\mathbf{C})$. They have absolute value 1, are multiplicative in the sense that $\epsilon(\rho_1 \oplus \rho_2) = \epsilon(\rho_1)\epsilon(\rho_2)$, and for $p \neq \infty$, any unramified representation has root number 1. The root number for the trivial and sign characters of $\mathrm{Gal}(\mathbf{C}/\mathbf{R})$ are 1 and $-i$ respectively [T, §1]. Finally, if $\rho : \mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q}) \to GL_n(\mathbf{C})$ is a global representation whose restrictions to decomposition groups are denoted by ρ_p, the global root number $\epsilon(\rho)$ equals the product of local root numbers $\prod \epsilon(\rho_p)$, and $\epsilon(\rho)$ figures into the functional equation of the Artin L-function $L(\rho, s)$.

If K is an n-dimensional p-adic algebra then $\mathrm{Gal}(\overline{\mathbf{Q}}_p/\mathbf{Q}_p)$ acts on the set of its n embeddings into $\overline{\mathbf{Q}}_p$. One thus has a representation $\rho_K : \mathrm{Gal}(\overline{\mathbf{Q}}_p/\mathbf{Q}_p) \to S_n \subset GL_n(\mathbf{C})$. For every field K on our database, we give the corresponding root number $\epsilon(K) := \epsilon(\rho_K)$. These particular root numbers play a central role in Galois embedding problems; for statements and examples see e.g. [JR1], especially page 144. The $\epsilon(K)$ are simpler than general root numbers in several ways. First, as will be clear from our method of computation, $\epsilon(K)$ is always in $\{1, i, -1, -i\}$. Second, for K a number field, the global root number $\epsilon(K) = \prod \epsilon(K_p)$ is always 1 [T, §3 Cor. 1]. Finally, computing general local root numbers requires the evaluation of Gauss sums over general p-adic fields. We avoid evaluating Gauss sums for our particular local root numbers as follows.

Let $(\cdot, \cdot)$ be the Hilbert symbol on $\mathbf{Q}_p^\times/\mathbf{Q}_p^{\times 2} \times \mathbf{Q}_p^\times/\mathbf{Q}_p^{\times 2}$. By definition (d, a) is 1 if a is a norm from $\mathbf{Q}_p(\sqrt{d})$ and -1 otherwise. The pairing is bimultiplicative, and

TABLE 3.2. Some Hilbert symbols (d, a) and local root numbers $\epsilon(d)$. For d, $a \in \mathbf{Q}^\times/\mathbf{Q}^{\times 2}$ with images d_p, $a_p \in \mathbf{Q}_p^\times/\mathbf{Q}_p^{\times 2}$, one has the standard facts $\prod(d_p, a_p) = 1$ and $\prod \epsilon(d_p) = 1$. These product formulas let one deduce the p-adic tables from the $p = \infty$ table.

$p=\infty$		
	-1	
-1	$-$	

$p=2$			
	$*$	-1	2
$*$	$+$	$+$	$-$
-1	$+$	$-$	$+$
2	$-$	$+$	$+$

$p\equiv 3\ (4)$		
	$*$	p
$*$	$+$	$-$
p	$-$	$-$

$p\equiv 1\ (4)$		
	$*$	p
$*$	$+$	$-$
p	$-$	$+$

ϵ	$-i$

ϵ	1	i	1

ϵ	1	$-i$

ϵ	1	1

so determined by the values given on the generators in Table 3.2. Also one knows *a priori* that for all p, one has $(*, *) = 1$.

Let ρ_d be the quadratic character $\rho_d(a) = (d, a)$. Table 3.2 also gives some quadratic root numbers $\epsilon(d) := \epsilon(\rho_d)$. The remaining quadratic root numbers $\epsilon(d)$ can then be computed by the general formula [T, §3 Cor. 2]

$$\epsilon(d_1)\epsilon(d_2) = (d_1, d_2)\epsilon(d_1 d_2).$$

The main ingredient in our calculation is the formula

$$\epsilon(K) = (2, d)\ \mathrm{HW}(K)\ \epsilon(d), \tag{1}$$

obtained by combining the main theorems of [D] and [Se3]. In this formula, $d \in \mathbf{Q}_p^\times/\mathbf{Q}_p^{\times 2}$ is the discriminant class of K. Also $\mathrm{HW}(K)$ is the p-adic Hasse-Witt invariant of the quadratic form $\mathrm{Trace}_{K/\mathbf{Q}_p}(x^2)$ on K.

For the cases $(p, n) = (2, 4)$, $(2, 6)$, $(3, 6)$, and $(2, 8)$ we compute $\mathrm{HW}(K)$ directly, by diagonalizing the quadratic form $\mathrm{Trace}_{K/\mathbf{Q}_p}(x^2)$ and applying the formula $\mathrm{HW}(\sum a_j x_j^2) = \prod_{j<k}(a_j, a_k)$. For the remaining cases on our database, this direct computation is unnecessary as there are general formulas for $\mathrm{HW}(K)$, giving the following general formulas for $\epsilon(K)$.

