THE GENERALIZED FERMAT EQUATION $x^3 + y^3 = z^n$

MANVIR JASWAL

ABSTRACT. We prove that the equations $x^3+y^3 = z^n$ and $x^3+y^3 = 3z^n$ have no solution in coprime nonzero integers for any $n \geq 3$. For the first equation the open cases were prime exponents $p \equiv 1 \pmod 3$ above 10^9 outside a set of congruence classes treated by Chen and Siksek; in these cases the solution $1^3 + 2^3 = 3^2$ blocks the modular method. We replace Kraus's Frey curve by a hypergeometric motive of rank three over $K = \mathbb{Q}(\sqrt{-3})$, whose parameter at a solution is 3-adically close enough to a point of maximally unipotent monodromy for inertia at $\sqrt{-3}$ to act unipotently; the parameter of $1^3 + 2^3 = 3^2$ is not. By a theorem of Calegari, Emerton and Gee, the mod p representation of the fiber, twisted by a cubic character, is the reduction of a member of a compatible system of minimal ramification, and we show that the member at a prime above 3 is irreducible and ordinary at $\sqrt{-3}$. Ramification and unconditional discriminant bounds show that its reductions have trivial semisimplification, and as the Galois group of the maximal pro-3 extension of K unramified outside $\sqrt{-3}$ is generated by one inertia group, the member stabilizes its ordinary line, a contradiction. For $x^3 + y^3 = 3z^n$ the same argument also works at the primes $p \equiv 2 \pmod 3$, which are inert in K, and Frey curves and descents treat the remaining exponents.

2020 *Mathematics Subject Classification.* Primary 11D41; Secondary 11F80, 11R29, 11R42, 14D05, 11G25.

Key words and phrases. Generalized Fermat equation, Frey representations, hypergeometric motives, compatible systems of Galois representations, ordinary representations, local generation, discriminant bounds.

How AI was used in this work is described under Declarations, p. 101.

Contents

1. Introduction 2
2. Conventions 9

Part I: a Frey motive of rank three over $\mathbb{Q}(\sqrt{-3})$ 10
3. The Frey motive 10
4. Inertia at the prime above 3 16
5. The Frey representation of a solution 30
6. Irreducibility 38

Part II: a compatible system and its members above 5 39
7. A compatible system of minimal ramification 39
8. The member at 5: ramification, discriminants, groups and fields 49
9. The reductions modulo 5 53

Part III: the member at 3, and the proof of Theorem A 58
10. The member at 3 58
11. The reductions of the member at 3, and the proof of Theorem A 61

Part IV: the equation $x^3 + y^3 = 3z^n$ 76
12. The equation $x^3 + y^3 = 3z^n$ 76

Complements 98
13. Remarks 98
Appendix A. Computations 99
Declarations 101
References 101

1. Introduction

1.1. **The equation.** A solution of $x^3 + y^3 = z^n$ in *coprime nonzero integers* is a triple (a, b, c) of nonzero integers with $\gcd(a, b, c) = 1$ and $a^3 + b^3 = c^n$. For $n = 2$ there are such solutions, for example $1^3 + 2^3 = 3^2$. For $n \geq 3$ none is known, and none is expected. The case $n = 3$ is Euler's. For prime exponents $p \geq 17$ the equation has been attacked by the modular method since Darmon and Granville [37, Proposition 4.4], who attached to a solution a Frey curve and, assuming the Shimura–Taniyama conjecture, excluded solutions with c even. Kraus [80] wrote this curve as

$$E_{a,b}\colon\ Y^2 = X^3 + 3abX + b^3 - a^3$$

and proved that there is no solution for $17 \leq p < 10^4$, and Dahmen [35, §3.3.2] extended his argument to $p = 5, 7, 11, 13$. Chen and Siksek proved that there is no solution for $3 \leq n \leq 10^9$ [30, Theorem 2], and none for the prime exponents in a set of Dirichlet density 28219/44928 [30, Theorem 1 and §10]. Freitas [58, Theorem 3] proved that there is no solution for any prime $p \equiv 2 \pmod 3$ with $p \geq 17$. Bennett and Das [15] proved that for every solution (a, b, c) with $n \geq 3$ the greatest prime divisor of $a - b$ exceeds 10^{12}. What these results leave open is the set of primes $p \equiv 1 \pmod 3$ above 10^9 outside the congruence classes of Chen and Siksek.

The obstruction is the Catalan solution $1^3 + 2^3 = 3^2$. For every prime $p \geq 17$ and every solution of $x^3 + y^3 = z^p$, the mod p representation of Kraus's Frey curve is isomorphic to that of the elliptic curve $W = E_{2,1}\colon Y^2 = X^3 + 6X - 7$ of conductor 72 (Cremona label 72a1), the Frey curve of $2^3 + 1^3 = 3^2$, or to that of its quadratic twist by -1; in Kraus's normalization of the solution, a choice of the order of a, b and of the sign of (a, b, c), it is that of W [80, Théorème 6.1 and Proposition 6.3]. We refer to this isomorphism as *Kraus's congruence*. So the modular method, with this Frey curve, cannot conclude by comparing Hecke eigenvalues: W is a genuine elliptic curve whose mod p representation imitates that of a solution. Freitas separated the two for $p \equiv 2 \pmod 3$ by comparing symplectic types, for the twists by -3 of the two curves: a criterion he proved at 2 shows that the isomorphism is symplectic, and the criterion of Kraus and Oesterlé at the multiplicative prime 3 shows that it is symplectic only if -3 is a square modulo p [58, §2]. When $p \equiv 1 \pmod 3$ the two criteria agree. As Billerey, Chen, Dieulefait and Freitas put it [23, Remark 1.7], the Catalan solution $2^3 + 1^3 = 3^2$ "currently prevents the modular method from proving" such results for $x^3 + y^3 = z^p$.

1.2. **The results.**

Theorem A. *For every integer $n \geq 3$, the equation $x^3 + y^3 = z^n$ has no solution in coprime nonzero integers.*

For $3 \leq n \leq 10^9$ this is due to Chen and Siksek [30, Theorem 2], and for the prime exponents $p \equiv 2 \pmod 3$ with $p \geq 17$ to Freitas [58, Theorem 3]. We prove the case of every prime exponent $p \equiv 1 \pmod 3$ with $p \geq 17$ (Theorem 11.18), which contains the cases left open, and Theorem A is Corollary 11.19. Section 1.7 lists the published results on which the proof rests.

The proof replaces Kraus's Frey curve by a Frey motive of rank three over $K = \mathbb{Q}(\sqrt{-3})$. At a solution the parameter of the motive is 3-adically so close to a point of maximally unipotent monodromy that inertia at $\sqrt{-3}$ acts unipotently on the fiber, whereas the parameter of $1^3 + 2^3 = 3^2$ is farther away. By a theorem of Calegari, Emerton and Gee, the mod p representation of the fiber, twisted by a cubic character, is the reduction of a member of a compatible system of minimal ramification. We show that the member of that system at a prime above 3 is irreducible and ordinary at $\sqrt{-3}$. This member is unramified outside $\sqrt{-3}$, and its ramification there is so small that, by Odlyzko's discriminant bounds and finite group theory, every reduction of it has trivial semisimplification. As the Galois group of the maximal pro-3 extension of K unramified outside $\sqrt{-3}$ is generated by one inertia group, the member then stabilizes its ordinary line, a contradiction (Section 1.5).

For the coefficient 3 the obstruction is the same curve W: the Catalan solution can be read as $2^3 + 1^3 = 3 \cdot 3$, a point of $x^3 + y^3 = 3z^n$ with $n = 1$, and $2^3 + 1^3 = 9 \cdot 1^n$ is a solution of $x^3 + y^3 = 9z^n$ for every n.

Theorem B. *For every integer $n \geq 3$, the equation $x^3 + y^3 = 3z^n$ has no solution in coprime nonzero integers.*

This is Theorem 12.1, whose case $n = 3$ is classical. The prime exponents $p \equiv 3 \pmod 4$ with $p \geq 7$ come from Freitas's symplectic argument applied to a twist of Kraus's Frey curve, the prime exponents $7 \leq p < 10^8$ from a criterion of Kraus's type checked by computer (Theorem 12.2), and the exponents 4 and 5 from descents in the manner of Bruin [26] (Theorem 12.3). The prime exponents $p \geq 17$ also come from the method of Theorem A, which for $p \equiv 2 \pmod 3$ is carried out at a prime that is inert in $K = \mathbb{Q}(\sqrt{-3})$ (Theorem 12.4).

At such a prime the compatible system comes from a lifting lemma (Lemma 12.21), whose proof is that of a lifting theorem of Bellovin and Gee [13, Theorem 5.2.1] written out for this case. Theorem A does not use this lemma, and Theorem B depends on it only for the exponents $n \geq 3$ that are divisible neither by 3 nor by 4 and whose prime factors $p \geq 5$ all satisfy $p \equiv 5 \pmod{12}$ and $p > 10^8$ (see the proof of Theorem 12.1). For $n = 2$ there are solutions, such as $11^3 + (-2)^3 = 3 \cdot 21^2$. The equation $x^3 + y^3 = 9z^4$, which besides $2^3 + 1^3 = 9 \cdot 1^4$ has the solution $71^3 + (-23)^3 = 9 \cdot 14^4$, remains open (Remark 12.5).

1.3. **The Frey motive.** Let $K = \mathbb{Q}(\omega) = \mathbb{Q}(\sqrt{-3})$, where ω is a primitive cube root of unity, let $\mathcal{O} = \mathbb{Z}[\omega]$ be its ring of integers and $\mathfrak{p} = (\sqrt{-3})$ its prime above 3, and let ζ_9 be a primitive ninth root of unity; then $K(\zeta_9) = \mathbb{Q}(\zeta_9)$. For $s \neq 0, 1$ consider the affine surface

$$Z_s \colon \ (1 - y_0^9)(1 - y_1^9)(1 - y_2^9) = s$$

with the action of μ_9^3 by multiplication on the coordinates. It has a twisted form X_s over K, which becomes Z_s over $\overline{K}$ but on which G_K also permutes the three coordinates cyclically, through $\mathrm{Gal}(\mathbb{Q}(\zeta_9)/K)$ (Section 3); without this permutation no character of order 9 on each factor of μ_9^3 would be fixed by G_K. A character χ of μ_9^3 that has order 9 on each factor and is fixed by G_K cuts out of the cohomology H_c^2 of the surfaces X_s a local system $\mathbb{V}$ of rank three on $\mathbb{P}^1 \smallsetminus \{0, 1, \infty\}$ over K. Geometrically $\mathbb{V}$ is the hypergeometric local system with local exponents $\{1/9, 4/9, 7/9\}$ (up to a common sign) at $s = \infty$ and $\{0, 0, 0\}$ at $s = 0$. Its local monodromy is unipotent with one Jordan block at 0 (so $s = 0$ is a point of maximally unipotent monodromy), is a pseudo-reflection of order 3 at 1, and is semisimple with eigenvalues $\zeta_9, \zeta_9^4, \zeta_9^7$, or their inverses, at ∞, so that its cube is a scalar. The field K is forced by the exponents: $\{1/9, 4/9, 7/9\}$ is stable under multiplication by 4 and 7 modulo 1, but not by -1, so the local system is defined over the fixed field $\mathbb{Q}(\sqrt{-3})$ of $\{1, 4, 7\} \subset (\mathbb{Z}/9)^\times$ and not over $\mathbb{Q}$.

To a solution (a, b, c) of $x^3 + y^3 = z^p$ we attach the parameter

$$s_0 = \frac{c^p}{u^3} = 1 + \Big(\frac{w}{u}\Big)^3, \qquad \{u, w\} = \{a, b\},\ p \nmid u,$$

and the *Frey representation* $\rho = \mathbb{V}_{s_0} \otimes \kappa_u^{-n_\infty}$ of G_K (after Darmon's Frey representations [36]), where κ_u is the cubic Kummer character of u. Here $n_\infty \in \{1, 2\}$ is given by the local monodromy at ∞, which factors through a quotient μ_9 of the inertia group there: its cube is a scalar, so the subgroup $\mu_3 \subset \mu_9$ acts on $\mathbb{V}$ by scalars, $\zeta \mapsto \zeta^{n_\infty}$ (Proposition 3.3). The reduction of ρ modulo p is the *residual Frey representation* $\bar{\rho}$. Let $\mathfrak{q} \nmid 3p$ be a prime of K dividing abc. If $\mathfrak{q} \mid c$, then $v_\mathfrak{q}(s_0) = p\, v_\mathfrak{q}(c) \equiv 0 \pmod{p}$, and inertia at $\mathfrak{q}$ acts through a power of the unipotent monodromy at 0 with exponent divisible by p, which is trivial modulo p. If $\mathfrak{q} \mid w$, then $v_\mathfrak{q}(s_0 - 1) = 3v_\mathfrak{q}(w) \equiv 0 \pmod{3}$, and inertia acts through a power of the pseudo-reflection of order 3 at 1 with exponent divisible by 3, which is trivial. If $\mathfrak{q} \mid u$, then $v_\mathfrak{q}(s_0) = -3v_\mathfrak{q}(u) \equiv 0 \pmod{3}$, and inertia acts through a power of the monodromy at ∞ with exponent divisible by 3, a scalar that the twist removes. So $\bar{\rho}$ is unramified outside $3p$; it is conjugate self-dual up to the twist by the inverse square of the mod p cyclotomic character, and at the primes above p it is the reduction of a crystalline representation with Hodge–Tate weights $\{0, 1, 2\}$ (Section 5). It is irreducible (Section 6).

1.4. **Why the obstruction disappears.** For Kraus's curve the separation fails at 3: both $E_{a,b}$ and W have potentially multiplicative reduction at 3, with Tate parameters of valuations $2p\, v_3(c) - 3$ and 1, both prime to p, so their mod p representations have the same shape at 3. The rank-three motive is more sensitive. Its parameter at a solution is 3-adically very close

to the maximally unipotent point: $v_3(s_0) = p\, v_3(c) \geq p$, because $3 \mid c$ by a theorem of Kraus. We prove (Theorem 4.1) that inertia at the prime $\mathfrak{p}$ acts unipotently on $\mathbb{V}_s$ for every s in the punctured disc $v_3(s) > 15/2$. The radius has a simple origin: $\mathbb{V}$ is a triple multiplicative convolution of Kummer sheaves of $1-x$ of order 9, the binomial series of $(1-x)^{1/9}$ converges exactly on $v_3(x) > 5/2$, and $15/2 = 3 \cdot 5/2$. The Catalan solution $1^3 + 2^3 = 3^2$ sits at $s = 9$, with $v_3(s) = 2$: outside the disc.

Two further ingredients of Part I are computations at the two primes of K above 7. The irreducibility of $\bar{\rho}$ comes from the Frobenius polynomials at these primes of the fiber $\mathbb{V}_2$ of $\mathbb{V}$ at $s = 2$: Kraus's congruence forces $7 \nmid abc$ and $s_0 \equiv 2 \pmod 7$ (Proposition 5.1 (c), Lemma 5.2), and 7 is the smallest prime ℓ at which it confines s_0 to a single point of $\mathbb{P}^1(\mathbb{F}_\ell)$ other than 0, 1 and ∞. And the unipotence at $\mathfrak{p}$ needs, after the geometry, one arithmetic input: the character by which G_K acts on the line of invariants of the local monodromy in the fiber of $\mathbb{V}$ at the tangential base point $\partial/\partial s$ at $s = 0$ must be trivial. This character has order dividing 3 and is unramified outside $\mathfrak{p}$, and a cubic character of $K_\mathfrak{p}^\times$ is trivial on $1 + \mathfrak{p}^4$, where the binomial series of $(1+x)^{1/3}$ converges. So it is a character of the ray class group of K modulo $\mathfrak{p}^4$, and again its triviality is decided at the two primes above 7 (Section 4.4).

Theorem 4.1 is a statement about $\mathbb{V}$ alone, not about the equation, and it also says how the decomposition group at $\mathfrak{p}$ acts: up to semisimplification, through 1, ε_ℓ^{-1} and ε_ℓ^{-2}, for every prime $\ell \neq 3$. At a prime $\mathfrak{q} \nmid 3\ell$, inertia acts unipotently on $\mathbb{V}_s$ for every $s \in K$ with $v_\mathfrak{q}(s) > 0$, by tame ramification (Lemma 5.3); but $\mathfrak{p}$ divides the denominator 9 of the exponents of $\mathbb{V}$. The description of inertia for hypergeometric motives of rank two by Golfieri Madriaga, Pacetti and Rodriguez-Villegas excludes such primes, and they write that "it would be interesting to have an explicit description for wild primes" [66, §1]. The theorem is proved in Section 4 without a semistable model. Part IV uses it again, for the solutions of $x^3 + y^3 = 3^k z^p$ with $3 \mid z$ or $k \geq 8$ (Proposition 12.19). We do not know whether the radius $15/2$ is optimal; for the Legendre family at 2 and the Hesse family at 3, convolutions of two Kummer sheaves, the same argument gives exactly the part near 0 of the locus of potentially multiplicative reduction (Remark 4.17).

1.5. **The proof of Theorem A.** Let $p \geq 17$ be a prime with $p \equiv 1 \pmod 3$, and suppose that a solution exists. By a theorem of Calegari, Emerton and Gee [27, Theorem 4.2.11], $\bar{\rho}$ lifts to a representation that belongs to a *compatible system* $\{R_\lambda\}$: a family of three-dimensional representations R_λ of G_K, the *members* of the system, one for each prime λ of a number field, with the same characteristic polynomials of Frobenius at almost all primes. The system can be chosen polarized, with Hodge–Tate weights $\{0, 1, 2\}$, and with minimal ramification: each member is unramified outside $\mathfrak{p}$ and the primes above its residue characteristic (Part II). At $\mathfrak{p}$ the members have, up to Frobenius semisimplification, a common Weil–Deligne representation, on which inertia acts through a character of order dividing 3 and whose monodromy is a nilpotent matrix N (Propositions 7.8 and 10.5). The member at a prime above p, the *p-adic member*, lifts $\bar{\rho}$. Step (1) uses the members at the primes above 5, and steps (3)–(5) the member R at a prime above 3 (Part III), which is unramified outside $\mathfrak{p}$ because $\mathfrak{p}$ is the only prime of K above 3. The proof has five steps.

(1) *$N \neq 0$, and $\bar{\rho}(I_\mathfrak{p})$ is not scalar.* If N were zero, inertia at $\mathfrak{p}$ would act through scalars on the reductions modulo 5 of the members at the primes above 5. A reduction that is a sum of three characters is excluded by the class numbers of $K(\sqrt{5})$ and $K(\zeta_5)$: the characters would be 1, $\bar{\varepsilon}_5^{-1}$, $\bar{\varepsilon}_5^{-2}$, with $\bar{\varepsilon}_5$ the cyclotomic character modulo 5, and a nonsplit extension of 1 or $\bar{\varepsilon}_5^{-1}$ by $\bar{\varepsilon}_5^{-2}$, given by a suitable lattice, would define an

unramified cyclic extension of degree 5 of $K(\sqrt{5})$ or $K(\zeta_5)$, the field cut out by the quotient of the two characters. Otherwise the projective image of a constituent of dimension at least two would cut out a Galois extension of K unramified outside 5 with root discriminant below $3^{1/2} \cdot 5^{3/2} < 19.37$: the factor $3^{1/2}$ comes from the tame ramification of K at 3, and the factor $5^{3/2}$ from the ramification bound of Fontaine and Abrashkin at 5 for Hodge–Tate weights in $[0, 2]$ (Proposition 8.2). The prime 5 is the smallest prime ℓ for which these weights lie in the Fontaine–Laffaille range $[0, \ell - 2]$. When 25 or 5 does not divide the degree of the extension over K, its wild inertia groups at 5 have order at most 5, respectively 1, and the same bound improves to $3^{1/2} \cdot 5^{7/5}$, respectively $3^{1/2} \cdot 5$; this excludes the smaller projective images. Odlyzko's unconditional lower bounds for discriminants, class field theory and finite group theory exclude such an extension (part (2) of Theorem 9.3).

The theorem of Calegari, Emerton and Gee also lets one prescribe an irreducible component of the local lifting ring at the place 3 (a *polarized component at* 3, Section 7.4) on which the p-adic member must lie, and the argument just given applies whichever component is prescribed. If $\bar{\rho}(I_{\mathfrak{p}})$ consisted of scalars, $\bar{\rho}$ would have a lift at the place 3 with finite image on inertia, built with Hensel's lemma and Edixhoven's theorem on fixed points; this lift lies on a polarized component at 3 that consists of lifts with $N = 0$, and the system built on it would contradict what was just shown (Proposition 9.5). So $\bar{\rho}(I_{\mathfrak{p}})$ is not scalar.

(2) *N is a single Jordan block.* As $\mathfrak{p}$ is ramified over 3, a generator of tame inertia at $\mathfrak{p}$ can be taken to be the square of an element of $G_{\mathbb{Q}}$ outside G_K, and the polarization of $\bar{\rho}$ writes its image as a scalar times a matrix $A\,{}^tA^{-1}$ (Proposition 10.2). A matrix of this form that is a scalar times a unipotent matrix is 1 or a single Jordan block, because $A - {}^tA$ is alternating and so has even rank (Lemma 10.1). Since $\bar{\rho}(I_{\mathfrak{p}})$ is not scalar (step (1)), the unipotent factor of $\bar{\rho}$ on $I_{\mathfrak{p}}$ is not 1, so it is a single Jordan block. It is the reduction of the unipotent factor $\exp(t_p N)$ of the p-adic member, which lifts $\bar{\rho}$ (t_p is the p-adic tame character), and $(\exp(t_p N) - 1)^2$, whose reduction is not 0, would vanish if N^2 did; so N is a single Jordan block too (Corollary 10.3).

(3) *R is irreducible and ordinary at $\mathfrak{p}$.* A semisimple representation of dimension three whose monodromy at $\mathfrak{p}$ is a single Jordan block is irreducible (Proposition 10.7), and weak admissibility forces the decomposition group at $\mathfrak{p}$ to stabilize a line (Proposition 10.6).

(4) *Every reduction of R has trivial semisimplification* (Corollary 11.15). We bound the root discriminant of the field cut out by a reduction and compare it with Odlyzko's unconditional lower bounds. On the decomposition group at $\mathfrak{p}$ a reduction is, up to an unramified character, upper unitriangular. Its entries next to the diagonal are two homomorphisms with values in the residue field, combinations of the cubic characters of $\mathbb{Q}_3(\sqrt{-3})$, and the cup product of the two vanishes. These characters form a space of dimension 4 over $\mathbb{F}_3$; they are trivial on $1 + \mathfrak{p}^4$, and their upper ramification breaks are at most 3 (Lemma 11.2). The extension cut out by such a representation has largest upper ramification break at most $11/3$, the largest break that a Heisenberg extension of degree 27 of $K_{\mathfrak{p}}$ can have (Propositions 11.6 and 11.10; this also follows from a theorem of Abrashkin, Remark 11.8), but the bound on the root discriminant that this alone gives lies above all of Odlyzko's bounds.

What brings the bound down is the size of the ramification groups between the breaks 3 and $11/3$. On the ramification groups of upper index above 3 the entries next

to the diagonal vanish, and the corner entry depends linearly on the exterior product of the two homomorphisms. As their cup product vanishes, this exterior product lies in the kernel of the linear form that the cup product induces on the exterior square of the space of cubic characters; the exterior square has dimension 6, and the kernel dimension 5. So it suffices to compute, by Kummer theory, the Heisenberg extensions of degree 27 for five suitably chosen planes of cubic characters on which the cup product vanishes and whose exterior products span this kernel (Propositions 11.6 and 11.10). This brings the bound below Odlyzko's bounds for fields of large degree, with more room when the inertia groups at $\mathfrak{p}$ are small (Proposition 11.11). So the degree of the field is bounded, and finite group theory shows that a reduction has no irreducible constituent of dimension 2 or 3. Its constituents are therefore characters unramified outside $\mathfrak{p}$, which are trivial (Proposition 11.1).

(5) *Local generation.* The field K has one prime above 3 and class number one, so the Galois group of the maximal pro-3 extension of K unramified outside $\mathfrak{p}$ is generated by an inertia group at $\mathfrak{p}$ (Lemma 11.16). A representation unramified outside $\mathfrak{p}$ whose reduction has trivial semisimplification factors through this pro-3 group. So R has the same image as its inertia group at $\mathfrak{p}$, which stabilizes the ordinary line, and R is reducible: a contradiction.

1.6. **Earlier work.** The method of Part II, a lift of minimal ramification in a compatible system followed by the study of a member at a small prime, is that of Khare and Wintenberger for two-dimensional representations of $G_{\mathbb{Q}}$ [76, 77]; earlier instances of the switch to a small prime are due to Dieulefait [49] and Wintenberger [115]. The situation at 5 in step (1) is that of the theorems of Fontaine and Abrashkin on schemes with good reduction everywhere (Remark 9.4). The residual step (4) has a two-dimensional analogue in Şengün's theorem that G_K has no irreducible two-dimensional representation over $\overline{\mathbb{F}}_3$ unramified outside 3 [99, Theorem C]. That the Galois group of the maximal pro-3 extension of K unramified outside $\mathfrak{p}$ is generated by an inertia group at $\mathfrak{p}$ (step (5)) is an elementary and well-known property of $\mathbb{Q}(\sqrt{-3})$ and the prime 3, going back to Shafarevich and Koch [103, 79] (see [67, Remark 6.1.4]). The same step appears in dimension two in the work of Freitas, Kraus and Siksek [60, Theorem 9(b) and the proof of Theorem 1], where the image of the Galois representation of a suitable quadratic twist of an elliptic curve with good reduction away from one prime is shown to equal the image of an inertia group (see also [61]). Representations of G_K unramified outside $\mathfrak{p}$ with residual image a 3-group also occur in work of Freitas and Sánchez-Rodríguez [63].

A new ingredient is the way the ramification of the reductions of the member R at a prime above 3 is bounded: Fontaine–Laffaille theory is not available for R, and its place is taken by ordinarity at $\mathfrak{p}$, which weak admissibility forces once the monodromy operator is regular, given the Hodge–Tate weights $\{0, 1, 2\}$ (steps (3) and (4)). On its own, this argument shows that no semisimple representation $G_K \to \mathrm{GL}_3(\overline{\mathbb{Q}}_3)$ unramified outside $\mathfrak{p}$ is de Rham at $\mathfrak{p}$ with Hodge–Tate weights $\{0, 1, 2\}$ and regular monodromy there (Proposition 11.21).

The Frey representation is three-dimensional, of unitary type over an imaginary quadratic field, and comes from a motive of rank three that is not of GL_2-type: the local monodromy of $\mathbb{V}$ at $s = 1$ is a pseudo-reflection of order 3 (Proposition 3.3), which no twist of the symmetric square of a rank-two local system has. Darmon suggested that Katz's hypergeometric motives might connect generalized Fermat equations to higher-dimensional Galois representations [36, remark after Theorem 1.13]. Rank-two hypergeometric motives have been developed for generalized Fermat equations by Golfieri Madriaga and Pacetti [65] and by Golfieri Madriaga,

Pacetti and Rodriguez-Villegas [66], who list the extension of their results to hypergeometric motives of any rank among the questions they expect to address; see also the Frey abelian varieties of [23]. Among the neighboring problems, the twisted equations $x^3 + y^3 = q^\alpha z^p$, $q \geq 5$ prime, were treated by Bennett, Luca and Mulholland [16] and by Bennett, Bruni and Freitas [14], and recently by Freitas and Mocanu for $q = 5$ and certain primes p [62, Theorem 1.8]. The signatures (r, r, p) with $r \in \{5, 7, 11\}$ were treated by Billerey, Chen, Dieulefait and Freitas [23, 24], in part conditionally on Darmon's "big image" conjecture [36, Conjecture 4.1], in the form of [23, Conjecture 1.2]. For certain totally real fields F', among them every $\mathbb{Q}(\zeta_{3^m})^+$, Dieulefait and Golfieri Madriaga [48, Theorems 1.4 and 1.5] prove that Fermat's equation $x^p + y^p + z^p = 0$ has no nontrivial primitive solution in the ring of integers of F' for every prime $p \equiv 2 \pmod 3$ beyond a bound depending on F', using, when $3 \mid xyz$, a level-lowering argument at a prime above 3.

The conclusion of Theorem A was also known to follow from hypotheses of a different kind. Under Baker's explicit *abc* conjecture in the form of Laishram and Shorey, the equation has no solution for any $n \geq 3$ other than $n = 4$ [82, Theorem 4] (the exponent 4, which that theorem leaves out, is settled unconditionally [26, Theorem 1], [30, Theorem 2]); the *abc* conjecture implies that there are only finitely many solutions over all exponents together [37, §5.2]; and the Frey–Mazur conjecture (see [59, Conjecture 2.1]) implies the conclusion for p large, by Kraus's congruence. Zhou claims to derive the conclusion from inter-universal Teichmüller theory in a preprint [116], whose arguments we have not checked.

1.7. **Published results used.** Besides finite computations, the proof of Theorem A uses the following published results. Part IV cites those that the proof of Theorem B uses in addition.

- On the equation: Kraus [80, Théorème 6.1, Proposition 6.3 (ii), Lemme 6.4], with the modularity of elliptic curves over $\mathbb{Q}$ [25]; and, for the exponents they cover, Chen–Siksek [30, Theorem 2] and Freitas [58, Theorem 3].
- On the motive (Part I): Katz's theory of hypergeometric sheaves [74] and Beukers–Heckman [20]; proper and smooth base change [5]; Deligne's theory of weights [40, 41] and integrality [44]; Abhyankar's lemma and tame specialization [68], with tangential base points [43]; Berkovich's étale cohomology of analytic spaces [19]; the uniqueness of a polarizable variation of Hodge structure on an irreducible local system [42] and the Hodge numbers of hypergeometric variations [52]; Fontaine–Laffaille theory [57], Tsuji's comparison theorems [112, 113] in Beilinson's form [11], and Mokrane's weight spectral sequence [87] in Nakkajima's corrected form [90].
- For the compatible system (Part II): Calegari–Emerton–Gee [27, Theorem 4.2.11; also Lemma 1.5.20, Definition 2.1.9 and Theorem 2.1.16], which rests on the potential automorphy theorems of Barnet-Lamb–Gee–Geraghty–Taylor; these theorems [10, Theorems 4.5.1 and 5.5.1], which we also apply directly, and further results of the same paper [10, Lemmas 1.4.2, 1.4.3 and 5.3.1]; Bellovin–Gee [13, Theorem 3.3.7]; Edixhoven's theorem on fixed points of tame group actions [50, Proposition 3.4]; local–global compatibility, including at the residue characteristic [10, Theorem 2.1.1], [9, Theorem 1.1] (which rests on [8]; see also [28, Theorem 1.1]); Fontaine's Weil–Deligne representation of a potentially semistable representation [55]; Patrikis–Taylor [92, Theorem 1.7]; Clozel–Harris–Taylor [31, Lemma 2.1.1]; and Serre's theorem that locally algebraic abelian representations come from algebraic Hecke characters [100].

- At the prime 5: Fontaine–Laffaille theory and the ramification bound of Fontaine and Abrashkin [1, 54] (Theorem 8.1).
- At the prime 3 (Part III): Berger's theorem that de Rham representations are potentially semistable [17], Fontaine's theory of semistable representations [56, 55] and the theorem of Colmez and Fontaine [33].
- For discriminants and finite groups: the explicit formula in Poitou's unconditional form [93, 91]; the list of the simple groups of small order and of their automorphism groups in the ATLAS [34], and Dickson's classification of the finite subgroups of $\mathrm{PGL}_2(\overline{\mathbb{F}}_3)$ [47, 51].

The computations, listed in Appendix A with the software used and the separately written programs that repeat them, are in exact arithmetic, apart from evaluations of integrals with certified error bounds that give lower bounds for discriminants. The programs and their outputs are in [71].

1.8. **Organization.** Section 2 fixes conventions. Part I (Sections 3, 4, 5 and 6) constructs $\mathbb{V}$ and the Frey representation, with its local properties and its irreducibility. Part II (Sections 7, 8 and 9) constructs the compatible system and carries out step (1). Part III (Sections 10 and 11) carries out steps (2)–(5) and proves Theorem A. Part IV (Section 12) treats the equations $x^3 + y^3 = 3^k z^n$ with $k \geq 1$ and proves Theorem B.

Section 13 discusses the obstructing point and the exponents $p \equiv 2 \pmod 3$ and states three open questions, and Appendix A lists the computations. The Supplement, a separate document distributed with this paper, whose items are numbered S1, S2, ..., contains the computations for Part IV and computations that check results proved in the text.

2. Conventions

2.1. **The field K.** Throughout, $K = \mathbb{Q}(\omega)$ with $\omega^2 + \omega + 1 = 0$, $\mathcal{O} = \mathbb{Z}[\omega]$, and c is complex conjugation, with a lift $\tilde{\mathsf{c}} \in G_{\mathbb{Q}}$, which we take to be a complex conjugation of $\overline{\mathbb{Q}}$; so $\tilde{\mathsf{c}}^2 = 1$. The prime of K above 3 is $\mathfrak{p} = (1-\omega) = (\sqrt{-3})$; $K_{\mathfrak{p}}$ is the completion, and v_3 is the valuation on an algebraic closure of $\mathbb{Q}_3$ (or on its completion $\mathbb{C}_3$) with $v_3(3) = 1$. The ring $\mathcal{O}$ is a principal ideal domain with unit group $\mu_6 = \{\pm 1, \pm\omega, \pm\omega^2\}$, and $\mu_6 \to (\mathcal{O}/\mathfrak{p}^2)^\times$ is an isomorphism. The prime 7 splits in K as $7 = \mathfrak{l}\bar{\mathfrak{l}}$ with

$$\mathfrak{l} = (2-\omega), \qquad \bar{\mathfrak{l}} = (3+\omega) = \mathsf{c}(\mathfrak{l});$$

the residue fields are $\mathbb{F}_7$, with $\omega \equiv 2 \pmod{\mathfrak{l}}$ and $\omega \equiv 4 \pmod{\bar{\mathfrak{l}}}$. For a prime $p \equiv 1 \pmod 3$ we write $v, \bar{v}$ for the two primes of K above p; then $K_v = K_{\bar{v}} = \mathbb{Q}_p$.

2.2. **Galois groups.** For a field F we write G_F for its absolute Galois group. For a prime $\mathfrak{q}$ of K, $G_{K_{\mathfrak{q}}} \subset G_K$ is a decomposition group, $I_{\mathfrak{q}}$ its inertia subgroup, and $\mathrm{Frob}_{\mathfrak{q}}$ a *geometric* Frobenius element. Local and global Artin maps send uniformizers to geometric Frobenius elements. (With the other normalization some characters below are replaced by their inverses; the statements are unchanged.) For a prime ℓ, ε_ℓ is the ℓ-adic cyclotomic character and $\bar{\varepsilon}_\ell$ its reduction. Hodge–Tate weights are normalized so that ε_p has weight -1. Then the p-adic cohomology H^2 of a smooth projective surface over a p-adic field has Hodge–Tate weights in $\{0, 1, 2\}$, the weight i occurring with multiplicity $h^{i,2-i}$.

For $u \in K^\times$ the *cubic Kummer character* $\kappa_u \colon G_K \to \mu_3 \subset \mathcal{O}^\times$ is $\kappa_u(\sigma) = \sigma(u^{1/3})/u^{1/3}$. If $u \in \mathbb{Q}^\times$, then $\kappa_u^{\mathsf{c}} = \kappa_u^{-1}$, where $\kappa^{\mathsf{c}}(\sigma) = \kappa(\tilde{\mathsf{c}}\sigma\tilde{\mathsf{c}}^{-1})$: for $u^{1/3}$ real, $\tilde{\mathsf{c}}$ fixes $u^{1/3}$ and inverts μ_3.

2.3. **Coefficients.** For each prime ℓ we fix an embedding $\iota_\ell\colon \overline{\mathbb{Q}} \hookrightarrow \overline{\mathbb{Q}}_\ell$. Through ι_ℓ we regard elements of K as elements of $\overline{\mathbb{Q}}_\ell$. A representation of G_K over $\overline{\mathbb{Q}}_\ell$ *has coefficients in* K if the characteristic polynomials of the Frobenius elements at almost all primes lie in $K[T]$. For a continuous representation ρ of a profinite group on a finite-dimensional $\overline{\mathbb{Q}}_p$-vector space, $\bar\rho$ denotes the semisimplification of the reduction of a stable lattice, a representation over $\overline{\mathbb{F}}_p$. By the Brauer–Nesbitt theorem it is independent of the lattice. A continuous representation of G_K with finitely many ramified primes is determined up to semisimplification by the characteristic polynomials of the $\mathrm{Frob}_{\mathfrak{q}}$ at the unramified primes (Chebotarev).

2.4. **Local systems.** For a connected scheme Y, a lisse $\overline{\mathbb{Q}}_\ell$-sheaf on Y is a continuous representation of its étale fundamental group (for the analytic spaces of Section 4 see Section 4.1). A lisse sheaf is *constant* if the geometric fundamental group acts trivially (over a base field F the Galois group G_F may still act on the fiber), and *unipotent* if it has a finite filtration by lisse subsheaves whose graded pieces are constant. Sub-objects, quotients and extensions of unipotent lisse sheaves are unipotent. For a representation ρ of $G_{K_{\mathfrak{q}}}$ with $\mathfrak{q} \nmid \ell$, Grothendieck's monodromy theorem attaches a Weil–Deligne representation $\mathrm{WD}(\rho) = (\phi, N)$, with ϕ of finite image on $I_{\mathfrak{q}}$ and N nilpotent, such that $\rho(\sigma) = \phi(\sigma)\exp(t_\ell(\sigma)N)$ for $\sigma \in I_{\mathfrak{q}}$, where $t_\ell\colon I_{\mathfrak{q}} \to \mathbb{Z}_\ell(1)$ is the ℓ-adic tame character.

Part I: a Frey motive of rank three over $\mathbb{Q}(\sqrt{-3})$

3. The Frey motive

The local system $\mathbb{V}$ of the introduction comes from a family of surfaces. Its Frobenius data at the two primes above 7 are used for the irreducibility of the Frey representation (Section 6) and for the triviality of a limit character at $s = 0$ (Section 4.4).