Proposition 3.3.1. *Let $K/\mathbf{Q}_p$ be an extension with discriminant class d, ramification index e, and inertial degree f. If K has odd degree and p is odd, then*

$$\epsilon(K) = (2\,(-1)^{(ef-1)/2}, d)\epsilon(d). \tag{2}$$

If K has odd degree and $p = 2$, then

$$\epsilon(K) = 1. \tag{3}$$

If K is tame and p is odd, then

$$\epsilon(K) = \begin{cases} 1 & \text{if } e \text{ is odd,} \\ (2e, p)(-1)^{(p-1)(f+1+e)/4}\epsilon(d) & \text{if } e \text{ is even but } f \text{ is odd,} \\ -(d, p)(-1)^{(p-1)f/4} & \text{if } e \text{ and } f \text{ are both even.} \end{cases} \tag{4}$$

Proof: The calculation establishing Formula (2) is

$$\begin{aligned}\epsilon(K) &= (2,d)\,\mathrm{HW}(K)\epsilon(d)\\ &= (2,d)\cdot((-1)^{(ef-1)/2},d)c_p(K)\cdot\epsilon(d)\\ &= (2\,(-1)^{(ef-1)/2},d)\epsilon(d).\end{aligned}$$

Here the second equality translates to the notation of [CP] and the third equality applies Theorem II.6.4 of [CP] which says $c_p(K)=1$.

The remaining two cases are tame and so $c=(e-1)f$. If $p=2$, then c is even and moreover $d\in\{1,*\}$. If p is odd, then c is odd exactly when e is even and f is odd. In this case, $d\in\{p,*p\}$ while otherwise $d\in\{1,*\}$. This partial knowledge of d naturally simplifies many formulas; for example, if $d\in\{1,*\}$ then $\epsilon(d)=1$.

For Formula (3), one has

$$\begin{aligned}\epsilon(K) &= (2,d)\,\mathrm{HW}(K)\epsilon(d)\\ &= (2,d)\cdot(d,(-1)^{(n-1)/2})(-1)^{(n^2-1)/8}c_2(K)\cdot 1\\ &= (d,2\,(-1)^{(n-1)/2})(-1)^{(n^2-1)/8}(-1)^{(f^2-1)/8}\\ &= (d,2)(-1)^{(e^2-1)/8}\\ &= ((-1)^{(e-1)/2}e,2)(-1)^{(e^2-1)/8}\\ &= 1.\end{aligned}$$

The second equality is again a translation into the notation of [CP], although this time requiring a factor not present in the case p odd. The third equality applies Corollary 1 of [E]. The fourth equality removes the sign $(-1)^{(n-1)/2}$ because $(1,-2)=(1,2)=1$ and $(*,2)=(*,-2)=-1$. The fifth equality is explained in the next paragraph. The last equality holds because both factors are 1 if $e\equiv 1,7\ (8)$ and -1 if $e\equiv 3,5\ (8)$.

For the equality $d=(-1)^{(e-1)/2}e$ in $\mathbf{Q}_2^\times/\mathbf{Q}_2^{\times 2}$, note that the odd degree 2-adic field K can be presented as $K=K^u[x]/(x^e-a)$ for some $a\in K^u$. So its discriminant class in $\mathbf{Q}_2^\times/\mathbf{Q}_2^{\times 2}$ is

$$\begin{aligned}d &= \mathrm{Norm}_{K^u/\mathbf{Q}_p}(\mathrm{disc}(x^e-a))d(K^u)\\ &= \mathrm{Norm}_{K^u/\mathbf{Q}_p}((-1)^{(e-1)/2}e^e a^{e-1})\cdot 1\\ &= (-1)^{f(e-1)/2}e^{fe}\mathrm{Norm}_{K^u/\mathbf{Q}_p}(a)^{e-1}\\ &= (-1)^{(e-1)/2}e.\end{aligned}$$

Finally, Formula (4) is derived in a similar fashion, this time using Theorem II.6.5 of [CP] to evaluate $\mathrm{HW}(K)$, and then consolidating several cases. Note that Part Ia of this theorem contains a misprint and should read $c_p\langle F\rangle=-(p,\mathrm{dis}\langle F\rangle)_p$. □

3.4. **Slopes.** For each subfield L of K, let $(n(L),c(L))$ be the corresponding point in the n-c plane. Let U be the lower boundary of the convex hull of these points, so that U runs from $(1,0)$ to $(n(K),c(K))$. Figure 3.1 presents both the points and U in the case $K=\mathbf{Q}_2(\sqrt{-3},\sqrt{-1},\sqrt{2})$. In this case, the points at $(2,2)$ and $(4,6)$ each come from two subfields while the points $(2,3)$ and $(4,8)$ each come from four subfields. The remaining points, that is the points on U, each come from just one subfield.

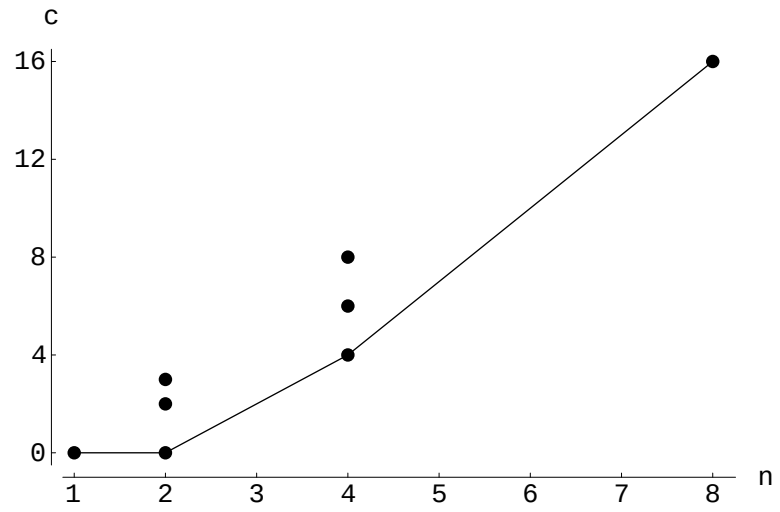

FIGURE 3.1. Slopes as illustrated by $K = \mathbf{Q}_2(\sqrt{-3}, \sqrt{-1}, \sqrt{2})$.