3.1. **The surfaces and the character.** Let $K_9 = K(\zeta_9) = \mathbb{Q}(\zeta_9)$, a cyclic cubic extension of K, and let $\sigma_0 \in \mathrm{Gal}(K_9/K)$ be the generator with $\sigma_0(\zeta_9) = \zeta_9^4$. Let $\mathrm{R}_{K_9/K}\mathbb{A}^1$ be the Weil restriction of the affine line, an affine space of dimension 3 over K, let $\mathrm{N}\colon \mathrm{R}_{K_9/K}\mathbb{A}^1 \to \mathbb{A}^1$ be the norm, and let $H = \mathrm{R}_{K_9/K}\mu_9$, a finite étale group scheme of order 729 over K acting on $\mathrm{R}_{K_9/K}\mathbb{A}^1$ by multiplication. Let $\mathcal{S} = \mathbb{P}^1_K \smallsetminus \{0, 1, \infty\}$ with coordinate s, and let

$$X = \{(y, s) \in \mathrm{R}_{K_9/K}\mathbb{A}^1 \times \mathcal{S} :\ \mathrm{N}(1 - y^9) = s\}, \qquad f\colon X \to \mathcal{S},$$

with fibers X_s. The action of H preserves X.

Fix a K-embedding $\tau_0\colon K_9 \to \overline{K}$ and put $\tau_j = \tau_0 \circ \sigma_0^j$ for $j \in \mathbb{Z}/3$. The isomorphism $K_9 \otimes_K \overline{K} \to \overline{K}^3$, $x \otimes z \mapsto (\tau_j(x)z)_j$, identifies $\mathrm{R}_{K_9/K}\mathbb{A}^1$ over $\overline{K}$ with $\mathbb{A}^3$, $\mathrm{N}(1 - y^9)$ with $\prod_j(1 - y_j^9)$, $H_{\overline{K}}$ with μ_9^3, and $X_s \otimes \overline{K}$ with the surface $Z_s\colon (1 - y_0^9)(1 - y_1^9)(1 - y_2^9) = s$ of the introduction. An element $\sigma \in G_K$ with $\sigma \circ \tau_0 = \tau_0 \circ \sigma_0^k$ acts on $\overline{K}$-points by $(y_j)_j \mapsto (\sigma(y_{j-k}))_j$, and on $H(\overline{K}) = \mu_9(\overline{K})^3$ by the same formula, where $\sigma(\zeta) = \zeta^{4^k}$ for $\zeta \in \mu_9$. For $e = (e_0, e_1, e_2) \in (\mathbb{Z}/9)^3$ let $\chi_e(g) = \prod_j \iota_\ell(g_j)^{e_j}$, a character of $H(\overline{K})$ with values in $\overline{\mathbb{Q}}_\ell^\times$.

Lemma 3.1. *The characters χ_e fixed by G_K are those with $e = m(1, 7, 4)$, $m \in \mathbb{Z}/9$. Those of order 9 on each factor of μ_9^3 are the six characters χ^m, $m \in (\mathbb{Z}/9)^\times$, where $\chi := \chi_{(1,7,4)}$. Each of them is trivial on the diagonal μ_3 and nontrivial on the diagonal μ_9.*

Proof. By the formulas above, $\chi_e(\sigma g) = \prod_j \iota_\ell(g_j)^{4^k e_{j+k}}$, so χ_e is fixed by G_K if and only if $e_{j+1} \equiv 7e_j \pmod 9$ for all j, that is $e = e_0(1, 7, 4)$. Such a character has order 9 on each

factor exactly when $e_0 \in (\mathbb{Z}/9)^\times$. On the diagonal, $\chi^m(\zeta,\zeta,\zeta) = \iota_\ell(\zeta)^{12m}$, which is 1 for $\zeta \in \mu_3$ and not for a primitive $\zeta \in \mu_9$. □

For a G_K-fixed character χ' of $H(\overline{K})$ the idempotent $\mathbf{1}_{\chi'} = |H|^{-1}\sum_g \chi'(g)^{-1} g^*$ acting on the cohomology of H-stable varieties commutes with G_K; its image on a cohomology group is called the χ'-part and is written with the exponent χ'. The automorphism $\sigma_0 \otimes 1$ of $\mathrm{R}_{K_9/K}\mathbb{A}^1$ is defined over K, preserves X and commutes with f; on $\overline{K}$-points it permutes the coordinates cyclically, so it carries the χ^m-part of the cohomology to the χ^{4m}-part.

Definition 3.2. Fix $m \in (\mathbb{Z}/9)^\times$. For a prime ℓ let

$$\mathbb{V} = \mathbb{V}_{\chi^m} \coloneqq \left(\mathrm{R}^2 f_! \,\overline{\mathbb{Q}}_\ell\right)^{\chi^m},$$

a sheaf on $\mathcal{S}$, with fibers $\mathbb{V}_s = H^2_c(X_s \otimes \overline{K}, \overline{\mathbb{Q}}_\ell)^{\chi^m}$. By the preceding paragraph $\mathbb{V}_{\chi^m} \cong \mathbb{V}_{\chi^{4m}} \cong \mathbb{V}_{\chi^{7m}}$, so up to isomorphism there are two such sheaves, $\mathbb{V}_\chi$ and $\mathbb{V}_{\chi^{-1}}$. The statements below hold for both, and where the two differ (only in Proposition 3.9) both cases are listed. We write $\mathbb{V}$ for either.

3.2. **Geometry over $\overline{K}$.** For $j \in \mathbb{Z}/9$, $j \neq 0$, let $\mathcal{L}_j$ be the Kummer sheaf of order 9 attached to the μ_9-torsor $y^9 = 1 - x$ on $\mathbb{A}^1 \smallsetminus \{1\}$ and the character $\zeta \mapsto \iota_\ell(\zeta)^j$ of μ_9, extended by zero to $\mathbb{A}^1$. For sheaves $\mathcal{K}, \mathcal{K}'$ on $\mathbb{G}_m$ let $\mathcal{K} \star \mathcal{K}'$ be the multiplicative convolution with compact supports, $(\mathcal{K}\star\mathcal{K}')_s = H^*_c(\mathbb{G}_m, \mathcal{K}(x) \otimes \mathcal{K}'(s/x))$.

Proposition 3.3. *Over $\overline{K}$, and over $\overline{\mathbb{F}}_q$ for every prime $\mathfrak{q} \nmid 3\ell$ of K with residue field $\mathbb{F}_q$:*

(a) *$\mathbb{V}$ is the convolution $\mathcal{L}_m \star \mathcal{L}_{7m} \star \mathcal{L}_{4m}$ restricted to $\mathcal{S}$, and $H^i_c(X_s, \overline{\mathbb{Q}}_\ell)^{\chi^m} = 0$ for $i \neq 2$;*

(b) *$\mathbb{V}$ is lisse of rank 3 on $\mathcal{S}$, irreducible, and tamely ramified at 0, 1, ∞;*

(c) *its local monodromy is unipotent with a single Jordan block at 0; a pseudo-reflection of order 3 at 1; and semisimple of order 9 at ∞, with eigenvalues $\iota_\ell(\zeta)^m, \iota_\ell(\zeta)^{4m}, \iota_\ell(\zeta)^{7m}$, or their inverses (according to the orientation), on a generator ζ of the tame inertia modulo 9.*

In particular the local monodromy at ∞ factors through the quotient μ_9 of the tame inertia group $\hat{\mathbb{Z}}'(1) = \varprojlim \mu_n$ at ∞ (the Kummer character of $1/s$), and $\mu_3 \subset \mu_9$ acts on $\mathbb{V}$ by the scalars $\zeta \mapsto \iota_\ell(\zeta)^{n_\infty}$, for an integer $n_\infty \in \{1,2\}$ depending only on $\mathbb{V}$. The stalks of $j_*\mathbb{V}$ (for $j\colon \mathcal{S} \to \mathbb{P}^1$) at 0, 1, ∞ have dimensions 1, 2, 0.

Proof. Put $x_j = 1 - y_j^9$. The map $Z_s \to Y_s = \{x_0x_1x_2 = s\}$ is a μ_9^3-torsor over the locus where no x_j equals 1, and on the χ^m-isotypic part the push-forward of $\overline{\mathbb{Q}}_\ell$ is $\boxtimes_j \mathcal{L}_{e_j}(x_j)$ with $(e_j) = m(1,7,4)$, extended by zero where some $x_j = 1$ (each e_j is nonzero, so the isotypic part has no invariants there). Hence $H^i_c(Z_s)^{\chi^m} = H^i_c(Y_s, \boxtimes_j \mathcal{L}_{e_j}(x_j))$, which is the fiber at s of the triple convolution. Katz's theory of hypergeometric sheaves [74, Chapter 8] shows that, the three characters being nontrivial and the exponents at ∞ being distinct from the (trivial) exponents at 0, the convolution is concentrated in one degree, is lisse of rank 3 on $\mathbb{G}_m \smallsetminus \{1\}$, irreducible, tame at $0, 1, \infty$, with the local monodromies of (c). At 0 the monodromy is a single unipotent Jordan block (the three characters at 0 coincide), at ∞ it is the direct sum of the three characters, and at 1 it is a pseudo-reflection whose nontrivial eigenvalue is the product of the characters, of order dividing 9 and here of order 3 since $12m \equiv 3m \pmod 9$. Over $\mathbb{C}$ this is the hypergeometric local system of Beukers and Heckman [20] with parameters $\{m/9, 4m/9, 7m/9\}$ (or their negatives) and $\{0,0,0\}$. The degree is 2 because Y_s is a torus of dimension 2 and the convolution of two of the rank-one sheaves $\mathcal{L}_j$ is placed in degree 1 (so the triple one in degree 2). The cube of the

monodromy at ∞ acts by $\iota_\ell(\zeta^3)^{\pm m}$ on all three eigenlines, because $4 \equiv 7 \equiv 1 \pmod 3$; so $n_\infty \equiv \pm m \pmod 3$. The dimensions of the stalks of $j_*\mathbb{V}$ are those of the invariants of the local monodromies: 1 (one Jordan block), 2 (a pseudo-reflection) and 0 (no exponent at ∞ is 0). □

3.3. **A smooth compactification.** Let $\bar{\mathcal{S}} = \mathbb{P}^1 \smallsetminus \{0, \infty\}$ with coordinate s, so that $\mathcal{S} = \bar{\mathcal{S}} \smallsetminus \{1\}$, and let $\bar{X} = \{(y, s) \in \mathrm{R}_{K_9/K}\mathbb{A}^1 \times \bar{\mathcal{S}} :\ \mathrm{N}(1 - y^9) = s\}$, so that $X = \bar{X} \times_{\bar{\mathcal{S}}} \mathcal{S}$. In this subsection all schemes are over $\mathcal{O}[1/3]$. The model constructed here extends $\mathbb{V}$ to a lisse sheaf over $\mathcal{O}[1/3\ell]$, which gives the behavior of $\mathbb{V}_{s_0}$ at the primes not dividing 3ℓ (Section 5), and it is the starting point for the crystallinity at p (Section 5.5).

Proposition 3.4.

(a) *There are a projective morphism $\tilde{f}^\flat\colon \tilde{X}^\flat \to \bar{\mathcal{S}}$ with an action of H over $\bar{\mathcal{S}}$, and an H-equivariant open immersion $\bar{X} \hookrightarrow \tilde{X}^\flat$ over $\bar{\mathcal{S}}$ whose complement $\tilde{D}^\flat$, with its reduced structure, is a divisor with strict normal crossings relative to $\bar{\mathcal{S}}$; after base change to $\mathcal{O}[1/3, \zeta_9]$ each component of $\tilde{D}^\flat$ is a disjoint union of copies of $\mathbb{P}^1_{\bar{\mathcal{S}}}$. The morphism $\tilde{f}^\flat$ is smooth outside the section $\{y = 0,\ s = 1\}$.*

(b) *Let $\tilde{f}\colon \tilde{X} \to \mathcal{S}$ and $\tilde{D}$ be the restrictions of $\tilde{f}^\flat$ and $\tilde{D}^\flat$ to $\mathcal{S}$. Then $\tilde{f}$ is smooth and projective, $X = \tilde{X} \smallsetminus \tilde{D}$, and $H^*(\tilde{D}^\flat_s, \overline{\mathbb{Q}}_\ell)^{\chi^m} = 0$ for every geometric point s of $\bar{\mathcal{S}}$ of characteristic different from ℓ.*

(c) *Consequently $\mathbb{V} \cong (\mathrm{R}^2\tilde{f}_*\overline{\mathbb{Q}}_\ell)^{\chi^m}$ extends to a lisse sheaf on $\mathcal{S}$ over $\mathcal{O}[1/3\ell]$, pure of weight 2, and for every point s of $\mathcal{S}$ its fiber is the χ^m-part of H^2 of the smooth projective surface $\tilde{X}_s$.*

Proof. Reduction to the split form. The ring $\mathcal{O}' = \mathcal{O}[1/3, \zeta_9]$ is finite étale and Galois over $\mathcal{O}[1/3]$, with group $\mathrm{Gal}(K_9/K)$, because K_9/K is unramified outside 3. Let $P = \mathrm{R}_{\mathcal{O}'/\mathcal{O}[1/3]}\mathbb{P}^1$, a smooth projective $\mathcal{O}[1/3]$-scheme containing $\mathrm{R}_{\mathcal{O}'/\mathcal{O}[1/3]}\mathbb{A}^1$ and acted on by H. The schemes below are obtained from $\bar{X} \subset P \times \bar{\mathcal{S}}$ by taking a scheme-theoretic closure, then reduced loci where a morphism to $\bar{\mathcal{S}}$ is not smooth, and blow-ups along them. These operations commute with the étale base change $\mathcal{O}[1/3] \to \mathcal{O}'$, and the properties to be proved, other than projectivity (which holds by construction), are local for the étale topology; so we may check them over $\mathcal{O}'$. Over $\mathcal{O}'$, as in Section 3.1, $P \cong (\mathbb{P}^1)^3$, $H \cong \mu_9^3$ acting coordinatewise, and $\bar{X} \cong \{\prod_j (1 - y_j^9) = s\} \subset \mathbb{A}^3 \times \bar{\mathcal{S}}$. In what follows $\{i, j, k\} = \{0, 1, 2\}$ and $x_j = 1 - y_j^9$. For $\zeta, \zeta' \in \mu_9$ let $L_{i,j,\zeta} = \{y_i = \infty,\ y_j = \zeta\}$, a line with coordinate y_k; $P_{i;\zeta,\zeta'} = \{y_i = \infty,\ y_j = \zeta,\ y_k = \zeta'\}$ (with $j < k$); and $Q_{j,\zeta} = \{y_j = \zeta,\ y_i = y_k = \infty\}$.

The closure. Write $y_j = Y_j/X_j$. The hypersurface $\bar{Z} \subset (\mathbb{P}^1)^3 \times \bar{\mathcal{S}}$ defined by $\prod_j (X_j^9 - Y_j^9) = s \prod_j X_j^9$ is a relative effective Cartier divisor, flat over $\bar{\mathcal{S}}$, since its equation is nonzero on every fiber. It contains $\bar{X}$ as the open subscheme $X_0X_1X_2 \neq 0$, and it is the scheme-theoretic closure of $\bar{X}$: it has no embedded points (a Cartier divisor in a regular scheme is Cohen–Macaulay), all its irreducible components have the same dimension, and by (ii)–(iv) below its boundary part has dimension at most 1 in every fiber, so it contains no component. Let s be a geometric point of $\bar{\mathcal{S}}$; its characteristic is not 3, and $s \neq 0$.

(i) *No coordinate infinite.* The partial derivatives of $\prod_j (1 - y_j^9)$ are $-9y_j^8 \prod_{i \neq j} x_i$. At a point with $\prod_j x_j = s \neq 0$ they all vanish only if $y = 0$, where the value is 1. So $\bar{Z}_s \cap \mathbb{A}^3$ is smooth if $s \neq 1$, and for $s = 1$ its only singular point is $y = 0$.

(ii) *Exactly one coordinate, y_i, infinite.* With $w = 1/y_i$ the equation is $g := (w^9 - 1)x_jx_k - sw^9 = 0$. On $w = 0$ it reads $x_jx_k = 0$, so $\bar{Z}_s \cap \{y_i = \infty\}$ is

the union of the 18 lines $L_{i,j,\zeta}$ and $L_{i,k,\zeta}$, $\zeta \in \mu_9$. At $w = 0$ we have $\partial g/\partial w = 0$, $\partial g/\partial y_j = 9y_j^8 x_k$ and $\partial g/\partial y_k = 9y_k^8 x_j$. If $x_j = 0 \neq x_k$, then $y_j \neq 0$ and $\partial g/\partial y_j \neq 0$; similarly if $x_k = 0 \neq x_j$. So the singular points with exactly one infinite coordinate are the $3 \cdot 81 = 243$ points $P_{i;\zeta,\zeta'}$.

(iii) *Exactly two coordinates, y_i, y_k, infinite.* With $w_i = 1/y_i$ and $w_k = 1/y_k$ the equation is $(w_i^9 - 1)(w_k^9 - 1)x_j = s w_i^9 w_k^9$. At $w_i = w_k = 0$ it forces $y_j \in \mu_9$, and there $\partial/\partial y_j = -9y_j^8(w_i^9 - 1)(w_k^9 - 1) \neq 0$. So $\bar{Z}_s$ is smooth at the 27 points $Q_{j,\zeta}$, with local coordinates (w_i, w_k), in which $L_{i,j,\zeta} = \{w_i = 0\}$ and $L_{k,j,\zeta} = \{w_k = 0\}$ meet transversally.

(iv) *All coordinates infinite.* The equation $\prod_j (w_j^9 - 1) = s \prod_j w_j^9$ fails at $w = 0$.

The points $P_{i;\zeta,\zeta'}$. Near the section $P_{i;\zeta,\zeta'} \times \bar{\mathcal{S}}$ put $x'_j = x_j(1 - w^9)/(-s)$. Then

$$(w^9 - 1)\, x_j x_k - s w^9 = s\,(x'_j x_k - w^9),$$

and (x'_j, x_k, w), together with the projection to $\bar{\mathcal{S}}$, is an étale coordinate system on $(\mathbb{P}^1)^3 \times \bar{\mathcal{S}}$ near this section: at the point, $dx'_j \equiv (9\zeta^8/s)\, dy_j$ modulo dw and ds, and $dx_k = -9\zeta'^8\, dy_k$. So near the section $\bar{Z}$ is étale-locally isomorphic to $A_8 \times \bar{\mathcal{S}}$, where $A_8 = \{uv = w^9\} \subset \mathbb{A}^3$, the section corresponding to the origin and the two lines $L_{i,j,\zeta}$, $L_{i,k,\zeta'}$ through $P_{i;\zeta,\zeta'}$ to the axes $\{u = w = 0\}$ and $\{v = w = 0\}$ respectively.

The resolution. For $e \geq 3$ the blow-up of the origin of $\{uv = w^e\}$ is covered by three charts: $v = uv_1$, $w = uw_1$, with equation $v_1 = u^{e-2} w_1^e$ (smooth); the symmetric chart $u = vu_1$, $w = vw_1$ (smooth); and $u = wu_2$, $v = wv_2$, with equation $u_2 v_2 = w^{e-2}$. The exceptional divisor consists of two copies of $\mathbb{P}^1$ ($\{u = v_1 = 0\}$ and $\{v = u_1 = 0\}$, completed in the third chart by $\{w = v_2 = 0\}$ and $\{w = u_2 = 0\}$ respectively), which meet only at the origin of the third chart; this point is smooth if $e = 3$ (and the two curves meet transversally there) and is a singular point of the form $\{u_2 v_2 = w^{e-2}\}$ if $e \geq 4$. The strict transforms of the two axes meet the exceptional divisor transversally, one in each copy, at the origin of the first chart and at the origin of the second chart, away from the third chart. Let $\tilde{X}^\flat$ be obtained from $\bar{Z}$ by blowing up four times the reduced locus of boundary points at which the morphism to $\bar{\mathcal{S}}$ is not smooth (at the first step, the 243 sections $P_{i;\zeta,\zeta'} \times \bar{\mathcal{S}}$; the other non-smooth point, $y = 0$ over $s = 1$, is not on the boundary). Since blowing up commutes with flat base change, the computation with $e = 9, 7, 5, 3$ shows: $\tilde{X}^\flat$ is smooth over $\bar{\mathcal{S}}$ along the boundary; over each section $P_{i;\zeta,\zeta'} \times \bar{\mathcal{S}}$ lies a chain $E_1 \cup \cdots \cup E_8$ of copies of $\mathbb{P}^1_{\bar{\mathcal{S}}}$, with $E_r \cap E_{r+1}$ a section and no other intersections between them; and the strict transforms of $L_{i,j,\zeta}$ and $L_{i,k,\zeta'}$ are disjoint near the chain and meet E_1 and E_8 (in some order) transversally, in one section each. The morphism $\tilde{f}^\flat \colon \tilde{X}^\flat \to \bar{\mathcal{S}}$ is projective, as a composite of blow-ups and a projective morphism, and by (i)–(iv) it is smooth outside the section $\{y = 0,\ s = 1\}$. The group H preserves $\bar{Z}$ and each blow-up center, so it acts on $\tilde{X}^\flat$ over $\bar{\mathcal{S}}$; the same holds for $\mathrm{Gal}(K_9/K)$, which is how the construction descends to $\mathcal{O}[1/3]$.

The boundary. $\tilde{D}^\flat$ is the union of the strict transforms of the 54 lines $L_{i,j,\zeta}$ (each isomorphic to $L_{i,j,\zeta}$, a smooth curve) and of the $243 \cdot 8$ curves E_r. By (ii)–(iv), two distinct lines $L_{i,j,\zeta}$ and $L_{i',j',\zeta'}$ meet only if $i' = i$ and $j' \neq j$ (at a point $P_{i;\cdot,\cdot}$, where the resolution separates them) or $(i', j', \zeta') = (k, j, \zeta)$ (at $Q_{j,\zeta}$, transversally). Hence the double points of each fiber $\tilde{D}^\flat_s$ are the 27 points $Q_{j,\zeta}$ and, on each of the 243 chains, its 7 inner double points and its 2 ends; there are no triple points. The generator of $\mathrm{Gal}(K_9/K)$ maps $L_{i,j,\zeta}$ to a line $L_{i+1,j+1,\zeta'}$ and the chain over $P_{i;\zeta,\zeta'}$ to the chain over a point whose infinite coordinate is y_{i+1}; since two lines with the same difference $j - i$ never meet and chains over distinct points are disjoint,

the conjugates of a component are pairwise disjoint, so over $\mathcal{O}[1/3]$ every component of $\tilde{D}^\flat$ is still smooth over $\bar{\mathcal{S}}$. This proves (a), and $X = \tilde{X} \smallsetminus \tilde{D}$.

The χ^m-part of the cohomology of the boundary. Let s be a geometric point of $\bar{\mathcal{S}}$ of characteristic $\neq \ell$, and let $\mu_9^{(i)}$ be the factor of μ_9^3 that multiplies y_i. It fixes every point of $L_{i,j,\zeta}$ and every point $P_{i;\zeta,\zeta'}$. Near $P_{i;\zeta,\zeta'}$ it fixes x_j' and x_k and multiplies w by a ninth root of unity: an automorphism of A_8 that preserves both axes, hence each blow-up center, each curve E_r over $P_{i;\zeta,\zeta'}$ and each double point of that chain. At $Q_{j,\zeta}$ it fixes the point and maps both lines through it to themselves ($L_{i,j,\zeta}$ pointwise). Hence every component D_a of $\tilde{D}_s^\flat$ is mapped to itself by a factor $\mu_9^{(i)}$ acting trivially on $H^*(D_a, \overline{\mathbb{Q}}_\ell)$ (pointwise on the lines; on $E_r \cong \mathbb{P}^1$ every automorphism acts trivially on cohomology), and every double point is fixed by a factor $\mu_9^{(i)}$ that maps each of the two components through it to itself. Order the components, and let $j_a \colon D_a \to \tilde{D}_s^\flat$ and $j_{ab} \colon D_a \cap D_b \to \tilde{D}_s^\flat$ be the inclusions. As there are no triple points, the sequence of sheaves

$$0 \to \overline{\mathbb{Q}}_\ell \to \bigoplus_a j_{a*}\overline{\mathbb{Q}}_\ell \to \bigoplus_{a<b} j_{ab*}\overline{\mathbb{Q}}_\ell \to 0, \qquad (f_a)_a \mapsto (f_a - f_b)_{a<b},$$

is exact; it is H-equivariant when $g \in H$ acts on the last term by pull-back followed by the sign -1 on the summands where g reverses the order of the two components. Let $v = (v_a)_a$ lie in the χ^m-part of $\bigoplus_a H^q(D_a)$. Given a, choose $g \in \mu_9^{(i)}$, with $\mu_9^{(i)}$ as above for D_a, such that $\chi^m(g) \neq 1$; this is possible because χ^m has order 9 on each factor (Lemma 3.1). The a-component of $g^*v = \chi^m(g)\, v$ reads $v_a = \chi^m(g)\, v_a$, so $v_a = 0$. The same argument, with an element of a factor that fixes the double point and preserves both components through it (so that no sign occurs), shows that the χ^m-part of $\bigoplus_{a<b} H^0(D_a \cap D_b)$ vanishes. Taking χ^m-parts is exact because $|H|$ is invertible in $\overline{\mathbb{Q}}_\ell$, so the long exact cohomology sequence gives $H^*(\tilde{D}_s^\flat, \overline{\mathbb{Q}}_\ell)^{\chi^m} = 0$. This proves (b).

Consequences. For $s \in \mathcal{S}$ the H-equivariant exact sequence $H^{q-1}(\tilde{D}_s) \to H_c^q(X_s) \to H^q(\tilde{X}_s) \to H^q(\tilde{D}_s)$ gives $H_c^q(X_s)^{\chi^m} \cong H^q(\tilde{X}_s)^{\chi^m}$. In families, over $\mathcal{O}[1/3\ell]$, apply $\mathrm{R}\tilde{f}_*$ to the H-equivariant triangle $j_!\overline{\mathbb{Q}}_\ell \to \overline{\mathbb{Q}}_\ell \to i_*\overline{\mathbb{Q}}_\ell \to$ on $\tilde{X}$, where $j \colon X \to \tilde{X}$ and $i \colon \tilde{D} \to \tilde{X}$ are the inclusions, and take χ^m-parts. By proper base change [5, Exposé XII, Corollaire 5.2 (iii)] the stalks of $(\mathrm{R}^q(\tilde{f}i)_*\overline{\mathbb{Q}}_\ell)^{\chi^m}$ are the groups $H^q(\tilde{D}_s)^{\chi^m} = 0$, so $(\mathrm{R}^q f_!\overline{\mathbb{Q}}_\ell)^{\chi^m} \cong (\mathrm{R}^q\tilde{f}_*\overline{\mathbb{Q}}_\ell)^{\chi^m}$. Since $\tilde{f}$ is smooth and proper, $\mathrm{R}^q\tilde{f}_*\overline{\mathbb{Q}}_\ell$ is lisse with fibers $H^q(\tilde{X}_s)$ [5, Exposé XVI, Corollaire 2.2], and so is its direct summand, the χ^m-part; at closed points its Frobenius eigenvalues have absolute value $|k(s)|^{q/2}$ in every complex embedding [40, Théorème (1.6)], $\tilde{X}_s$ being smooth and projective. □

3.4. **Hodge numbers and duality.**

Lemma 3.5. *For $s \in K \smallsetminus \{0,1\}$ and any embedding $K \hookrightarrow \mathbb{C}$, the Hodge numbers of $H^2(\tilde{X}_s(\mathbb{C}), \mathbb{C})^{\chi^m}$ are $h^{2,0} = h^{1,1} = h^{0,2} = 1$.*

Proof. By Proposition 3.3 the local system $H^2(\tilde{X}_s)^{\chi^m}$, $s \in \mathcal{S}(\mathbb{C})$, is the irreducible hypergeometric local system with parameters $\{m/9, 4m/9, 7m/9\}$ (or their negatives) and $\{0,0,0\}$, and the χ^m-part of the variation of Hodge structure $\mathrm{R}^2\tilde{f}_*\mathbb{C}$ is a polarizable variation of Hodge structure on it. An irreducible local system underlies at most one such variation up to a shift of the Hodge filtration [42, Proposition 1.13], and the Hodge numbers of the hypergeometric variations were computed by Fedorov [52] (see also Dettweiler–Sabbah [45]): when all the parameters at 0 are equal, the Hodge numbers are all equal to 1. The weight is 2, so they are $(1,1,1)$ in degrees $(2,0), (1,1), (0,2)$. □

Lemma 3.6. *For $s \in \mathbb{Q} \smallsetminus \{0,1\}$ there is an isomorphism of G_K-representations $\mathbb{V}_s^{\mathsf{c}} \cong \mathbb{V}_s^{\vee} \otimes \varepsilon_\ell^{-2}$.*

Proof. Write $\mathbb{V}_{\chi',s}$ for the χ'-part. Poincaré duality on the geometrically irreducible surface $\tilde{X}_s$ is a perfect G_K-equivariant pairing $H^2 \times H^2 \to H^4 = \overline{\mathbb{Q}}_\ell(-2)$, invariant under H, which acts trivially on H^4. Hence it pairs the χ'-part with the χ''-part trivially unless $\chi'\chi'' = 1$, and $\mathbb{V}_{\chi^{-m},s} \cong \mathbb{V}_{\chi^m,s}^{\vee}(-2)$. On the other hand, because $s \in \mathbb{Q}$ and $K_9/\mathbb{Q}$ is Galois, $\tilde{\mathsf{c}}$ induces an isomorphism of K-varieties between the conjugate $X_s \times_{K,\mathsf{c}} K$ and X_s, compatible with the actions of H through an automorphism $g \mapsto g^{\tilde{\mathsf{c}}}$ of $H(\overline{K}) = \mu_9(\overline{K})^3$ which permutes the three factors and acts on each by $\zeta \mapsto \tilde{\mathsf{c}}(\zeta)$. Transport of structure therefore identifies $\mathbb{V}_{\chi^m,s}^{\mathsf{c}}$ with the χ'-part of $H_c^2(X_s)$, where $\chi'(g) = \chi^m(g^{\tilde{\mathsf{c}}^{-1}})$. The character χ' is fixed by G_K (as $\tilde{\mathsf{c}}$ normalizes G_K) and of order 9 on each factor, as χ^m is, so $\chi' = \chi^n$ for some $n \in (\mathbb{Z}/9)^\times$ by Lemma 3.1. On the diagonal, $\tilde{\mathsf{c}}^{-1}(\zeta) = \zeta^j$ with $j \equiv -1 \pmod 3$, so $\iota_\ell(\zeta)^{12n} = \chi'(\zeta,\zeta,\zeta) = \iota_\ell(\zeta)^{12mj}$ and $n \equiv -m \pmod 3$. Hence $\chi' \in \{\chi^{-m}, \chi^{-4m}, \chi^{-7m}\}$ and $\mathbb{V}_{\chi^m,s}^{\mathsf{c}} \cong \mathbb{V}_{\chi^{-m},s}$. Combining the two isomorphisms gives the claim. □

3.5. **Integrality and traces.**

Lemma 3.7. *Let $\mathfrak{q} \nmid 3\ell$ be a prime of K with residue field $\mathbb{F}_q$, and let $s \in \mathbb{F}_{q^k} \smallsetminus \{0,1\}$. Then* $\operatorname{tr}(\operatorname{Frob}_{\mathfrak{q}}^k \mid \mathbb{V}_s) \in \mathcal{O}$, *and*

$$\operatorname{tr}(\operatorname{Frob}_{\mathfrak{q}}^k \mid \mathbb{V}_s) = \frac{1}{729} \sum_{g \in H(\overline{\mathbb{F}}_q)} \chi^m(g)^{-1}\, \#\{y \in X_s(\overline{\mathbb{F}}_q) :\ (F^k \circ g)(y) = y\},$$

where F is the q-power Frobenius of $X \otimes \mathbb{F}_q$, which maps X_s to X_{s^q}.

Proof. The formula is the Lefschetz trace formula for the twisted Frobenius $F^k \circ g$ (the Frobenius of a twisted form of X_s) combined with $H_c^i(X_s)^{\chi^m} = 0$ for $i \neq 2$. The right side lies in $\mathbb{Q}(\zeta_9)$ (through ι_ℓ); the automorphism $\zeta_9 \mapsto \zeta_9^n$ with $n \equiv 1 \pmod 3$ carries it to the trace on the χ^{nm}-part, which is the same trace, since $\sigma_0 \otimes 1$ commutes with Frobenius and carries the χ^m-part to the χ^{4m}-part. So the trace lies in the fixed field K. It is a sum of eigenvalues of Frobenius on $H_c^2(X_s)$, which are algebraic integers [44, Exposé XXI, 5.5.3]. □

3.6. **The data at the primes above 7.** The primes $\mathfrak{l}, \bar{\mathfrak{l}}$ above 7 are inert in K_9/K (since 7 has order 3 modulo 9). For $\mathfrak{q} \in \{\mathfrak{l}, \bar{\mathfrak{l}}\}$ let $\mathfrak{Q}$ be the prime of K_9 above $\mathfrak{q}$, which is unique; we identify its residue field $\mathcal{O}_{K_9}/\mathfrak{Q}$, of order 7^3, with $\mathbb{F}_{343}$. Every prime of $\overline{K}$ above $\mathfrak{q}$ lies above $\mathfrak{Q}$; so $\mathbb{F}_{343}$ is the subfield of order 343 of the residue field $\overline{\mathbb{F}}_7$ of the prime used to define $\operatorname{Frob}_{\mathfrak{q}}$, and on $\mu_9 \subset K_9$ the reduction at that prime is the reduction modulo $\mathfrak{Q}$. As $7 \nmid 9$, reduction modulo $\mathfrak{Q}$ maps $\mu_9(K_9)$ isomorphically onto $\mu_9(\mathbb{F}_{343})$. Let $\vartheta\colon \mathbb{F}_{343}^\times \to \mu_9(K_9)$ be the character with

$$\vartheta(z) \equiv z^{(343-1)/9} = z^{38} \pmod{\mathfrak{Q}}$$

(the ninth-power residue symbol modulo $\mathfrak{Q}$), extended by $\vartheta(0) = 0$, and $\vartheta_6 = \vartheta \circ \mathrm{N}_{\mathbb{F}_{7^6}/\mathbb{F}_{343}}$.

Lemma 3.8. *Let $\mathfrak{q} \in \{\mathfrak{l}, \bar{\mathfrak{l}}\}$. There is $m' \in (\mathbb{Z}/9)^\times$, with m' replaced by $-m'$ when m is replaced by $-m$, such that for $s \in \mathbb{F}_{7^k} \smallsetminus \{0,1\}$:*

$$\operatorname{tr}(\operatorname{Frob}_{\mathfrak{q}} \mid \mathbb{V}_s) = \textstyle\sum_{x \in \mathbb{F}_{343},\ \mathrm{N}_{\mathbb{F}_{343}/\mathbb{F}_7}(x) = s} \vartheta(1-x)^{m'} \qquad (k=1),$$

$$\operatorname{tr}(\operatorname{Frob}_{\mathfrak{q}}^2 \mid \mathbb{V}_s) = \textstyle\sum_{x \in \mathbb{F}_{7^6},\ \mathrm{N}_{\mathbb{F}_{7^6}/\mathbb{F}_{49}}(x) = s} \vartheta_6(1-x)^{m'} \qquad (k=2),$$

$$\operatorname{tr}(\operatorname{Frob}_{\mathfrak{q}}^3 \mid \mathbb{V}_s) = \textstyle\sum_{x_0x_1x_2 = s,\ x_j \in \mathbb{F}_{343}} \vartheta(1-x_0)^{m'}\vartheta(1-x_1)^{4m'}\vartheta(1-x_2)^{7m'} \qquad (k=3).$$

Proof. Over $\mathbb{F}_7$ the geometric Frobenius F permutes the three coordinates cyclically, $F(y)_j = y_{j-1}^7$ (for a suitable numbering, since $\mathfrak{q}$ is inert in K_9). For $g \in \mu_9^3$ a fixed point of $F \circ g$ is determined by y_0, which satisfies $y_0 = \delta(g)\, y_0^{343}$ with $\delta(g) = g_0^{343} g_1^{49} g_2^7$ (exponents modulo 9: $g_0 g_1^4 g_2^7$), and the equation of X_s becomes $\mathrm{N}_{\mathbb{F}_{343}/\mathbb{F}_7}(1 - y_0^9) = s$ with $y_0^9 \in \mathbb{F}_{343}$. For $y_0^9 = z \neq 0$ the condition $y_0^{342} = \delta(g)^{-1}$ reads $z^{38} = \delta(g)^{-1}$ (as $342 = 9 \cdot 38$), and there are then 9 choices of y_0; $y_0 = 0$ only occurs for $s = 1$. The G_K-fixed characters are the powers of δ (Lemma 3.1, in the numbering in which Frobenius shifts the coordinates), so averaging $\chi^m(g)^{-1}$ over the 81 elements g with given $\delta(g)$ in Lemma 3.7 leaves $\sum_z \vartheta(z)^{m'}$ over $z = 1 - x$ with $\mathrm{N}(x) = s$. The same computation with F^2 (which still permutes the coordinates cyclically) gives the second formula, and F^3 fixes the coordinates, which gives the triple sum. Replacing χ^m by χ^{-m} replaces every exponent by its negative. □

We write ω also for the image of $\omega \in K$ in the coefficients, and let

$$P^+(T) = T^3 - (6 - 3\omega)T^2 + (63 + 21\omega)T - 343,$$
$$P^-(T) = T^3 - (9 + 3\omega)T^2 + (42 - 21\omega)T - 343 = \overline{P^+}(T).$$

Proposition 3.9. *Let $P_{\mathfrak{q}}(T) = \det(T - \mathrm{Frob}_{\mathfrak{q}} \mid \mathbb{V}_2)$ for $\mathfrak{q} \in \{\mathfrak{l}, \bar{\mathfrak{l}}\}$, and for $\mathfrak{q} \nmid 3\ell$ let $\Omega_{\mathfrak{q}}(T) = \det(T - \mathrm{Frob}_{\mathfrak{q}} \mid H_c^1(\mathcal{S} \otimes \overline{\mathbb{F}}_q, \mathbb{V}))$. Then:*

(a) *$(P_{\mathfrak{l}}, P_{\bar{\mathfrak{l}}}) = (P^+, P^-)$ for one of the two sheaves $\mathbb{V}_\chi, \mathbb{V}_{\chi^{-1}}$ and (P^-, P^+) for the other;*

(b) *$\Omega_{\mathfrak{l}}(T)$ and $\Omega_{\bar{\mathfrak{l}}}(T)$ are $(T-1)(T^2 - 2\omega T + 49\omega^2)$ and $(T-1)(T^2 - 2\omega^2 T + 49\omega)$ in some order; in particular $T = 1$ is a root of both, and the other roots have absolute value 7.*