The slopes of K are by definition the slopes of the segments forming U, so 0, 2, and 3 in the example. Suppose the segment with slope s goes from (n_1, c_1) to (n_2, c_2). Then we define the additive multiplicity of s to be the horizontal length $a_s = n_2 - n_1$ and the multiplicative multiplicity to be the quotient $m_s = n_2/n_1$. Trivially one has

$$\begin{aligned} 1 + \sum_s a_s &= \prod_s m_s = n(K), \\ \sum_s a_s s &= c(K). \end{aligned}$$

In our example, these equations are $1+(1+2+4) = 2^3 = 8$ and $1\cdot 0+2\cdot 2+4\cdot 3 = 16$ respectively.

Ramification theory says that in general the endpoints and turning points of U each come from exactly one subfield, and we call these subfields *distinguished.* The distinguished subfields will be described Galois-theoretically in §3.6 below, where the uniqueness will be clear. From the Galois-theoretic description it is also clear that the distinguished fields form a chain. In the example, the chain is

$$K_1^0 \subset K_2^0 \subset K_4^4 \subset K_8^{16}. \tag{5}$$

Here we are superscripting by c and subscripting by n, these invariants characterizing the subfield among all subfields of K, as already mentioned above.

Another labeling scheme is also useful. For $s \in [0, \infty)$, let K^s be the largest distinguished subfield with all slopes $< s$. Similarly, for $s \in [0, \infty)$ let K^{s+} be the largest distinguished subfield with all slopes $\leq s$. It is natural to regard the allowed upper indices as forming a single totally ordered set, by declaring that $s+$ is infinitesimally larger than s. In the above example, K_1^0, K_2^0, K_4^4, and K_8^{16} are K^σ for any σ in $\{0\}$, $[0+, 2]$, $[2+, 3]$, and $[3+, \infty)$ respectively.

In general $K^0 = \mathbf{Q}_p$, $K^{0+} = K^1$ is the maximal unramified subfield, and K^{1+} is the maximal tamely ramified subfield. Thus $[K^{0+} : K^0] = f$ and $[K^{1+} : K^1] = e_t$,

where e_t is the prime-to-p part of e. Besides 0 and 1, the only other s for which $[K^{s+} : K^s]$ can be greater than 1 are rational numbers greater than 1. These s are by definition the wild slopes of K and their multiplicative multiplicities $[K^{s+} : K^s]$ have the form p^{ℓ_s} for ℓ_s a positive integer.

To compactly indicate the slopes of K we write $[\cdots]_{e_t}^f$ where the brackets include the wild slopes in increasing order, each such s repeated ℓ_s times. We call this symbol the *slope content* of K, writing $\mathrm{SC}(K)$. Here "content" is meant to evoke "Jordan-Hölder content," because in the Galois context of §3.6, each slope s corresponds to an abelian subquotient Q^s of the Galois group G. In writing slope contents, we allow ourselves to omit 1's as subscripts and superscripts. Thus the slope content of our example field $\mathbf{Q}_2(\sqrt{-3}, \sqrt{-1}, \sqrt{2})$ is $[2, 3]_1^2 = [2, 3]^2$.

3.5. **Galois and inertia groups.** Let K^g be a splitting field over $\mathbf{Q}_p$ of our given polynomial $f(x)$ and let $G = \mathrm{Gal}(K^g/\mathbf{Q}_p)$. Similarly, let I be the inertia group $\mathrm{Gal}(K^g/K^{g,u})$.

If K is tame with residual degree f and ramification index e, then G is an extension of the cyclic group $I = C_e$ by the cyclic group $G/I = C_u$. Here u is a multiple of f computed by the following proposition.

Proposition 3.5.1. *Let $K = \mathbf{Q}_p(\zeta, \beta_{e,r})$ be a tamely ramified extension, as in Proposition 2.2.1, so that ζ is a primitive $(p^f - 1)^{\text{st}}$ root of unity and $\beta_{e,r}$ is a root of $h_{e,r}(x) = x^e - \zeta^r p$. Then, the Galois closure K^g of K is $\mathbf{Q}_p(\zeta, \beta_{e,r}, \zeta_e, \omega)$ where ζ_e is a primitive e^{th} root of unity, and ω is a primitive $\dfrac{(p^f-1)e}{\gcd((p-1)r,\, p^f-1)}$ root of unity. Moreover, $K^{g,u} = \mathbf{Q}_p(\zeta, \zeta_e, \omega)$ and the residue degree u of K^g is the smallest positive integer which satisfies the three conditions: $f \mid u$, $e \mid (p^u - 1)$, and $e \cdot (p^f - 1) \mid (p^u - 1) \cdot \gcd\big((p-1)r,\, p^f - 1\big)$.*