Proof. By the Grothendieck–Lefschetz formula and $H_c^0 = H_c^2 = 0$ (Proposition 3.3: $\mathbb{V}$ is irreducible and nontrivial), $\mathrm{tr}(\mathrm{Frob}_{\mathfrak{q}}^k \mid H_c^1) = -\sum_{s \in \mathbb{F}_{7^k} \smallsetminus \{0,1\}} \mathrm{tr}(\mathrm{Frob}_{\mathfrak{q}}^k \mid \mathbb{V}_s)$. We evaluated the sums of Lemma 3.8 at both primes and for all six values of m' (Appendix A, item C1); every value lies in $\mathbb{Z}[\omega]$. At $\mathfrak{l}$, the traces at $s = 2$ over $\mathbb{F}_7, \mathbb{F}_{49}, \mathbb{F}_{343}$ are $6 - 3\omega$, $-99 - 87\omega$, $-267 - 486\omega$ for the three values of m' in one class modulo 3 (the class $m' \equiv 2 \pmod 3$, called class I in item C1), and their complex conjugates $9 + 3\omega$, $-12 + 87\omega$, $219 + 486\omega$ for the other class; Newton's identities turn them into P^+ and P^- respectively. Since m' changes class with m, one sheaf has $P_{\mathfrak{l}} = P^+$ and the other $P_{\mathfrak{l}} = P^-$. For $s \in \mathbb{Q}$, Lemma 3.6 and purity give $\mathrm{tr}(\mathrm{Frob}_{\bar{\mathfrak{l}}} \mid \mathbb{V}_s) = \mathrm{tr}(\mathrm{Frob}_{\mathfrak{l}} \mid \mathbb{V}_s^{\mathsf{c}}) = 49\, \mathrm{tr}(\mathrm{Frob}_{\mathfrak{l}}^{-1} \mid \mathbb{V}_s) = \overline{\mathrm{tr}(\mathrm{Frob}_{\mathfrak{l}} \mid \mathbb{V}_s)}$, so $P_{\bar{\mathfrak{l}}} = \overline{P_{\mathfrak{l}}}$. This proves (a). The power sums of $\mathrm{Frob}_{\mathfrak{q}}$ on H_c^1 are $(1 + 2\omega,\ 95 + 94\omega,\ -285)$ or $(-1 - 2\omega,\ 1 - 94\omega,\ -285)$, at both primes and for both classes, and Newton's identities give the two cubics in (b). The roots of $T^2 - 2\omega T + 49\omega^2$ are $\omega(1 \pm 4\sqrt{-3})$, of absolute value 7, and those of the other quadratic are their conjugates. □

4. Inertia at the prime above 3

Theorem 4.1. *Let $\ell \neq 3$ be a prime and $s_0 \in K_{\mathfrak{p}}^\times$ with $v_3(s_0) > 15/2$. Then the semisimplification of $\mathbb{V}_{s_0}$ as a representation of $G_{K_{\mathfrak{p}}}$ is $1 \oplus \varepsilon_\ell^{-1} \oplus \varepsilon_\ell^{-2}$. In particular the inertia group $I_{\mathfrak{p}}$ acts unipotently on $\mathbb{V}_{s_0}$.*

Overview. For a prime $\mathfrak{q} \nmid 3\ell$ of K and s_0 with $v_{\mathfrak{q}}(s_0) > 0$, the analogue of Theorem 4.1 is Lemma 5.3 (b): $I_{\mathfrak{q}}$ acts on $\mathbb{V}_{s_0}$ through powers of the local monodromy γ_0 at $s = 0$, a single unipotent Jordan block. Its proof uses that $\mathbb{V}$ is lisse on $\mathcal{S}$ over $\mathcal{O}[1/3\ell]$ and tamely ramified along $0, 1, \infty$, so that by Abhyankar's lemma the covers trivializing it near $s = 0$ are Kummer covers of order prime to the residue characteristic. At $\mathfrak{p}$ neither input is available:

Proposition 3.4 gives a lisse sheaf only over $\mathcal{O}[1/3\ell]$, and the Kummer covers $y^9=1-x$ from which $\mathbb{V}$ is built have degree divisible by 3. For the same reason we cannot use the log-smooth (toroidal) models that describe tame degenerations, and we know of no semistable model of the surfaces over the 3-adic disc. We use instead one analytic fact, Lemma 4.3: over $\mathbb{C}_3$ the torsor $y^9=1-x$ is trivial on the disc $v_3(x)>5/2$, the disc of convergence of $(1-x)^{1/9}$. By Lemma 4.6 and its proof, $\mathbb{V}_s$ is H^2_c of the torus $x_0x_1x_2=s$ with coefficients in $\mathcal{L}_{e_0}(x_0)\otimes\mathcal{L}_{e_1}(x_1)\otimes\mathcal{L}_{e_2}(x_2)$. The three valuations $v_3(x_j)$ add up to $v_3(s)$, so if $v_3(s)>15/2$ then at every point of the torus some $v_3(x_j)$ exceeds $5/2$ and the jth Kummer factor is constant near it: $15/2=3\cdot 5/2$ is exactly the condition for the three regions $\{v_3(x_j)>5/2\}$ to cover the torus. Lemma 4.7 and Proposition 4.8 carry out this covering one convolution at a time, first for $\mathcal{L}_{e_1}\star\mathcal{L}_{e_2}$ on the discs $v_3(z)>d'$ with $d'>5=5/2+5/2$, then for $\mathbb{V}$ on the discs $v_3(s)>d$ with $d>15/2=5+5/2$, with a Mayer–Vietoris sequence for each cover. They show that every torsion sheaf $\mathbb{V}_n$ of Lemma 4.6 is unipotent of length at most 4 on the punctured disc $D_{\mathbb{C}_3}$, where $D=\{v_3(s)>d\}\subset\mathcal{S}^{\mathrm{an}}$ for a fixed $d>15/2$.

The length bound does not depend on n, and this is what passes to $\overline{\mathbb{Q}}_\ell$-coefficients: for $x\in D(K_\mathfrak{p})$ and $\gamma_1,\dots,\gamma_4$ in the group Π_D described below, $(\gamma_1-1)\cdots(\gamma_4-1)$ kills the stalk at $\bar{x}$ of every $\mathbb{V}_n$, hence the lattice $\varprojlim_n \mathbb{V}_{n,\bar{x}}$ (Corollary 4.12). The value 4 comes from the second Mayer–Vietoris sequence, which makes $\mathbb{V}_n|_{D_{\mathbb{C}_3}}$ an extension of two sheaves, each unipotent of length at most 2. This value is not sharp on $\mathbb{V}_{\bar{x}}$, since the product of any three factors γ_i-1 already kills $\mathbb{V}_{\bar{x}}$ (Proposition 4.14 (a)). Unipotence at each level with lengths growing with n would not suffice: a character with values in $1+\ell\mathbb{Z}_\ell$ and of infinite order is unipotent of length $\le n$ modulo ℓ^n for every n, but it is not unipotent. We use no description of the étale fundamental group of the punctured disc over $\mathbb{C}_3$ (which has covers of degree divisible by 3 that are not Kummer covers), only the subgroup Π_D of the geometric fundamental group of $\mathcal{S}$ that preserves the components over $D_{\mathbb{C}_3}$ of all finite étale covers (Definition 4.10); by the above, it acts unipotently on $\mathbb{V}_{\bar{x}}$. Section 4.3 shows that the decomposition group of a $K_\mathfrak{p}$-point of the disc normalizes Π_D and agrees, modulo Π_D, with the decomposition group of the tangential base point at $s=0$ (Lemma 4.13), which acts by conjugation on the inertia group $I_0\subset\Pi_D$ at $s=0$ through the cyclotomic character $\chi_{\mathrm{cyc}}\colon G_{K_\mathfrak{p}}\to\hat{\mathbb{Z}}^\times$ (whose ℓ-adic component is ε_ℓ); I_0 acts on $\mathbb{V}$ through the local monodromy γ_0. As γ_0 is a single Jordan block, the filtration of $\mathbb{V}_{s_0}$ defined by Π_D is a Galois-stable flag whose graded pieces carry characters $\beta_1,\beta_1\varepsilon_\ell^{-1},\beta_1\varepsilon_\ell^{-2}$ (Proposition 4.14). Geometry does not determine β_1 (Remark 4.19): Section 4.4 identifies it with the restriction of a global character of K unramified outside $\mathfrak{p}$, and the Frobenius data at the primes above 7 show that this character is trivial.

4.1. **Analytic setting.** Let $\mathbb{C}_3$ be the completion of an algebraic closure $\overline{K_\mathfrak{p}}$ of $K_\mathfrak{p}$. Analytic spaces are Berkovich spaces, and we use the étale cohomology of [19]; theorem numbers in brackets refer to that paper. For a $K_\mathfrak{p}$-analytic space X and a complete field $k\supset K_\mathfrak{p}$ we write $X_k=X\widehat{\otimes}_{K_\mathfrak{p}}k$, and for a scheme $\mathcal{X}$ of finite type over k we write $\mathcal{X}^{\mathrm{an}}$ for its analytification. For a point x of an analytic space and an analytic function f we put $v_3(f(x))=-\log_3|f(x)|\in\mathbb{R}\cup\{\infty\}$. On $\mathbb{G}_m^{\mathrm{an}}$ with coordinate x, and for $-\infty\le d_1<d_3\le\infty$, the open subset $\{d_1<v_3(x)<d_3\}$ is an *open annulus* (a *punctured open disc* if $d_3=\infty$), and the subsets $\{d_2\le v_3(x)<d_3\}$, $\{d_1<v_3(x)\le d_2\}$ with $d_1<d_2<d_3$ are *half-open annuli*. These sets do not contain the point 0. All of them are connected.

Coefficients. Let $E=\mathbb{Q}_\ell(\iota_\ell(\zeta_9))\subset\overline{\mathbb{Q}}_\ell$, let $\mathcal{O}_E$ be its ring of integers, λ a uniformizer and $\Lambda_n=\mathcal{O}_E/\lambda^n$. As $\ell\ne 3$, the elements 9 and $1-\zeta$ ($\zeta\in\mu_9(\mathcal{O}_E)\smallsetminus\{1\}$) are units of $\mathcal{O}_E$. Sheaves are étale sheaves of Λ_n-modules. We write $\mathcal{L}_{j,n}$ for the Kummer sheaf $\mathcal{L}_j$ defined

before Proposition 3.3, with coefficients Λ_n and extended by zero at $x = 1$. Statements about $\overline{\mathbb{Q}}_\ell$-coefficients are deduced at the end from statements at every level n (Corollary 4.12).

Facts from [19]. The torsion orders below are powers of ℓ, prime to the residue characteristic 3.

(B1) *Base change.* For a Hausdorff morphism $\varphi\colon Y \to X$ of k-analytic spaces, a sheaf $\mathcal{F}$ on Y and a point $x \in X$, the stalk of $\mathrm{R}^q\varphi_!\mathcal{F}$ at a geometric point over x is $H^q_c(Y_{\bar{x}}, \mathcal{F})$, where $Y_{\bar{x}}$ is the fiber of φ over x base-changed to the completion of an algebraic closure of the completed residue field $\mathcal{H}(x)$ [Thm. 5.3.1]; and $\mathrm{R}^q\varphi_!$ commutes with every base change $X' \to X$ [Thm. 7.7.1]. In particular, if k is algebraically closed, P and B are Hausdorff k-analytic spaces, $\mathrm{pr}\colon P \times B \to B$ is the projection and $\mathcal{G}$ is a sheaf on P, then $\mathrm{R}^q\mathrm{pr}_!(\mathrm{pr}_P^*\mathcal{G})$ is the constant sheaf on B with value $H^q_c(P, \mathcal{G})$ (base change along $B \to \mathcal{M}(k)$).

(B2) *Comparison.* For a compactifiable morphism φ of k-schemes of finite type and a torsion sheaf $\mathcal{F}$, $(\mathrm{R}^q\varphi_!\mathcal{F})^{\mathrm{an}} \cong \mathrm{R}^q\varphi_!^{\mathrm{an}}\mathcal{F}^{\mathrm{an}}$ [Thm. 7.1.1, Cor. 7.1.4].

(B3) *Excision and Mayer–Vietoris.* If $T \subset X$ is open with closed complement R, there is a long exact sequence $\cdots \to H^q_c(T, \mathcal{F}) \to H^q_c(X, \mathcal{F}) \to H^q_c(R, \mathcal{F}) \to H^{q+1}_c(T, \mathcal{F}) \to \cdots$ [Prop. 5.2.6(ii)]. Relative to a Hausdorff morphism φ, the exact sequences $0 \to j_!j^*\mathcal{F} \to \mathcal{F} \to i_*i^*\mathcal{F} \to 0$ and, for an open cover $X = U_1 \cup U_2$, $0 \to j_{12!}j_{12}^*\mathcal{F} \to j_{1!}j_1^*\mathcal{F} \oplus j_{2!}j_2^*\mathcal{F} \to \mathcal{F} \to 0$ give long exact sequences of the sheaves $\mathrm{R}^q\varphi_!$ of the restrictions, since $\mathrm{R}(\varphi j)_! = \mathrm{R}\varphi_! \circ j_!$ for an open immersion j and $i_* = i_!$ for a closed immersion i [Cor. 5.2.4, Cor. 5.2.5].

(B4) *Poincaré duality.* If k is algebraically closed, X is a separated smooth k-analytic curve and $\mathcal{F}$ is finite locally constant, then $H^q(X, \mathcal{F}^\vee(1)) \cong H^{2-q}_c(X, \mathcal{F})^\vee$ [Thm. 7.4.3]. The trace maps are compatible with composition [Thm. 7.2.1(b),(c)], so the duality is compatible with restriction from X to an open subset on one side and extension by zero on the other.

(B5) *Affinoid curves.* If k is algebraically closed and X is an affinoid domain in the analytification of a projective curve $\mathcal{X}$ whose complement is a disjoint union of open discs $D_1, \ldots, D_r$, and $x_i \in D_i(k)$, then restriction gives $H^1(\mathcal{X} \smallsetminus \{x_1, \ldots, x_r\}, \mathbb{Z}/\ell^n) \cong H^1(X, \mathbb{Z}/\ell^n)$ [Thm. 6.3.9 and the proof of Thm. 6.4.1]; and $H^q(X, \mathbb{Z}/\ell^n) = 0$ for $q \geq 2$ for every one-dimensional k-affinoid space X [Thm. 6.4.1(i)]. If a paracompact space X is an increasing union of closed analytic domains X_i and the images of $H^{q-1}(X_{i+1})$ and $H^{q-1}(X_{i+2})$ in $H^{q-1}(X_i)$ coincide for all i, then $H^q(X) = \varprojlim H^q(X_i)$ [Lemma 6.3.12].

(B6) *Local structure.* Étale morphisms are quasifinite and flat by definition [Def. 3.3.4], hence open maps [Prop. 3.2.7]; finite morphisms are closed maps (they induce compact maps of the underlying spaces [p. 28, after Lemma 1.3.7], and compact maps are closed [p. 14]). The analytification of an étale, resp. finite, resp. proper, morphism of schemes of finite type over k is étale [Prop. 3.3.11], resp. finite, resp. proper [Prop. 2.6.9]; so the analytification of a proper k-scheme is compact [Example 1.5.3(iii)]. If $\varphi\colon Y \to X$ is étale, $y \in Y$, and $\mathcal{H}(\varphi(y)) \to \mathcal{H}(y)$ is an isomorphism, then φ maps an open neighborhood of y isomorphically onto an open neighborhood of $\varphi(y)$ [Thm. 3.4.1, and the beginning of its proof: a morphism of Fét(X, x) that becomes an isomorphism in Fét$(\mathcal{H}(x))$ is an isomorphism of germs].

Besides (B1)–(B6), Lemma 4.2 (b) uses that a morphism of sheaves is an isomorphism if it is one on all stalks [Cor. 4.2.3]; otherwise we use from [19] only definitions and elementary properties from its §§1–5.

Locally constant and unipotent sheaves. Let X be a connected analytic space over an algebraically closed field. A sheaf $\mathcal{F}$ on X is *locally constant* if every point has an étale neighborhood U such that $\mathcal{F}|_U$ is isomorphic to the constant sheaf M_U of a finitely generated Λ_n-module M, and *constant* if $\mathcal{F} \cong M_X$. It is *unipotent of length* $\leq k$ if it is locally constant and has a filtration $0 = \mathcal{F}_0 \subset \mathcal{F}_1 \subset \cdots \subset \mathcal{F}_k = \mathcal{F}$ by locally constant subsheaves with constant quotients $\mathcal{F}_i/\mathcal{F}_{i-1}$.

Lemma 4.2. *Let X be a connected analytic space over an algebraically closed field.*

(a) *Kernels, images and cokernels of morphisms between locally constant sheaves are locally constant, and an extension of locally constant sheaves is locally constant.*

(b) *A morphism between constant sheaves $M_X \to N_X$ is induced by a homomorphism $M \to N$. A locally constant subsheaf of a constant sheaf is constant, and so is the quotient of a constant sheaf by a locally constant subsheaf.*

(c) *Let $\mathcal{F}$ be unipotent of length $\leq k$. Every locally constant subsheaf of $\mathcal{F}$, and the quotient of $\mathcal{F}$ by every locally constant subsheaf, is unipotent of length $\leq k$. An extension of a sheaf unipotent of length $\leq k'$ by $\mathcal{F}$ is unipotent of length $\leq k + k'$. The kernel and the cokernel of a morphism $\varphi\colon \mathcal{F} \to \mathcal{G}$, with $\mathcal{G}$ unipotent of length $\leq k'$, are unipotent of lengths $\leq k$ and $\leq k'$.*

Proof. A section of a constant sheaf S_U of finite sets is, étale-locally on U, a constant; since étale morphisms are open maps (B6), a section over U defines a locally constant function on the topological space $|U|$, hence a constant one if U is connected. As $\mathrm{Hom}(M_U, N_U)$ is the set of sections of the constant sheaf with value $\mathrm{Hom}_{\Lambda_n}(M, N)$, a morphism $M_U \to N_U$ is étale-locally, and on connected U globally, induced by a homomorphism $M \to N$; this proves the first assertion of (b), and the assertions of (a) about kernels, images and cokernels, which may be checked étale-locally. For an extension $0 \to \mathcal{A} \to \mathcal{B} \to \mathcal{C} \to 0$ with $\mathcal{A} = A_U$ and $\mathcal{C} = C_U$ constant, choose a surjection $\Lambda_n^r \to C$ with kernel C_0; étale-locally the r generators lift to sections of $\mathcal{B}$, giving $\psi\colon \Lambda_{n,U}^r \to \mathcal{B}$ over $\Lambda_{n,U}^r \to C_U$; then $\mathcal{B}$ is the quotient of $A_U \oplus \Lambda_{n,U}^r$ by the graph of the morphism $-\psi|_{C_{0,U}}\colon C_{0,U} \to A_U$, which is étale-locally induced by a homomorphism $C_0 \to A$; so $\mathcal{B}$ is étale-locally constant. For the second assertion of (b), let $\mathcal{G} \subset M_X$ be locally constant. By the first assertion, every point has an étale neighborhood U on which $\mathcal{G}|_U = (G_U)_U$ for a submodule $G_U \subset M$, so the stalk $\mathcal{G}_{\bar{x}} \subset M$ is a locally constant function of $x \in |X|$ (images of étale maps are open), hence constant, equal to G say; and $\mathcal{G} = G_X$ because a subsheaf is determined by its stalks. The quotient is $(M/G)_X$. For (c), if $\mathcal{F}' \subset \mathcal{F}$ is locally constant, the subsheaves $\mathcal{F}' \cap \mathcal{F}_i = \ker(\mathcal{F}' \to \mathcal{F}/\mathcal{F}_i)$ are locally constant by (a), and $(\mathcal{F}' \cap \mathcal{F}_i)/(\mathcal{F}' \cap \mathcal{F}_{i-1})$ is a locally constant subsheaf of the constant sheaf $\mathcal{F}_i/\mathcal{F}_{i-1}$, hence constant by (b). The quotient case is the same with the filtration $(\mathcal{F}_i + \mathcal{F}')/\mathcal{F}'$, whose graded pieces are quotients of $\mathcal{F}_i/\mathcal{F}_{i-1}$ by locally constant subsheaves. Extensions: concatenate the filtrations. Kernels and cokernels: $\ker\varphi \subset \mathcal{F}$ and $\mathrm{im}\,\varphi \subset \mathcal{G}$ are locally constant by (a), so by the first assertion of (c) $\ker\varphi$ is unipotent of length $\leq k$, and $\mathcal{G}/\mathrm{im}\,\varphi$ of length $\leq k'$. □

Lemma 4.3 (radius)**.** *Let k be a complete field containing $K_{\mathfrak{p}}$ and $j \in \mathbb{Z}/9 \smallsetminus \{0\}$. Over the open disc $\{v_3(x) > 5/2\}$ of $\mathbb{A}_k^{1,\mathrm{an}}$ the μ_9-torsor $y^9 = 1 - x$ has a section. Hence, if k is algebraically closed, $\mathcal{L}_{j,n}$ is constant on $\{v_3(x) > 5/2\}$, and for every analytic space Y*

over k and every analytic function g on Y with $v_3(g) > 5/2$ everywhere on Y, the pull-back $\mathcal{L}_{j,n}(g)$ is constant.

Proof. The coefficient of x^i in the binomial series $f(x) = \sum_i \binom{1/9}{i}(-x)^i$ has valuation $v_3\big(\prod_{0\le t<i}(1-9t)/(9^i\, i!)\big) = -2i - v_3(i!) = -(5i - s_3(i))/2$, where $s_3(i)$ is the sum of the ternary digits of i (Legendre). On a closed disc $\{v_3(x) \ge r\}$ the ith term has valuation at least $(r-5/2)i$, so for $r > 5/2$ the series converges there; it defines an analytic function on $\{v_3(x) > 5/2\}$, with coefficients in $\mathbb{Q}$, and $f^9 = 1 - x$ there (an identity of formal power series). So $y = f(x)$ is a section of the torsor, and over an algebraically closed k (where μ_9 is constant) the torsor is trivial and its push-out $\mathcal{L}_{j,n}$ is constant. The last assertion follows by pull-back. □

Lemma 4.4 (annuli)**.** *Let k be an algebraically closed complete field containing $K_{\mathfrak{p}}$, $-\infty \le d_1 < d_3 \le \infty$, and $A = \{d_1 < v_3(x) < d_3\} \subset \mathbb{G}_m^{\mathrm{an}}$.*

(a) *$H^0(A, \Lambda_n) = \Lambda_n$; $H^1(A, \Lambda_n(1))$ is free of rank one over Λ_n, generated by the Kummer class of the coordinate x; and $H^q(A, \Lambda_n) = 0$ for $q \ge 2$. Restriction to an open sub-annulus $A' = \{d_1' < v_3(x) < d_3'\}$, $d_1 \le d_1' < d_3' \le d_3$, is an isomorphism on H^q for every q.*

(b) *$H^1_c(A, \Lambda_n) \cong \Lambda_n$, $H^2_c(A, \Lambda_n) \cong \Lambda_n(-1)$, and $H^q_c(A, \Lambda_n) = 0$ for $q \ne 1, 2$. Extension by zero from A' to A is an isomorphism on H^q_c for every q.*

(c) *For $d_1 < d_2 < d_3$ the half-open annuli $Z = \{d_2 \le v_3(x) < d_3\}$ and $Z' = \{d_1 < v_3(x) \le d_2\}$ satisfy $H^q_c(Z, \mathcal{F}) = H^q_c(Z', \mathcal{F}) = 0$ for all q and every sheaf $\mathcal{F}$ on A that is unipotent of some length.*

Proof. It suffices to take coefficients $\mathbb{Z}/\ell^n$: as $\ell \ne 3$, E is unramified over $\mathbb{Q}_\ell$, so $\lambda^n \mathcal{O}_E = \ell^n \mathcal{O}_E$ and Λ_n is free of finite rank over $\mathbb{Z}/\ell^n$. (a) Write A as the union of the increasing sequence of closed annuli $B_i = \{a_i \le v_3(x) \le b_i\}$ with $a_i, b_i \in \mathbb{Q}$, $a_i \downarrow d_1$, $b_i \uparrow d_3$. The complement of B_i in $\mathbb{P}^{1,\mathrm{an}}$ is the disjoint union of the open discs $\{v_3(x) > b_i\} \cup \{0\}$ and $\{v_3(x) < a_i\} \cup \{\infty\}$, so by (B5), with $x_1 = 0$ and $x_2 = \infty$, restriction gives $H^1(\mathbb{G}_m, \mu_{\ell^n}) \cong H^1(B_i, \mu_{\ell^n})$, and $H^q(B_i, \mu_{\ell^n}) = 0$ for $q \ge 2$. By Kummer theory on $\mathbb{G}_m$ over k, $H^1(\mathbb{G}_m, \mu_{\ell^n}) = k[x^{\pm 1}]^\times / (k[x^{\pm 1}]^\times)^{\ell^n} = \mathbb{Z}/\ell^n$, generated by the class of x. The B_i are connected, so $H^0(B_i) = \mathbb{Z}/\ell^n$, and the restriction maps $H^q(B_{i+1}) \to H^q(B_i)$ are isomorphisms for $q = 0, 1$ (the Kummer class of x restricts to the Kummer class of x). The space A is paracompact (locally compact, Hausdorff and a countable union of compact sets), and the hypothesis of the last statement of (B5) holds in every degree $q \ge 1$, so $H^q(A) = \varprojlim_i H^q(B_i)$; with $H^0(A) = \mathbb{Z}/\ell^n$ (A is connected) this gives the first three assertions. The last one follows, as A' has the same description and restriction carries constants to constants and the Kummer class of x to that of x. (b) By Poincaré duality (B4), $H^q_c(A, \mathbb{Z}/\ell^n)$ is dual to $H^{2-q}(A, \mu_{\ell^n})$, and extension by zero is dual to restriction; so (b) follows from (a). (c) Z is closed in A with complement $\{d_1 < v_3(x) < d_2\}$, and extension by zero from the complement is an isomorphism by (b); by excision (B3), $H^*_c(Z, \mathbb{Z}/\ell^n) = 0$. The same holds for Z', with complement $\{d_2 < v_3(x) < d_3\}$. Every finitely generated Λ_n-module has a composition series with quotients Λ_1, a finite-dimensional $\mathbb{F}_\ell$-vector space, so $H^*_c(Z, M_Z) = 0$ for every constant sheaf, and by induction on the length $H^*_c(Z, \mathcal{F}|_Z) = 0$ for every unipotent $\mathcal{F}$. Likewise for Z'. □

Lemma 4.5. *Let k be as in Lemma 4.4, $j \in \mathbb{Z}/9 \smallsetminus \{0\}$, $r > 5/2$ and $U_r = \{v_3(x) < r\} \subset \mathbb{G}_m^{\mathrm{an}}$. Then $H^1_c(U_r, \mathcal{L}_{j,n})$ is free of rank one over Λ_n, and $H^q_c(U_r, \mathcal{L}_{j,n}) = 0$ for $q \ne 1$.*

Proof. The complement of U_r in $\mathbb{G}_m^{\mathrm{an}}$ is the closed half-open annulus $Z=\{r\le v_3(x)<\infty\}$, contained in $\{v_3(x)>5/2\}$, where $\mathcal{L}_{j,n}$ is constant (Lemma 4.3). So $H_c^*(Z,\mathcal{L}_{j,n})=0$ by Lemma 4.4 (c), and excision (B3) and comparison (B2) give $H_c^q(U_r,\mathcal{L}_{j,n})\cong H_c^q(\mathbb{G}_m^{\mathrm{an}},\mathcal{L}_{j,n})\cong H_c^q(\mathbb{G}_m,\mathcal{L}_{j,n})=H_c^q(\mathbb{G}_m\smallsetminus\{1\},\mathcal{L}_{j,n})$. On the curve $\mathbb{G}_m\smallsetminus\{1\}=\mathbb{P}^1\smallsetminus\{0,1,\infty\}$ the sheaf $\mathcal{L}_{j,n}$ is lisse of rank one, and its local monodromy at $x=1$ is multiplication by ζ^j for a primitive 9th root of unity ζ; since $\zeta^j-1\in\Lambda_n^\times$, the coinvariants H_c^2 vanish, and $H_c^0=0$ as the curve is affine. The same holds with coefficients Λ_1. The complex $P=\mathrm{R}\Gamma_c(\mathbb{G}_m\smallsetminus\{1\},\mathcal{L}_{j,n})$ is perfect and $P\otimes^{\mathbb{L}}_{\Lambda_n}\Lambda_1$ computes the cohomology with coefficients Λ_1, which is therefore concentrated in degree 1; so P is a free Λ_n-module placed in degree 1, of rank $-\chi_c=1$ (the curve has Euler characteristic -1 and the sheaf is tame of rank one). □

Lemma 4.6 (integral convolution)**.** *Let $(e_0,e_1,e_2)=m(1,7,4)$. Over an algebraically closed field of characteristic 0:*

(a) *for every $z\in\mathbb{G}_m$, $H_c^q(\mathbb{G}_m,\mathcal{L}_{e_1,n}(x)\otimes\mathcal{L}_{e_2,n}(z/x))$ vanishes for $q\neq1$ and is free of rank 2 for $z\neq1$, of rank 1 for $z=1$; so, with $\mathrm{pr}(x,z)=z$, the sheaf $\mathcal{M}_n=\mathrm{R}^1\mathrm{pr}_!(\mathcal{L}_{e_1,n}(x)\otimes\mathcal{L}_{e_2,n}(z/x))$ on $\mathbb{G}_m$ is the only nonzero direct image;*

(b) *the sheaf $\mathbb{V}_n=(\mathrm{R}^2f_!\Lambda_n)^{\chi^m}$ on $\mathcal{S}$ is defined and lisse over K, $(\varprojlim_n\mathbb{V}_n)\otimes_{\mathcal{O}_E}\overline{\mathbb{Q}}_\ell=\mathbb{V}$, and $\mathbb{V}_n\cong\mathrm{R}^1\mathrm{pr}_!(\mathcal{L}_{e_0,n}(x)\otimes\mathcal{M}_n(s/x))|_{\mathcal{S}}$, with $\mathrm{pr}(x,s)=s$.*

Proof. (a) For $z\neq1$ the sheaf $\mathcal{L}_{e_1,n}(x)\otimes\mathcal{L}_{e_2,n}(z/x)$ is the extension by zero of a lisse sheaf of rank one on $\mathbb{G}_m\smallsetminus\{1,z\}$; at $x=1$ only the first factor is ramified, with monodromy ζ^{e_1}; for $z=1$ it is the extension by zero of a lisse sheaf on $\mathbb{G}_m\smallsetminus\{1\}$ with monodromy $\zeta^{e_1+e_2}=\zeta^{2m}$ at $x=1$. In both cases the monodromy at 1 is a nontrivial root of unity ζ' with $\zeta'-1\in\Lambda_n^\times$, and the argument of Lemma 4.5 applies (Euler characteristics -2 and -1). The second assertion follows by proper base change. (b) The boundary argument in the proof of Proposition 3.4 works with coefficients Λ_n (9 is invertible in Λ_n, so the χ^m-projector is defined and exact), and gives $(\mathrm{R}^2f_!\Lambda_n)^{\chi^m}\cong(\mathrm{R}^2\tilde f_*\Lambda_n)^{\chi^m}$, which is lisse by smooth and proper base change. The second assertion is the definition of $\mathbb{V}$ (Definition 3.2). For the third, the computation in the proof of Proposition 3.3 (a) also works with coefficients Λ_n: on the χ^m-isotypic part, the direct image of Λ_n along the finite map $y\mapsto x=(1-y_j^9)_j$ is $\boxtimes_j\mathcal{L}_{e_j,n}(x_j)$, extended by zero where some $x_j=1$ (there the stabilizer contains a factor μ_9 on which χ^m is nontrivial). Hence $(\mathrm{R}f_!\Lambda_n)^{\chi^m}$ is the direct image of $\boxtimes_j\mathcal{L}_{e_j,n}(x_j)$ along $(x_0,x_1,x_2)\mapsto x_0x_1x_2$, which by proper base change and (a) is $\mathrm{R}\mathrm{pr}_!(\mathcal{L}_{e_0,n}(x)\otimes\mathcal{M}_n(s/x))[-1]$. Taking R^2 gives the claim. □

4.2. **Unipotence on the disc.** Let k be an algebraically closed complete field containing $K_{\mathfrak{p}}$ (below, $k=\mathbb{C}_3$, or the completion of an algebraic closure of the residue field of a point of a disc over $\mathbb{C}_3$). Let $(e_0,e_1,e_2)=m(1,7,4)$ and let $\mathcal{M}_n$, $\mathbb{V}_n$ be as in Lemma 4.6; we use the same letters for their analytifications, which by (B2) are given by the same formulas with the analytic $\mathbb{G}_m$.

Lemma 4.7. *Let $d'>5$ and $D'=\{v_3(z)>d'\}\subset\mathbb{G}_m^{\mathrm{an}}$ over k. For every n, $\mathcal{M}_n|_{D'}$ has a subsheaf $\mathcal{C}_1$ such that $\mathcal{C}_1$ and $\mathcal{M}_n|_{D'}/\mathcal{C}_1$ are constant, free of rank one over Λ_n. In particular $\mathcal{M}_n|_{D'}$ is unipotent of length ≤2.*

Proof. Let $\mathcal{U}=\mathbb{G}_m^{\mathrm{an}}\times D'$ with coordinates (x,z), $\mathrm{pr}(x,z)=z$, and $\mathcal{F}=\mathcal{L}_{e_1,n}(x)\otimes\mathcal{L}_{e_2,n}(z/x)$. By Lemma 4.6 (a), (B1) and (B2), $\mathcal{M}_n|_{D'}=\mathrm{R}^1\mathrm{pr}_!\mathcal{F}$ and $\mathrm{R}^q\mathrm{pr}_!\mathcal{F}=0$ for $q\neq1$. As $5/2<d'-5/2$, the open sets $\mathcal{U}_1=\{v_3(x)>5/2\}$ and $\mathcal{U}_2=\{v_3(x)<d'-5/2\}$ cover $\mathcal{U}$, and

$\mathcal{U}_{12} = \mathcal{U}_1 \cap \mathcal{U}_2 = A \times D'$ with $A = \{5/2 < v_3(x) < d' - 5/2\}$. Write $\mathcal{F}_*$ for the restriction of $\mathcal{F}$ to $\mathcal{U}_*$.

- On $\mathcal{U}_2 = U \times D'$, $U = \{v_3(x) < d' - 5/2\}$, we have $v_3(z/x) > d' - (d' - 5/2) = 5/2$, so $\mathcal{L}_{e_2,n}(z/x)$ is constant there (Lemma 4.3) and $\mathcal{F}_2 \cong \mathrm{pr}_x^*(\mathcal{L}_{e_1,n}|_U)$. By (B1), $\mathrm{R}^q\mathrm{pr}_!\mathcal{F}_2$ is constant with value $H_c^q(U, \mathcal{L}_{e_1,n})$, free of rank one for $q = 1$ and zero otherwise (Lemma 4.5, $r = d' - 5/2$).
- On $\mathcal{U}_{12}$ both factors are constant, and $\mathrm{R}^q\mathrm{pr}_!\mathcal{F}_{12}$ is constant with value $H_c^q(A, \Lambda_n)$: Λ_n for $q = 1$, $\Lambda_n(-1)$ for $q = 2$, zero otherwise (Lemma 4.4 (b)).
- On $\mathcal{U}_1$, $\mathcal{L}_{e_1,n}(x)$ is constant (Lemma 4.3), so $\mathcal{F}_1 \cong \mathcal{L}_{e_2,n}(z/x)$. The automorphism $(x, z) \mapsto (x', z) = (z/x, z)$ of $\mathcal{U}$ over D' carries $\mathcal{U}_1$ onto $\mathcal{W} = \{v_3(x') < v_3(z) - 5/2\}$ and $\mathcal{F}_1$ onto $\mathrm{pr}_{x'}^*\mathcal{L}_{e_2,n}$. The open subset $\mathcal{W}' = \{v_3(x') < d' - 5/2\} \times D'$ lies in $\mathcal{W}$, because $v_3(z) > d'$. The fiber of the closed complement $\mathcal{Z} = \mathcal{W} \smallsetminus \mathcal{W}'$ over a point z of D' is, over the completion k_z of an algebraic closure of $\mathcal{H}(z)$, the half-open annulus $\{d' - 5/2 \le v_3(x') < v_3(z) - 5/2\}$, which lies in $\{v_3(x') > 5/2\}$ since $d' > 5$; there $\mathcal{L}_{e_2,n}$ is constant. By Lemma 4.4 (c) over k_z and (B1), $\mathrm{R}\mathrm{pr}_!$ of the restriction to $\mathcal{Z}$ vanishes, so by excision (B3) and (B1) $\mathrm{R}^q\mathrm{pr}_!\mathcal{F}_1 \cong \mathrm{R}^q\mathrm{pr}_!(\mathrm{pr}_{x'}^*\mathcal{L}_{e_2,n}|_{\mathcal{W}'})$ is constant with value $H_c^q(\{v_3(x') < d' - 5/2\}, \mathcal{L}_{e_2,n})$, free of rank one for $q = 1$ and zero otherwise (Lemma 4.5).