Proof: The extension $K/\mathbf{Q}_p(\zeta)$ is obtained by taking an e^{th} root, and so the splitting field of $h_{e,r}(x)$ over $\mathbf{Q}_p(\zeta)$ is generated by $\beta_{e,r}$ and ζ_e. The field K^g is the splitting field of $h_{e,r}(x)$ and all of its conjugates with respect to $\mathrm{Gal}(\mathbf{Q}_p(\zeta)/\mathbf{Q}_p)$. Frobenius, as a generator of $\mathrm{Gal}(\mathbf{Q}_p(\zeta)/\mathbf{Q}_p)$, takes $h_{e,r}(x)$ to $h_{e,pr}(x)$. Hence K^g contains the ratios of roots of $h_{e,pr}(x)$ by roots of $h_{e,r}(x)$, which in turn are roots of $x^e - \zeta^{r(p-1)}$. Thus, K^g contains $L = \mathbf{Q}_p(\zeta, \beta_{e,r}, \zeta_e, \omega)$. The field L contains the roots of the conjugates $h_{e,p^j r}$ of $h_{e,r}$, since their roots are roots of $h_{e,r}$ times powers of ω. Thus, $K^g = L$ and $K^{g,u}$, the unramified subfield of K^g, is then clearly $\mathbf{Q}_p(\zeta, \zeta_e, \omega)$. Finally, the three divisibility conditions correspond in order to $K^{g,u}$ containing ζ, ζ_e and ω. □

If the degree of the given tame field K is more than 11, our database just gives the general form $C_e.C_u$ of the Galois group. For $n \leq 11$, it completely identifies the Galois group, as discussed in the next paragraph. If K is a ramified degree p extensions of $\mathbf{Q}_p$, the Galois group G is always a semi-direct product $C_p : C_u$, with u given in Proposition 2.3.1.

In degrees ≤ 11, our database always gives the isomorphism type of G as a permutation group of the roots of $f(x)$ in K^g. We give G as a transitive subgroup of S_n, well-defined up to conjugation; this is exactly the sense in which permutation groups are classified in the literature. Each tabulated G is actually a link which gives information about the corresponding group. Generally, the database gives

the inertia group I as well. However in some cases, such as when I is intransitive without a standard name, the database just gives $|I|$.

It remains to explain how we compute G when K is wildly ramified of composite degree. In this case, as is typical in computing Galois groups, we usually do not compute K^g explicitly, but rather collect enough information to eliminate all but one of the finite number of possibilities for G.

One source of information is the invariants described in §3.1-§3.4. Also we only try to compute G when we have already identified the Galois group of each of the proper subfields of K. When this information does not suffice, we introduce resolvent fields L and work with them. So the L are fields built directly from K and embeddable in K^g. To keep computations feasible, it is important to keep the degree L small. Details for our five individually treated (p, n) are given in the next section.

3.6. **Galois slopes.** The constructions of §3.4 applied now to K^g give distinguished subfields $K^{g,\sigma}$ for σ of the form s or $s+$. The database gives its slope content $\mathrm{SC}(K^g)$. Usually we write $\mathrm{GSC}(K)$ instead of $\mathrm{SC}(K^g)$ and speak of the Galois slope content of K.

In this Galois setting, slopes can be described group-theoretically as follows. Define G^σ to be the subgroup of G fixing $K^{g,\sigma}$. The G^σ form a decreasing family of normal subgroups with intersection the identity subgroup. Let L be a subfield of K^g, and let H be subgroup of G fixing L. Then one has the formula $L^\sigma = L \cap K^{g,\sigma}$.

Define $Q^s = G^s/G^{s+}$. One has

$$[L^{s+} : L^s] = \frac{|HG^s|}{|HG^{s+}|} \leq \frac{|G^s|}{|G^{s+}|} = |Q^s|, \tag{6}$$

a group-theoretic interpretation of multiplicative slope multiplicity. A straightforward way of computing $\mathrm{GSC}(K)$ is to use enough resolvents so that for every s one resolvent sees all of Q^s.

One can often avoid using so many resolvents by using general ramification-theoretic facts. Well known such facts include that Q^0 is cyclic, Q^1 is cyclic with order prime to p, each wild Q^s is of the form $C_p^{\ell_s}$, and all the G^σ are normal in G. Also useful are structural facts about each Q^s as a module for the tame quotient G/G^{1+}. For example, suppose δ_s is the prime-to-p part of the denominator of s. Then the image $\overline{Q}^1$ of Q^1 in the endomorphism ring of Q^s has order δ_s. Moreover, the algebra of endomorphisms $\mathbf{F}_p[\overline{Q}^1]$ is a finite field with p^{m_s} elements, where m_s is the smallest integer such that δ_s divides $p^{m_s} - 1$. Thus whenever one sees a slope s arise, one knows right away that m_s divides ℓ_s.

3.7. **Galois mean slope.** Besides giving all the Galois slopes of K, our tables also give their weighted mean, where the weight of a Galois slope s is its additive multiplicity. Thus suppose K has Galois slope content $[s_1, \ldots, s_m]_t^u$, with the s_i, as always, given in increasing order. Then the Galois mean slope of K is

$$\mathrm{GMS}(K) = \frac{c(K^g)}{n(K^g)} = \left(\sum_{i=1}^{m} \frac{p-1}{p^i} s_{m+1-i} \right) + \frac{1}{p^m} \frac{t-1}{t}. \tag{7}$$

It is reasonable to view $\mathrm{GMS}(K)$ as the single number best measuring ramification in K^g.

4. Some details in the cases $(p,n) = (2,4)$, $(2,6)$, $(3,6)$, $(2,8)$, and $(3,9)$

The general procedure outlined in §3.4–3.6 for passing from a p-adic field K to its Galois group $\mathrm{Gal}(K^g/\mathbf{Q}_p)$ and Galois slope content $\mathrm{GSC}(K)$ has many branches. The branch taken by a particular K depends on its Galois-theoretic details. In §4.1 and §4.2, we describe all branches of the computation in the quartic and sextic cases respectively, and give summarizing tables. In §4.3 and §4.4, we present a typical branch in the octic and nonic cases respectively.

4.1. **Quartic 2-adic fields.** There are five transitive subgroups of S_4 up to conjugation. They are distinguished by their parity and the order of their centralizer in S_4. So the Galois group G associated to a quartic 2-adic field $K = \mathbf{Q}_2[x]/f_4(x)$ is determined by its discriminant class $d \in \mathbf{Q}_2^\times/\mathbf{Q}_2^{\times 2}$ and the order of $\mathrm{Aut}(K/\mathbf{Q}_2)$.

Table 4.1. Quartic transitive permutation groups

G	C_4	V_4	D_4	A_4	S_4
Parity (computed via $d \in \mathbf{Q}_2^\times/\mathbf{Q}_2^{\times 2}$)	$-$	$+$	$-$	$+$	$-$
Centralizer order (computed as $\lvert\mathrm{Aut}(K)\rvert$)	4	4	2	1	1

If $G = C_4$ or $G = V_4$, one of course has $\mathrm{GSC}(K) = \mathrm{SC}(K)$. Similarly, if $G = D_4$ one can construct the octic field K^g and use it to directly calculate $\mathrm{GSC}(K)$. If $G = A_4$ or $G = S_4$, then the resolvent cubic is cyclic or non-cyclic respectively, with Galois slope content $[\,]^3$ or $[\,]_3^2$. Here $\mathrm{SC}(K)$ already contains two wild slopes, completing the computation of $\mathrm{GSC}(K)$.

Table 4.2. Summary of the main invariants of the 59 quartic 2-adic fields. Wild slopes which are in $\mathrm{SC}(K)$ are in bold.

c	f	G	$\mathrm{GSC}(K)$	#
0	4	C_4	$[\,]^4$	1
4	1	S_4	$[\mathbf{4/3}, \mathbf{4/3}]_3^2$	1
4	2	V	$[\mathbf{2}]^2$	1
4	2	C_4	$[\mathbf{2}]^2$	1
4	2	D_4	$[2, \mathbf{2}]^2$	2
6	1	A_4	$[\mathbf{2}, \mathbf{2}]^3$	1
6	1	D_4	$[\mathbf{2}, \mathbf{2}]^2$	2
6	2	V	$[\mathbf{3}]^2$	2
6	2	C_4	$[\mathbf{3}]^2$	2
6	2	D_4	$[2, \mathbf{3}]^2$	2
8	1	V	$[\mathbf{2}, \mathbf{3}]$	4
8	1	D_4	$[\mathbf{2}, \mathbf{3}]^2$	2
8	1	S_4	$[\mathbf{8/3}, \mathbf{8/3}]_3^2$	2
9	1	D_4	$[\mathbf{2}, 3, \mathbf{7/2}]$	8
10	1	D_4	$[2, \mathbf{3}, \mathbf{7/2}]$	8
11	1	D_4	$[\mathbf{3}, \mathbf{4}]^2$	4
11	1	C_4	$[\mathbf{3}, \mathbf{4}]$	8
11	1	D_4	$[2, \mathbf{3}, \mathbf{4}]$	8

4.2. **Sextic 2-adic and 3-adic fields.** There are 16 transitive subgroups of S_6 up to conjugation, 12 of which are solvable (see, e.g., [BM]). Parities and centralizer orders do not suffice to distinguish the 12 candidates for G, unlike the case for quartics.

However, one can use the non-trivial outer automorphism of S_6 to look at the twin group G^t, which is a perhaps non-transitive subgroup of S_6 [Ro]. Then, the

TABLE 4.3. Solvable sextic transitive permutation groups. T10 = $C_3^2 : C_4$ and T13 = $C_3^2 : D_4$ are self-twin. Otherwise, the G^t are all intransitive, with the corresponding partition of six being given by the subscripts.

G	T1	T2	T3	T4	T5	T6
Twin group G^t	$C_3C_2C_1$	$S_3C_1^3$	$S_3C_2C_1$	$A_4C_1^2$	S_3C_3	A_4C_2
Parity	$-$	$-$	$-$	$+$	$-$	$-$

G	T7	T8	T9	T10	T11	T13
Twin group G^t	$S_4^+C_2$	$S_4C_1^2$	S_3S_3	T10	S_4C_2	T13
Parity	$+$	$-$	$-$	$+$	$-$	$-$

partition of six one obtains gives more than enough information to distinguish the twelve G, as indicated by Table 4.3.

On the level of fields, given K we immediately compute the twin sextic algebra K^t and factor it; this twin sextic algebra is given in the database as a special feature for sextics. The two ambiguities are distinguished by the parities of the groups: T7 is even while T11 is odd, and T10 = $C_3^2 : C_4$ is even while T13 = $C_3^2 : D_4$ is odd.

To compute the Galois slope content $\mathrm{GSC}(K)$ we distinguish two cases, according to whether K^t factors or not. If K^t factors then there are at most two factors different from $\mathbf{Q}_p$. If there is just one such factor L, then $\mathrm{GSC}(K) = \mathrm{GSC}(L)$ and we are done. Suppose there are two factors L' and L'' with Galois slope contents $[S']_{t'}^{u'}$ and $[S'']_{t''}^{u''}$. If S' and S'' are disjoint then $\mathrm{GSC}(K)$ is computed as $[S' \cup S'']_{\mathrm{lcm}(t',t'')}^{u}$. Here $\mathrm{lcm}(u', u'')$ divides u which in turn divides $\mathrm{lcm}(u', u'')\gcd(t', t'')$. Determining the correct u is a simple matter not involving wild ramification. When S' and S'' are not disjoint then the correct wild slopes are those appearing in the degree 8 or degree 9 field $L' \otimes L''$. Finally, if K^t doesn't factor one must have $G = C_3^2 : C_4$ or $G = C_3^2 : D_4$. This can occur only for $p = 3$ with C_3^2 the wild ramification subgroup. Since C_4 and D_4 each act irreducibly on C_3^2, the single visible Galois slope must also coincide with the hidden Galois slope.