The Mayer–Vietoris sequence (B3) for $\mathcal{U} = \mathcal{U}_1 \cup \mathcal{U}_2$ reads

$$0 = \mathrm{R}^0\mathrm{pr}_!\mathcal{F} \to \mathrm{R}^1\mathrm{pr}_!\mathcal{F}_{12} \xrightarrow{\alpha} \mathrm{R}^1\mathrm{pr}_!\mathcal{F}_1 \oplus \mathrm{R}^1\mathrm{pr}_!\mathcal{F}_2 \to \mathcal{M}_n|_{D'} \to \mathrm{R}^2\mathrm{pr}_!\mathcal{F}_{12} \to 0.$$

All terms other than $\mathcal{M}_n|_{D'}$ are constant, so $\mathcal{M}_n|_{D'}$ is an extension of constant sheaves and is locally constant (Lemma 4.2 (a)). So $\mathcal{C}_1 = \operatorname{coker}\alpha$ is constant (Lemma 4.2 (b)), and $\mathcal{M}_n|_{D'}/\mathcal{C}_1 \cong \mathrm{R}^2\mathrm{pr}_!\mathcal{F}_{12}$ is constant, free of rank one. On stalks α is an injective map $\Lambda_n \to \Lambda_n^2$; the image of 1 has a unit coordinate (otherwise it would be killed by λ^{n-1}), so $\operatorname{coker}\alpha$ is free of rank one. □

Proposition 4.8. *Let $d > 15/2$ and $D = \{v_3(s) > d\} \subset \mathcal{S}^{\mathrm{an}}$ over $K_{\mathfrak{p}}$, so that $D_k = \{v_3(s) > d\} \subset \mathbb{G}_m^{\mathrm{an}}$ over k. For every n, $\mathbb{V}_n|_{D_k}$ is unipotent of length ≤ 4.*

Proof. Choose d' with $5 < d' < d - 5/2$. Let $\mathcal{U} = \mathbb{G}_m^{\mathrm{an}} \times D_k$ with coordinates (x, s), $\mathrm{pr}(x, s) = s$, and $\mathcal{F} = \mathcal{L}_{e_0,n}(x) \otimes \mathcal{M}_n(s/x)$, so that $\mathbb{V}_n|_{D_k} = \mathrm{R}^1\mathrm{pr}_!\mathcal{F}$ (Lemma 4.6 (b), (B1), (B2)). As $d - d' > 5/2$, the open sets $\mathcal{U}_1 = \{v_3(x) > 5/2\}$ and $\mathcal{U}_2 = \{v_3(x) < d - d'\}$ cover $\mathcal{U}$, and $\mathcal{U}_{12} = A' \times D_k$ with $A' = \{5/2 < v_3(x) < d - d'\}$.

- On $\mathcal{U}_2 = U \times D_k$, $U = \{v_3(x) < d - d'\}$, we have $v_3(s/x) > d'$, so $\phi(x, s) = s/x$ maps $\mathcal{U}_2$ into $D' = \{v_3(z) > d'\}$, and by Lemma 4.7 $\mathcal{M}_n(s/x)|_{\mathcal{U}_2} = \phi^*(\mathcal{M}_n|_{D'})$ is an extension of a constant sheaf with value C_2 by a constant sheaf with value C_1, where C_1 and C_2, free of rank one over Λ_n, are the values of the constant sheaves $\mathcal{C}_1$ and $\mathcal{M}_n|_{D'}/\mathcal{C}_1$. So $\mathcal{F}_2$ is an extension of $\mathrm{pr}_x^*(\mathcal{L}_{e_0,n}|_U) \otimes C_2$ by $\mathrm{pr}_x^*(\mathcal{L}_{e_0,n}|_U) \otimes C_1$. By (B1) the $\mathrm{R}^q\mathrm{pr}_!$ of these two sheaves are constant, so by the long exact sequence $\mathrm{R}^q\mathrm{pr}_!\mathcal{F}_2$ is an extension of the kernel of a morphism between constant sheaves by the cokernel of another, hence unipotent of length ≤ 2 (Lemma 4.2).
- On $\mathcal{U}_{12}$, $\mathcal{L}_{e_0,n}(x)$ is constant and $\mathcal{M}_n(s/x)$ is an extension of constant sheaves as above, so $\mathrm{R}^q\mathrm{pr}_!\mathcal{F}_{12}$ is unipotent of length ≤ 2 in the same way.
- On $\mathcal{U}_1$, $\mathcal{L}_{e_0,n}(x)$ is constant and $\mathcal{F}_1 \cong \mathcal{M}_n(s/x)$. The automorphism $(x, s) \mapsto (z, s) = (s/x, s)$ carries $\mathcal{U}_1$ onto $\mathcal{W} = \{v_3(z) < v_3(s) - 5/2\}$ and $\mathcal{F}_1$ onto $\mathrm{pr}_z^*\mathcal{M}_n$. The open subset $\mathcal{W}' = \{v_3(z) < d - 5/2\} \times D_k$ lies in $\mathcal{W}$. The fiber of $\mathcal{Z} = \mathcal{W} \smallsetminus \mathcal{W}'$ over

a point s of D_k is the half-open annulus $\{d - 5/2 \le v_3(z) < v_3(s) - 5/2\}$ over k_s, contained in the open annulus $\{d' < v_3(z) < v_3(s) - 5/2\} \subset D'_{k_s}$ (as $d - 5/2 > d'$), on which $\mathcal{M}_n$ is unipotent by Lemma 4.7 over k_s. By Lemma 4.4 (c) and (B1), $\mathrm{R}\mathrm{pr}_!$ of the restriction to $\mathcal{Z}$ vanishes, so by excision $\mathrm{R}^q\mathrm{pr}_!\mathcal{F}_1 \cong \mathrm{R}^q\mathrm{pr}_!(\mathrm{pr}_z^*\mathcal{M}_n|_{\mathcal{W}'})$, which is constant by (B1).

In the Mayer–Vietoris sequence (B3), $\mathrm{R}^1\mathrm{pr}_!\mathcal{F}$ is an extension of $\ker(\mathrm{R}^2\mathrm{pr}_!\mathcal{F}_{12} \to \mathrm{R}^2\mathrm{pr}_!\mathcal{F}_1 \oplus \mathrm{R}^2\mathrm{pr}_!\mathcal{F}_2)$ by $\operatorname{coker}(\mathrm{R}^1\mathrm{pr}_!\mathcal{F}_{12} \to \mathrm{R}^1\mathrm{pr}_!\mathcal{F}_1 \oplus \mathrm{R}^1\mathrm{pr}_!\mathcal{F}_2)$. The sheaves $\mathrm{R}^q\mathrm{pr}_!\mathcal{F}_1 \oplus \mathrm{R}^q\mathrm{pr}_!\mathcal{F}_2$ and $\mathrm{R}^q\mathrm{pr}_!\mathcal{F}_{12}$ are unipotent of length ≤ 2, so by Lemma 4.2 (c) the kernel and the cokernel are unipotent of length ≤ 2, and $\mathbb{V}_n|_{D_k}$ is unipotent of length ≤ 4. □

4.3. **A substitute for the fundamental group of the disc.** Proposition 4.8 is a statement about sheaves on the punctured disc $D_{\mathbb{C}_3}$, on which $G_{K_\mathfrak{p}}$ acts only through the homeomorphisms $\tilde{\sigma} = \mathrm{id} \otimes \sigma$ defined below. This subsection turns it into a statement about the representations $\mathbb{V}_{s_0}$ of $G_{K_\mathfrak{p}}$. For this we need a group that acts on the fibers of $\mathbb{V}$, is normalized by the decomposition groups of the $K_\mathfrak{p}$-points of the disc, and contains, up to conjugation, the inertia group at $s = 0$. Rather than a fundamental group of the punctured disc, we use the étale fundamental group of $\mathcal{S}_{K_\mathfrak{p}}$, which contains these decomposition groups and admits the tangential base point at $s = 0$, and in it a closed subgroup Π_D of the geometric fundamental group: the elements that, on every finite étale cover, preserve the connected component over the disc attached to each point of the fiber (Definition 4.10); it is the image of the profinite fundamental group of $D_{\mathbb{C}_3}$, but we do not need that group (see the paragraph after Corollary 4.12). It acts on the fibers of the $\mathbb{V}_n$ unipotently, with length at most 4 for every n, because the $\mathbb{V}_n$ are unipotent of length at most 4 on the disc (Proposition 4.8, Lemma 4.11, and Corollary 4.12). As D is defined over $K_\mathfrak{p}$, Galois permutes these components, so the image of the section of $G_{K_\mathfrak{p}}$ at a $K_\mathfrak{p}$-point of the disc normalizes Π_D. As every component over the disc reaches $s = 0$, a suitable path from that point (Lemma 4.13 (a)) to the tangential base point at $s = 0$ conjugates Π_D to the corresponding group there, which contains the local inertia group I_0, and carries one section of $G_{K_\mathfrak{p}}$ to the other modulo Π_D (Lemmas 4.9 and 4.13). This carries the action of $G_{K_\mathfrak{p}}$ on I_0, through the cyclotomic character, to $\mathbb{V}_{s_0}$ (Proposition 4.14).

Fix $d > 15/2$ and $D = \{v_3(s) > d\} \subset \mathcal{S}^{\mathrm{an}}$ over $K_\mathfrak{p}$. For a geometric point $\bar{x}$ of $\mathcal{S}_{K_\mathfrak{p}}$ let $F_{\bar{x}}$ be the fiber functor on finite étale covers of $\mathcal{S}_{K_\mathfrak{p}}$, $\pi_1(\bar{x}) = \pi_1(F_{\bar{x}}) = \mathrm{Aut}(F_{\bar{x}})$ the étale fundamental group, and $\pi_1^{\mathrm{geo}}(\bar{x}) = \pi_1^{\mathrm{geo}}(F_{\bar{x}})$ the kernel of $\pi_1(\bar{x}) \to G_{K_\mathfrak{p}}$, that is $\pi_1(\mathcal{S}_{\overline{K}_\mathfrak{p}}, \bar{x})$ [68, Exposé V, §§4–7, and Exposé IX, Théorème 6.1]. The two kinds of base points give the following fiber functors.

- For $x \in D(K_\mathfrak{p})$, $F_{\bar{x}}(Y)$ is the set of $\overline{K}_\mathfrak{p}$-points of Y above x; $G_{K_\mathfrak{p}}$ acts on it by conjugating coordinates, and this defines a section $s_x \colon G_{K_\mathfrak{p}} \to \pi_1(\bar{x})$.
- The tangential base point $\vec{t} = \partial/\partial s$ at $s = 0$ [43, §15]. Let $\Omega = \bigcup_{e \ge 1} \overline{K}_\mathfrak{p}((s^{1/e}))$, with roots chosen so that $(s^{1/ee'})^{e'} = s^{1/e}$; it is algebraically closed (Puiseux). Then $F_{\vec{t}}(Y) = \mathrm{Hom}_{\mathcal{S}}(\operatorname{Spec}\Omega, Y)$. The group $G_{K_\mathfrak{p}}$ acts on Ω through the coefficients, fixing every $s^{1/e}$, which defines a section $s_{\vec{t}}$; the inertia group $I_0 = \mathrm{Gal}(\Omega/\overline{K}_\mathfrak{p}((s))) \cong \hat{\mathbb{Z}}(1)$ lies in $\pi_1^{\mathrm{geo}}(\vec{t})$, and $s_{\vec{t}}(\sigma)\,\theta\,s_{\vec{t}}(\sigma)^{-1} = \theta^{\chi_{\mathrm{cyc}}(\sigma)}$ for $\theta \in I_0$, where χ_{cyc} is the cyclotomic character, because σ fixes $s^{1/e}$ and acts on the eth roots of unity. (Points act on rings of functions on the left: $(\gamma y)^\# = \gamma \circ y^\#$.) If Y is defined over K, every point of $F_{\vec{t}}(Y)$ is defined over $\Omega_K = \bigcup_e \overline{K}((s^{1/e})) \subset \Omega$: the points of Y over Ω_K form a subset of $F_{\vec{t}}(Y)$, and both sets have $\deg Y$ elements, since Ω_K is algebraically

closed as well (Puiseux). So the fiber $\mathbb{V}_{\bar{t}}$ of Section 4.4, restricted to $G_{K_\mathfrak{p}}$, is the fiber of $\mathbb{V}$ at $F_{\bar{t}}$ with $G_{K_\mathfrak{p}}$ acting through $s_{\bar{t}}$, and I_0 acts on it through the local monodromy γ_0 at $s=0$. This is the fiber functor at the tangent vector $\partial/\partial s$ of [43, §15]: there a cover R gives the cover $R_{(s)} = \coprod_y T_y^*$ of the punctured tangent line at 0, mapping to it by the principal parts $z \mapsto a_y z^{e_y}$ of $R \to \mathbb{P}^1$ at the points y above 0 [43, 15.14–15.15, 15.18, 15.20–15.21]; here z is a local coordinate at y, defined over the field of definition of y, with $s = a_y z^{e_y} + \cdots$. A point of R over Ω specializing to y has a Puiseux expansion $z = c\, s^{1/e_y} + \cdots$ with $a_y c^{e_y} = 1$, and sending it to the point c of T_y^* is a bijection from $F_{\bar{t}}(R)$ onto the fiber of $R_{(s)}$ over $\partial/\partial s$, compatible with $G_{K_\mathfrak{p}}$ (which acts on the coefficients) and with I_0 (which multiplies s^{1/e_y}, hence c, by roots of unity).

Fix $b \in D(K_\mathfrak{p})$. For an open normal subgroup N of $\pi_1(\bar{b})$ let $Y_N \to \mathcal{S}_{K_\mathfrak{p}}$ be the corresponding connected Galois cover, G_N its automorphism group, $\bar{Y}_N$ the normalization of $\mathbb{P}^1_{K_\mathfrak{p}}$ in Y_N, and $Y_{N,D} \subset (Y_N \otimes_{K_\mathfrak{p}} \mathbb{C}_3)^{\mathrm{an}}$ the preimage of $D_{\mathbb{C}_3}$, a finite étale cover of $D_{\mathbb{C}_3}$. The group G_N acts on $(\bar{Y}_N \otimes \mathbb{C}_3)^{\mathrm{an}}$ through the first factor, and $\sigma \in G_{K_\mathfrak{p}}$ through $\tilde{\sigma} = \mathrm{id} \otimes \sigma$, a homeomorphism which commutes with G_N, preserves $Y_{N,D}$, and on $\mathbb{C}_3$-points is the conjugation of coordinates.

Lemma 4.9.

(a) *$Y_{N,D}$ has finitely many connected components; each is open and closed and maps onto $D_{\mathbb{C}_3}$. The groups G_N and $G_{K_\mathfrak{p}}$ (through $\tilde{\sigma}$) permute them.*

(b) *Every point $z \in \bar{Y}_N(\overline{K}_\mathfrak{p})$ above $s=0$ has a basis of open neighborhoods U in $(\bar{Y}_N \otimes \mathbb{C}_3)^{\mathrm{an}}$ with $U \smallsetminus \{z\}$ connected and contained in $Y_{N,D}$. Let $c_N(z)$ be the component of $Y_{N,D}$ containing these sets. Then $c_N(gz) = g\, c_N(z)$ for $g \in G_N$, $c_N(\sigma z) = \tilde{\sigma}\, c_N(z)$ for $\sigma \in G_{K_\mathfrak{p}}$, and every component of $Y_{N,D}$ is $c_N(z)$ for some z.*

Proof. (a) The cover $Y_{N,D} \to D_{\mathbb{C}_3}$ is finite étale of some degree r, as $D_{\mathbb{C}_3}$ is connected. If $Y_{N,D}$ is a disjoint union of nonempty open subsets, each of them is finite étale over $D_{\mathbb{C}_3}$, so its image is open and closed (B6), hence equal to $D_{\mathbb{C}_3}$, and the degrees add up to r. So there is a decomposition into at most r nonempty open and closed subsets that cannot be refined, and these are the connected components. The last assertion holds because g and $\tilde{\sigma}$ are homeomorphisms preserving $Y_{N,D}$. (b) The curve $\bar{Y}_N \otimes \mathbb{C}_3$ is smooth. Let t be a uniformizer at z; on an affine open neighborhood $\mathcal{Z}$ of z, t is regular, étale as a map $\mathcal{Z} \to \mathbb{A}^1$, and vanishes only at z. By (B6), t maps an open neighborhood of z in $\mathcal{Z}^{\mathrm{an}}$ isomorphically onto an open neighborhood of 0, so z has a basis of open neighborhoods U isomorphic to discs $\{|t| < \rho\}$, with $U \smallsetminus \{z\} \cong \{0 < |t| < \rho\}$ connected. For small ρ, U meets the fiber above 0 only in z and maps into $D_{\mathbb{C}_3} \cup \{0\}$, so $U \smallsetminus \{z\} \subset Y_{N,D}$. Two such neighborhoods contain a third, so $c_N(z)$ is well defined, and the equivariance holds because g and $\tilde{\sigma}$ are homeomorphisms carrying z to gz, σz and preserving $Y_{N,D}$. Let T be a component. If no point z above 0 lay in the closure of T in the compact space $(\bar{Y}_N \otimes \mathbb{C}_3)^{\mathrm{an}}$, each such z would have an open neighborhood disjoint from T, the complement of their union would be a compact set containing T whose image in $\mathbb{P}^{1,\mathrm{an}}$ misses 0, and T would not meet the preimage of some punctured disc $\{0 < |s| < \rho\}$, contradicting (a). So some z lies in the closure of T; then $U \smallsetminus \{z\}$ meets T for every U as above, and being connected it lies in T. □

For $x \in D(K_\mathfrak{p})$ and $y \in F_{\bar{x}}(Y_N)$, let $c(y)$ be the component of $Y_{N,D}$ containing y. For $y \in F_{\bar{t}}(Y_N)$, the morphism $\operatorname{Spec}\Omega \to Y_N \to \bar{Y}_N$ extends, by the valuative criterion, to the valuation ring $\bigcup_e \overline{K}_\mathfrak{p}[[s^{1/e}]]$ of Ω; let $\mathrm{sp}(y) \in \bar{Y}_N(\overline{K}_\mathfrak{p})$ be the image of its closed point, a

point above 0, and put $c(y)=c_N(\mathrm{sp}(y))$. In both cases $c(gy)=g\,c(y)$ for $g\in G_N$ and

$$c(s_F(\sigma)y)=\tilde{\sigma}\,c(y)\qquad(\sigma\in G_{K_\mathfrak{p}}),\tag{4.1}$$

where F is the fiber functor and s_F its section: for $F_{\bar{x}}$, $s_x(\sigma)y$ is the conjugate point $\tilde{\sigma}(y)$; for $F_{\vec{t}}$, $\mathrm{sp}(s_{\vec{t}}(\sigma)y)=\sigma(\mathrm{sp}(y))$ and Lemma 4.9 (b) applies. For $\theta\in I_0$, $\mathrm{sp}(\theta y)=\mathrm{sp}(y)$, since θ acts trivially on the residue field $\overline{K}_\mathfrak{p}$.

Definition 4.10. For $F=F_{\bar{x}}$ ($x\in D(K_\mathfrak{p})$) or $F=F_{\vec{t}}$, let $\Pi_D(F)$ be the closed subgroup of $\pi_1^{\mathrm{geo}}(F)$ of the elements γ with $c(\gamma y)=c(y)$ for every N and every $y\in F(Y_N)$.

So $I_0\subset\Pi_D(F_{\vec{t}})$. For $x\in D(K_\mathfrak{p})$, if $\gamma\in\pi_1^{\mathrm{geo}}(\bar{x})$ satisfies $c(\gamma y_N)=c(y_N)$ for one point $y_N\in F_{\bar{x}}(Y_N)$, then it does for all, because γ commutes with G_N and G_N acts transitively on $F_{\bar{x}}(Y_N)$.