4.3. **An octic 2-adic example.** We illustrate our general procedure of computing Galois groups and Galois slope content with the polynomial

$$f_8(x) = x^8 - 4x^4 + 4x^2 - 2.$$

Throughout, we subscript fields by their degree and superscript them by their discriminant exponent as in (5), and so in particular we have $K = K_8^{25} = \mathbf{Q}_2[x]/f_8(x)$.

The element $y = x^2$ of K_8^{25} generates a quartic subfield $K_4^8 = \mathbf{Q}_2[y]/f_4(y)$ with

$$f_4(y) = y^4 - 4y^2 + 4y - 2.$$

The complete list of subfields is

$$K_1^0 \subset K_4^8 \subset K_8^{25},$$

and so the slope content of K_8^{25} is $[8/3, 8/3, 17/4]$.

Construct a resolvent field for K_8^{25} as follows. Let $\pm\alpha$, $\pm\beta$, $\pm\gamma$, $\pm\delta$ be the complex roots of $f_8(x)$. Form the monic octic polynomial $g_8(x)$ with complex roots

TABLE 4.4. Summary of the main invariants of the 47 sextic 2-adic fields and the 75 sextic 3-adic fields. Galois groups are described in their twin form to emphasize that most of these fields can be directly built from fields of lower degree. Wild slopes which are in $\mathrm{SC}(K)$ are in bold.

Sextic 2-adic fields				
c	f	G^t	$\mathrm{GSC}(K)$	#
0	6	C_3C_2	$[\,]^6$	1
4	2	S_3	$[\,]_3^2$	1
4	2	S_3C_3	$[\,]_3^6$	1
6	1	S_4	$[4/3, \mathbf{4/3}]_3^2$	1
6	3	C_3C_2	$[\mathbf{2}]^2$	2
6	3	$S_4^+C_2$	$[4/3, \mathbf{4/3}]_3^2$	1
6	3	A_4	$[2, \mathbf{2}]^3$	1
6	3	A_4C_2	$[2, \mathbf{2}]^6$	1
6	3	A_4C_2	$[2, 2, \mathbf{2}]^3$	2
8	1	S_3C_2	$[\mathbf{2}]_3^2$	2
8	1	S_4C_2	$[4/3, 4/3, \mathbf{2}]_3^2$	2
9	3	C_3C_2	$[\mathbf{3}]^3$	4
9	3	A_4C_2	$[2, 2, \mathbf{3}]^3$	4
10	1	$S_4^+C_2$	$[8/3, \mathbf{8/3}]_3^2$	2
10	1	S_4	$[8/3, \mathbf{8/3}]_3^2$	2
10	1	S_4C_2	$[2, 8/3, \mathbf{8/3}]_3^2$	4
11	1	S_3C_2	$[\mathbf{3}]_3^2$	4
11	1	S_4C_2	$[4/3, 4/3, \mathbf{3}]_3^2$	4
11	1	S_4C_2	$[8/3, 8/3, \mathbf{3}]_3^2$	8

Sextic 3-adic fields				
c	f	G^t	$\mathrm{GSC}(K)$	#
0	6	C_3C_2	$[\,]^6$	1
3	3	C_3C_2	$[\,]_2^3$	2
6	1	$C_3^2:D_4$	$[5/4, \mathbf{5/4}]_4^2$	2
6	2	S_3C_2	$[\mathbf{3/2}]_2^2$	2
6	2	$C_3^2:D_4$	$[3/2, \mathbf{3/2}]_2^2$	2
6	2	S_3^2	$[3/2, \mathbf{3/2}]_2^2$	1
7	1	S_3	$[\mathbf{3/2}]_2$	2
7	1	S_3C_2	$[\mathbf{3/2}]_2^2$	2
7	1	S_3C_3	$[\mathbf{3/2}]_2^3$	2
8	2	C_3C_2	$[\mathbf{2}]^2$	3
8	2	S_3	$[\mathbf{2}]^2$	1
8	2	S_3C_3	$[\mathbf{2}]^6$	1
8	2	S_3C_3	$[2, \mathbf{2}]^2$	3
8	2	$C_3^2:C_4$	$[2, \mathbf{2}]^4$	2
9	1	C_3C_2	$[\mathbf{2}]_2$	6
9	1	S_3C_2	$[\mathbf{2}]_2^2$	2
9	1	S_3C_3	$[3/2, \mathbf{2}]_2$	6
9	1	S_3S_3	$[3/2, \mathbf{2}]_2^2$	2
10	1	$C_3^2:D_4$	$[9/4, \mathbf{9/4}]_4^2$	6
10	2	S_3C_2	$[\mathbf{5/2}]_2^2$	3
10	2	S_3^2	$[3/2, \mathbf{5/2}]_2^2$	3
11	1	S_3C_2	$[\mathbf{5/2}]_2^2$	3
11	1	S_3	$[\mathbf{5/2}]_2$	3
11	1	S_3C_3	$[\mathbf{5/2}]_2$	3
11	1	S_3S_3	$[2, \mathbf{5/2}]_2^2$	3
11	1	S_3C_3	$[2, \mathbf{5/2}]_2$	9

$(\alpha \pm \beta \pm \gamma \pm \delta)^2/2$. Then one has

$$g_8(x) = x^8 + 16x^6 + 64x^5 + 368x^4 + 512x^3 + 384x^2 + 512x + 576.$$

The polynomial $g_8(x)$ is irreducible over $\mathbf{Q}_2$ defining a field L_8^{26}. The complete list of subfields is

$$L_1^0 \subset L_2^3 \subset L_8^{26},$$

and so the slope content of L_8^{26} is $[3, 23/6, 23/6]$.

Now the largest the Galois group G can be is the wreath product $2 \wr S_4 = 2^4 : S_4$ and so one has $|G| \leq 2^7 \cdot 3$. The polynomial discriminant of $f_4(y)$ is $-2^8 11$ giving

the discriminant class $*$, as $\mathbf{Q}_2(\sqrt{-2^8 11})$ is unramified over $\mathbf{Q}_2$. So 2 divides $|Q^0|$. Since 3 divides the denominator of a slope, 3 divides $|Q^1|$. Since we have found six wild slopes, our analysis concludes with

$$(8)\quad \mathrm{Gal}(K^g/\mathbf{Q}_2) = 2^4 : S_4 = \mathrm{T44} \quad \text{and} \quad \mathrm{GSC}(K) = \left[2\frac{2}{3},\ 2\frac{2}{3},\ 3,\ 3\frac{5}{6},\ 3\frac{5}{6}, 4\frac{1}{4}\right]_3^2.$$

4.4. **A nonic 3-adic example.** When a slope occurs to high multiplicity, the situation can be more subtle to analyze. Consider in general a nonic 3-adic field K_9 with a 3-adic subfield K_3. Applying the resolvent construction of [JR2, Eq. 10], one gets a nonic 3-adic algebra K_{9x} also containing K_3. Applying the same resolvent construction again, one gets a third nonic 3-adic algebra K_{9xx}, also containing K_3. If K_{9xx} is a field, then the orders of the corresponding Galois groups G, G_{9x}, G_{9xx} are exactly divisible by 3^4, 3^3, and 3^2 respectively. At issue is to determine the four slopes $s_1 \le s_2 \le s_3 \le s_4$ corresponding to the factors of 3 in $|G|$.

Let $v_1 \le v_2$ be the two slopes of K_{9xx}. Let v_3 be the largest slope of K_{9x} and let v_4 be the largest slope of K_9. If the v_i are all distinct, then it is obvious that they form the desired Galois slopes of K. Two explicit examples of this situation can be extracted from Table 6.2 of [JR2].

Now consider the example $K = K_9^9$ defined by

$$f_9(x) = x^9 - 2x^6 + 2.$$

The element $y = x^3$ generates the unramified cubic subfield K_3^0. The fields K_{9x}^9 and K_{9xx}^9 are respectively defined by

$$f_{9x}(x) = x^9 - 9x^7 - x^6 + 27x^5 + 6x^4 - 28x^3 - 9x^2 + 3x - 1,$$
$$f_{9xx}(x) = x^9 - x^6 + x^3 + 1.$$

In this example, (v_1, v_2, v_3, v_4) are readily computed to be $(0, 3/2, 3/2, 3/2)$. So the question is whether the wild slope $3/2$ actually has multiplicity three, or whether there are some hidden wild slopes s strictly less than $3/2$.

The answer given in [JR2] says that in fact always $v_2 \le v_3 \le v_4$ and always repetitions truly correspond to multiplicities. This is because G has just one normal subgroup of order 3 and one normal subgroup of order 9, the kernels of $G \to G_{9x}$ and $G \to G_{9xx}$ respectively. This uniqueness forces that it is always the largest slope which disappears at each step of the resolvent construction.

Since K_3^0 is unramified, one has $\mathrm{Gal}(K_3^0/\mathbf{Q}_3) \cong A_3$ and 3 divides $|Q^0|$. Since 2 divides the denominator of a wild slope, we know 2 divides $|Q^1|$. From Table 3.2 of [JR2], there is then only one possibility for the Galois group $G = \mathrm{Gal}(K^g/\mathbf{Q}_3)$. Our analysis of K concludes with the identifications

$$(9)\qquad \mathrm{Gal}(K^g/\mathbf{Q}_3) = [3^3 : 2]3 = \mathrm{T22} \quad \text{and} \quad \mathrm{GSC}(K) = \left[1\frac{1}{2},\ 1\frac{1}{2},\ 1\frac{1}{2}\right]_2^3.$$

5. Interactive features of the database and global applications

Our database has two interactive features, the *p-adic identifier* and the *GRD calculator*. We describe these in §5.1 and §5.2 respectively. In §5.3 we indicate the role our database plays in three applications; [APSo] and [APSi] use the p-adic identifier and [JR4] uses the GRD calculator.

5.1. **The p-adic identifier.** The p-adic identifier lets one input a polynomial $f(x) \in \mathbf{Z}[x]$ and a prime p. It uses `gp` to factor the polynomial over $\mathbf{Q}_p$ to high p-adic precision, and then uses Panayi's root finding algorithm to identify each factor. It returns the entries from the database corresponding to the factor fields of $\mathbf{Q}_p[x]/f(x)$. As simple examples, inputting $(f_8(x), 2)$ and $(f_9(x), 3)$ yields the conclusions (8) of §4.3 and (9) of §4.4 respectively.

5.2. **The GRD calculator.** A single numerical measure of ramification in a polynomial $f(x) \in \mathbf{Z}[x]$ is the root discriminant of its splitting field in $\mathbf{C}$, what we call its Galois root discriminant. The GRD calculator accepts a polynomial $f(x) \in \mathbf{Z}[x]$ as input. When all factors of all completions of $\mathbf{Q}[x]/f(x)$ are in the database, it returns lower and upper bounds on the Galois mean slope β_p of each ramifying prime p, and hence bounds on the Galois root discriminant $\prod p^{\beta_p}$. In favorable cases, certainly when the p-adic algebra has only one wild factor, the lower and upper bounds on β_p agree. In the remaining cases, it is typically easy to start with the bounds and continue by hand to exactly determine β_p. As simple examples, the polynomials $f_8(x)$ and $f_9(x)$ from §4.3 and §4.4 have global Galois groups $2^4 : S_4$ and $T24$ of order 384 and 324 respectively. The GRD calculator yields $2^{373/96}11^{1/2} \approx 49.01$ and $2^{8/9}3^{79/54}11^{1/2} \approx 30.64$ for the respective Galois root discriminants.

5.3. **Sample global applications.** The paper [APSo] searches in parametrized families of $SL_3(2)$ number fields, extracting those number fields which meet certain local conditions. Then it finds automorphic cohomology classes on GL_3 which numerically match these number fields, the weight of the matching class being governed by the local behavior of 2 in the number field. The paper [APSi] finds A_6 fields which embed in $3.A_6$ fields and finds automorphic cohomology classes on GL_3 which numerically match the $3.A_6$ fields. Here the local behavior of the prime 3 governs the more complicated obstructions to the embedding problem. The paper [JR4] finds all Galois fields K with certain given Galois groups and root discriminants less than certain bounds.

All three of these papers use our database repeatedly, but none of them enter into the corresponding detailed local analyses. This is exactly in keeping with the philosophy we put forth in §1.1: the goal of the database is to make as many local issues as possible utterly routine, so that attention can be focused elsewhere.

References

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

[APSo] Ash A., Pollack D., Soares, D., 2004. $\mathrm{SL}_3(\mathbb{F}_2)$-extensions of $\mathbb{Q}$ and arithmetic cohomology modulo 2. Experiment. Math. 13 no. 3, 298–307.

[APSi] Ash A., Pollack D., Sinnott W., 2004. A_6-extensions of $\mathbf{Q}$ and the mod p cohomology of $GL(3, \mathbf{Z})$. J. Number Theory, in press.

[BR] Bayer, P., Rio, A., 1999. Dyadic exercises for octahedral extensions. J. Reine Angew. Math. 517, 1–17.

[BM] Butler, G., McKay, J., 1983. The transitive groups of degree up to eleven. Comm. Algebra, 11(8), 863–911.

[CP] Conner, P. E., Perlis, R., 1984. A survey of trace forms of algebraic number fields. Vol. 2 of Series in Pure Mathematics. World Scientific Publishing Co., Singapore.

[D] Deligne, P., 1976. Les constantes locales de l'équation fonctionnelle de la fonction L d'Artin d'une représentation orthogonale. Invent. Math. 35, 299–316.

[E] Epkenhans, M., 1989. Trace forms of dyadic number fields. J. Number Theory 38, 359–365.

[HL] Heath, L. S., Loehr, N. A., 1999. New algorithms for generating Conway polynomials over finite fields. In: Proceedings of the Tenth Annual ACM-SIAM Symposium on Discrete Algorithms (Baltimore, MD, 1999). ACM, New York, 429–437.

[JR1] Jones, J. W., Roberts, D. P., 1999. Sextic number fields with discriminant $(-1)^j 2^a 3^b$. In: Number theory (Ottawa, ON, 1996). Vol. 19 of CRM Proc. Lecture Notes. Amer. Math. Soc., Providence, RI, 141–172.

[JR2] Jones, J. W., Roberts, D. P., 2004. Nonic 3-adic fields. In: Algorithmic Number Theory (ANTS-VI). Springer LNCS 3076, 293–308.

[JR3] Jones, J. W., Roberts, D. P. Octic 2-adic fields, in preparation.

[JR4] Jones, J. W., Roberts, D. P. Galois number fields with small root discriminant, submitted.

[Kr] Krasner, M., 1979. Remarques au sujet d'une note de 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 288 (18), A863–A865.

[Na] Naito, H., 1995. Dihedral extensions of degree 8 over the rational p-adic fields. Proc. Japan Acad. Ser. A Math. Sci. 71 (1), 17–18.

[Pa] Panayi, P., 1995. Computation of Leopoldt's p-adic regulator. Ph.D. thesis, University of East Anglia.

[PARI2] PARI2, 2004. PARI/GP, version `2.1.6`. The PARI Group, Bordeaux, available from `http://pari.math.u-bordeaux.fr/`.

[PR] Pauli, S., Roblot, X.-F., 2001. On the computation of all extensions of a p-adic field of a given degree. Math. Comp. 70 (236), 1641–1659.

[Ro] Roberts, D. P., 1998. Twin sextic algebras. Rocky Mountain J. Math. 28 (1), 341–368.

[Se1] Serre, J.-P., 1979. Local Fields. Springer Verlag, New York.

[Se2] Serre, J.-P., 1978. 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 (22), A1031–A1036.

[Se3] Serre, J.-P., 1984. L'invariant de Witt de la forme $\mathrm{Tr}(x^2)$, Comment. Math. Helv. 59 no. 4, 651–676.

[T] Tate, J. T., 1977. Local constants. In: Algebraic number fields: L-functions and Galois properties (Proc. Sympos., Univ. Durham, Durham, 1975). Academic Press, London, 89–131, prepared in collaboration with C. J. Bushnell and M. J. Taylor.

[We] Weil, A., 1974. Exercices dyadiques. Invent. Math. 27, 1–22.