Lemma 4.11. *Let $x\in D(K_\mathfrak{p})$, let $\mathcal{F}$ be a lisse sheaf of Λ_n-modules on $\mathcal{S}_{K_\mathfrak{p}}$, $T=\mathcal{F}_{\bar{x}}$, and $\mathcal{G}'\subset\mathcal{G}$ locally constant subsheaves of the analytification of $\mathcal{F}$ restricted to $D_{\mathbb{C}_3}$. Then $\mathcal{G}_{\bar{x}}$ and $\mathcal{G}'_{\bar{x}}$ are $\Pi_D(F_{\bar{x}})$-stable submodules of T, and if $\mathcal{G}/\mathcal{G}'$ is constant then $\Pi_D(F_{\bar{x}})$ acts trivially on $\mathcal{G}_{\bar{x}}/\mathcal{G}'_{\bar{x}}$. Hence, if $\mathcal{F}|_{D_{\mathbb{C}_3}}$ is unipotent of length $\le k$, then $(\gamma_1-1)\cdots(\gamma_k-1)T=0$ for all $\gamma_1,\dots,\gamma_k\in\Pi_D(F_{\bar{x}})$.*

Proof. Choose N such that $\mathcal{F}$ becomes constant on the connected scheme Y_N (the Y_N are cofinal among finite étale covers), a point $y\in F_{\bar{x}}(Y_N)$, and let $C=c(y)$. For $y'\in F_{\bar{x}}(Y_N)$ the stalk of the pull-back of $\mathcal{F}$ at y' is T; for a section f we write $f(y')\in T$ for its value there. A section f of $\mathcal{F}$ over the connected space C is the restriction of a section over Y_N (the pull-back of $\mathcal{F}$ to Y_N is the constant sheaf T, and Y_N and C are connected, so restriction from Y_N to C is the identity of T), that is, of a morphism $\varphi\colon Y_N\to\mathcal{E}$ to the finite étale cover $\mathcal{E}$ of $\mathcal{S}_{K_\mathfrak{p}}$ that represents $\mathcal{F}$; so $f(y')=F_{\bar{x}}(\varphi)(y')$, and naturality of $\gamma\in\pi_1(\bar{x})$ gives $f(\gamma y)=\gamma f(y)$ whenever $\gamma y\in C$, in particular for $\gamma\in\Pi_D(F_{\bar{x}})$. Now let $\mathcal{G}$ be a locally constant subsheaf. On the connected space C it is a locally constant subsheaf of the constant sheaf $\mathcal{F}|_C$, hence constant (Lemma 4.2 (b)); so every element of $\mathcal{G}_{\bar{x}}=\mathcal{G}_y$ is $f(y)$ for a section f of $\mathcal{G}$ over C, and then $\gamma f(y)=f(\gamma y)\in\mathcal{G}_{\gamma y}=\mathcal{G}_{\bar{x}}$. So $\mathcal{G}_{\bar{x}}$ is $\Pi_D(F_{\bar{x}})$-stable, and likewise $\mathcal{G}'_{\bar{x}}$. If $\mathcal{G}/\mathcal{G}'$ is constant, every element q of its stalk at $\bar{x}$ is the value of a section over $D_{\mathbb{C}_3}$. On C this section lifts to a section f of $\mathcal{G}$ (both $\mathcal{G}|_C$ and $(\mathcal{G}/\mathcal{G}')|_C$ are constant on the connected space C), and the images of $f(y)$ and of $f(\gamma y)=\gamma f(y)$ in $(\mathcal{G}/\mathcal{G}')_{\bar{x}}$ are both q. So γ acts trivially on $\mathcal{G}_{\bar{x}}/\mathcal{G}'_{\bar{x}}$. The last assertion follows by applying this to the filtration. □

Corollary 4.12. *For $x\in D(K_\mathfrak{p})$ and $\gamma_1,\dots,\gamma_4\in\Pi_D(F_{\bar{x}})$, $(\gamma_1-1)\cdots(\gamma_4-1)$ is zero on $\mathbb{V}_{\bar{x}}$.*

Proof. By Proposition 4.8 with $k=\mathbb{C}_3$ and Lemma 4.11, the product kills $\mathbb{V}_{n,\bar{x}}$ for every n, hence $\varprojlim_n\mathbb{V}_{n,\bar{x}}$ and $\mathbb{V}_{\bar{x}}=(\varprojlim_n\mathbb{V}_{n,\bar{x}})\otimes_{\mathcal{O}_E}\overline{\mathbb{Q}}_\ell$ (Lemma 4.6 (b)). □

Π_D and fundamental groups of the disc. Let $x\in D(K_\mathfrak{p})$. The finite étale covers of the connected analytic space $D_{\mathbb{C}_3}$ have a profinite fundamental group $\pi_1^{\mathrm{alg}}(D_{\mathbb{C}_3},\bar{x})$. De Jong's étale fundamental group $\pi_1(D_{\mathbb{C}_3},\bar{x})$ classifies a larger class of covers and maps to it with dense image [39, §2, Theorem 2.10]. Pulling finite étale covers of $\mathcal{S}_{K_\mathfrak{p}}$ back to $D_{\mathbb{C}_3}$ gives a homomorphism from $\pi_1^{\mathrm{alg}}(D_{\mathbb{C}_3},\bar{x})$ to $\pi_1(\bar{x})$, and its image is $\Pi_D(F_{\bar{x}})$. Indeed, an automorphism of a fiber functor preserves the fiber of each connected component of a cover. So the image preserves c, and hence lies in $\Pi_D(F_{\bar{x}})$ by $(*)$ and $(**)$ in the proof of Lemma 4.13. Conversely, $\pi_1^{\mathrm{alg}}(D_{\mathbb{C}_3},\bar{x})$ acts transitively on the fiber of each connected cover [39, Theorem 2.10 (i)], so for every N and $y\in F_{\bar{x}}(Y_N)$ the orbit of y under the image is $\{y'\in F_{\bar{x}}(Y_N):c(y')=c(y)\}$, which contains γy for every $\gamma\in\Pi_D(F_{\bar{x}})$. An element of $\pi_1(\bar{x})$

commutes with G_N, so it is determined on $F_{\bar{x}}(Y_N)$ by the image of y; hence, for each N, γ agrees on $F_{\bar{x}}(Y_N)$ with some element of the image; as the image is compact, hence closed, γ lies in it. So $\Pi_D(F_{\bar{x}})$ is also the closure of the image of $\pi_1(D_{\mathbb{C}_3}, \bar{x})$. Lemma 4.11 is then the case we need of the correspondence between locally constant sheaves of finite sets on $D_{\mathbb{C}_3}$ and finite sets with a continuous action of $\pi_1^{\mathrm{alg}}(D_{\mathbb{C}_3}, \bar{x})$, a correspondence that follows from [39, Lemma 2.3, Theorem 2.10]. By contrast, we know of no published form of Lemma 4.13. Finally, Π_D is not generated by conjugates of the inertia group at $s = 0$, which act trivially on the fibers of the covers that are étale over $s = 0$. For an integer $j > d - 1/2$, the cover $w^{3^j} = 1 - s$ of $\mathcal{S}_{K_\mathfrak{p}}$ is étale over $s = 0$, but it has no section over $D_{\mathbb{C}_3}$: a section would extend over $s = 0$ and be a root of unity times the binomial series of $(1 - s)^{1/3^j}$, which converges only on $v_3(s) > j + 1/2$ (as in the proof of Lemma 4.3). So $\Pi_D(F_{\bar{x}})$ fixes no point of the fiber of this cover at $\bar{x}$.

Lemma 4.13 (paths inside D)**.** *Let F, F' be fiber functors of the two kinds above.*

(a) *There is an isomorphism of fiber functors $\delta\colon F \Rightarrow F'$ with $c \circ \delta = c$ on every $F(Y_N)$. For every such δ, $\delta^{-1}\Pi_D(F')\delta = \Pi_D(F)$.*

(b) *For every $\sigma \in G_{K_\mathfrak{p}}$, $s_F(\sigma)$ normalizes $\Pi_D(F)$, and $\delta^{-1}s_{F'}(\sigma)\delta \in \Pi_D(F)\, s_F(\sigma)$.*

(c) *If $F' = F_{\vec{t}}$, then $\delta^{-1} I_0\, \delta \subset \Pi_D(F)$.*

Proof. We first describe π_1^{geo} through the covers $\mathcal{S}_L = \mathcal{S} \otimes_{K_\mathfrak{p}} L$, $L/K_\mathfrak{p}$ finite Galois. Such a cover is connected and Galois over $\mathcal{S}_{K_\mathfrak{p}}$ with group $\mathrm{Gal}(L/K_\mathfrak{p})$, so it is one of the Y_N. For both kinds of F, $F(\mathcal{S}_L) = \mathrm{Hom}_{K_\mathfrak{p}}(L, \overline{K}_\mathfrak{p})$ (for $F_{\vec{t}}$, $\mathrm{Hom}_{K_\mathfrak{p}}(L, \Omega) = \mathrm{Hom}_{K_\mathfrak{p}}(L, \overline{K}_\mathfrak{p})$, because $\overline{K}_\mathfrak{p}$ is algebraically closed in each field $\overline{K}_\mathfrak{p}((s^{1/e}))$), and $s_F(\sigma)$ acts on it by $\tau \mapsto \sigma \circ \tau$. The projection $\pi_1(F) \to G_{K_\mathfrak{p}}$ of [68, Exposé IX, Théorème 6.1] is induced by $\mathcal{S}_{K_\mathfrak{p}} \to \mathrm{Spec}\, K_\mathfrak{p}$, that is, by the action of $\pi_1(F)$ on the sets $F(\mathcal{S}_L)$; so

$$(*) \qquad \gamma \in \pi_1(F) \text{ lies in } \pi_1^{\mathrm{geo}}(F) \iff \gamma \text{ acts trivially on every } F(\mathcal{S}_L).$$

Moreover $L \otimes_{K_\mathfrak{p}} \mathbb{C}_3 = \prod_\tau \mathbb{C}_3$, the product over $\tau \in \mathrm{Hom}_{K_\mathfrak{p}}(L, \overline{K}_\mathfrak{p})$, so the preimage of $D_{\mathbb{C}_3}$ in $(\mathcal{S}_L \otimes_{K_\mathfrak{p}} \mathbb{C}_3)^{\mathrm{an}}$ is the disjoint union of copies D_τ of $D_{\mathbb{C}_3}$, and $c(\tau) = D_\tau$ for $\tau \in F(\mathcal{S}_L)$: for $F = F_{\bar{x}}$ the point (x, τ) lies in D_τ; for $F = F_{\vec{t}}$, the normalization of $\mathbb{P}^1_{K_\mathfrak{p}}$ in $\mathcal{S}_L$ is $\mathbb{P}^1_L$, and $\mathrm{sp}(\tau)$ is the point 0 of the copy of $\mathbb{P}^1_{\mathbb{C}_3}$ indexed by τ, whose punctured neighborhoods lie in D_τ. In particular

$$(**) \qquad c \text{ is injective on } F(\mathcal{S}_L).$$

Together, $(*)$ and $(**)$ show that an element $\gamma \in \pi_1(F)$ with $c(\gamma y) = c(y)$ for every N and every $y \in F(Y_N)$ fixes every $F(\mathcal{S}_L)$ pointwise, so it is geometric and lies in $\Pi_D(F)$; this is how the two sections are compared in (b). (a) Fix compatible points $y_N \in F(Y_N)$. An isomorphism δ is the same as a compatible family of points $y'_N \in F'(Y_N)$, with $\delta(gy_N) = gy'_N$ [68, Exposé V, §§4–7]; since c is G_N-equivariant, $c \circ \delta = c$ means $c(y'_N) = c(y_N)$ for all N. The set P_N of $y' \in F'(Y_N)$ with $c(y') = c(y_N)$ is finite and nonempty: for $F' = F_{\bar{x}'}$ because the component $c(y_N)$ maps onto $D_{\mathbb{C}_3} \ni x'$ (Lemma 4.9 (a)); for $F' = F_{\vec{t}}$ because $c(y_N) = c_N(z)$ for some z above 0 (Lemma 4.9 (b)), and some $y' \in F_{\vec{t}}(Y_N)$ has $\mathrm{sp}(y') = z$ (embed the completion of the function field of $Y_N \otimes \overline{K}_\mathfrak{p}$ at z, a field $\overline{K}_\mathfrak{p}((u))$ with $u^e \in s \cdot \overline{K}_\mathfrak{p}[[u]]^\times$, into Ω over $\overline{K}_\mathfrak{p}((s))$). For $N' \subset N$ the map $Y_{N'} \to Y_N$ carries $P_{N'}$ into P_N, as it carries components into components and commutes with sp. So $\varprojlim P_N \neq \emptyset$, which gives δ. For the second assertion: by $c \circ \delta = c$ and the bijectivity of δ on each $F(Y_N)$, $\gamma' \in \pi_1(F')$ preserves c if and only if $\delta^{-1}\gamma'\delta$ does, and by $(*)$ $\gamma' \in \pi_1^{\mathrm{geo}}(F')$ if and only if $\delta^{-1}\gamma'\delta \in \pi_1^{\mathrm{geo}}(F)$. (b) For $\gamma \in \Pi_D(F)$ and $y \in F(Y_N)$, by (4.1), $c(s_F(\sigma)\gamma s_F(\sigma)^{-1}y) = \tilde{\sigma}\, c(\gamma s_F(\sigma)^{-1}y) = \tilde{\sigma}\, c(s_F(\sigma)^{-1}y) = c(y)$;

and $s_F(\sigma)\gamma s_F(\sigma)^{-1}$ lies in the normal subgroup $\pi_1^{\mathrm{geo}}(F)$. So $s_F(\sigma)$ normalizes $\Pi_D(F)$. Next let $h=\delta^{-1}s_{F'}(\sigma)\delta\, s_F(\sigma)^{-1}\in\pi_1(F)$. For every N and $y\in F(Y_N)$, using $c\circ\delta^{-1}=c$ on $F'(Y_N)$, then (4.1) for F', then $c\circ\delta=c$, then (4.1) for F,

$$c(hy)=c\big(s_{F'}(\sigma)\,\delta s_F(\sigma)^{-1}y\big)=\tilde\sigma\,c\big(\delta s_F(\sigma)^{-1}y\big)=\tilde\sigma\,c\big(s_F(\sigma)^{-1}y\big)=c(y).$$

For $y\in F(\mathcal{S}_L)$ this gives $hy=y$ by $(**)$. So h acts trivially on every $F(\mathcal{S}_L)$, hence $h\in\pi_1^{\mathrm{geo}}(F)$ by $(*)$, and $h\in\Pi_D(F)$. (c) This follows from $I_0\subset\Pi_D(F_{\vec t})$ and (a). □

Proposition 4.14. *Let $x\in D(K_\mathfrak{p})$, write $V=\mathbb{V}_{\bar x}$ and $\Pi_D=\Pi_D(F_{\bar x})$, and for a subspace $W\subset V$ let IW be the span of the $(\gamma-1)w$ with $\gamma\in\Pi_D$ and $w\in W$; put $I^0V=V$ and $I^{j+1}V=I(I^jV)$.*

(a) *$V\supsetneq IV\supsetneq I^2V\supsetneq I^3V=0$, the quotients are lines, and $I^2V=V^{\Pi_D}$.*

(b) *The I^jV are stable under $s_x(G_{K_\mathfrak{p}})$, which acts on I^2V, IV/I^2V and V/IV by characters β_1, $\beta_1\varepsilon_\ell^{-1}$ and $\beta_1\varepsilon_\ell^{-2}$. So the semisimplification of $\mathbb{V}_x$ as a $G_{K_\mathfrak{p}}$-representation is $\beta_1\oplus\beta_1\varepsilon_\ell^{-1}\oplus\beta_1\varepsilon_\ell^{-2}$.*

(c) *The character β_1 of $G_{K_\mathfrak{p}}$ does not depend on $x\in D(K_\mathfrak{p})$.*

Proof. (a) By Corollary 4.12, $I^4V=0$; hence $IW\neq W$ for every nonzero Π_D-stable subspace W, and the chain I^jV decreases strictly until it reaches 0. Let $\delta\colon F_{\bar x}\Rightarrow F_{\vec t}$ be as in Lemma 4.13 and $\gamma'=\delta^{-1}\theta_0\delta$ for a topological generator θ_0 of I_0. Then $\gamma'\in\Pi_D$, and through δ it acts on V as γ_0 acts on $\mathbb{V}_{\vec t}$: a single unipotent Jordan block of length 3 (Proposition 3.3 (c)). So $0\neq(\gamma'-1)^2V\subset I^2V$, and as $\dim V=3$ the dimensions are $3,2,1,0$. Finally $I^2V\subset V^{\Pi_D}\subset\ker(\gamma'-1)$, and the last space is a line. (b) By Lemma 4.13 (b), $s_x(\sigma)$ normalizes Π_D, so $s_x(\sigma)I^jV=I^jV$ by induction on j, as $g(\gamma-1)w=(g\gamma g^{-1}-1)gw$ for $g=s_x(\sigma)$. Let $b_j(\sigma)$ be the scalar by which $s_x(\sigma)$ acts on the line $\mathrm{gr}^j=I^jV/I^{j+1}V$; on gr^j the group Π_D acts trivially. By Lemma 4.13 (b), (c), $\delta^{-1}s_{\vec t}(\sigma)\delta=h\,s_x(\sigma)$ with $h\in\Pi_D$, and applying the isomorphism $g\mapsto\delta^{-1}g\delta$ from $\pi_1(F_{\vec t})$ onto $\pi_1(F_{\bar x})$ to the relation $s_{\vec t}(\sigma)\,\theta_0\,s_{\vec t}(\sigma)^{-1}=\theta_0^{\chi_{\mathrm{cyc}}(\sigma)}$ (from the description of $F_{\vec t}$), with $\delta^{-1}\theta_0\delta=\gamma'$, gives $(hs_x(\sigma))\gamma'(hs_x(\sigma))^{-1}=\gamma'^{\chi_{\mathrm{cyc}}(\sigma)}$. The image of I_0 in $\mathrm{GL}(V)$ is topologically generated by the unipotent element γ', so it is the group $\{\exp(aN):a\in\mathbb{Z}_\ell\}$, $N=\log\gamma'$, through which $I_0\cong\hat{\mathbb{Z}}(1)$ acts via its quotient $\mathbb{Z}_\ell(1)$; hence $\gamma'^{\chi_{\mathrm{cyc}}(\sigma)}=\exp(\varepsilon_\ell(\sigma)N)=1+\varepsilon_\ell(\sigma)(\gamma'-1)+(\gamma'-1)^2(\cdots)$. The map $\mathrm{gr}^j\to\mathrm{gr}^{j+1}$ induced by $\gamma'-1$ is nonzero for $j=0,1$, since the composite of the two is induced by $(\gamma'-1)^2$, which is nonzero on V and kills IV. Comparing the maps $\mathrm{gr}^j\to\mathrm{gr}^{j+1}$ induced by both sides of $(hs_x(\sigma))(\gamma'-1)(hs_x(\sigma))^{-1}=\gamma'^{\chi_{\mathrm{cyc}}(\sigma)}-1$, on which h acts trivially, gives $b_{j+1}(\sigma)b_j(\sigma)^{-1}=\varepsilon_\ell(\sigma)$. With $\beta_1=b_2$ this is (b). (c) Let $x'\in D(K_\mathfrak{p})$ and $\delta\colon F_{\bar x}\Rightarrow F_{\bar x'}$ as in Lemma 4.13. Then δ^{-1} carries $\mathbb{V}_{\bar x'}^{\Pi_D(F_{\bar x'})}$ onto V^{Π_D} and $s_{x'}(\sigma)$ to $h\,s_x(\sigma)$ with $h\in\Pi_D$, which acts on V^{Π_D} as $s_x(\sigma)$ does. □

Since ε_ℓ is unramified at $\mathfrak{p}$, $I_\mathfrak{p}$ acts on the semisimplification of $\mathbb{V}_{s_0}$ through the single character $\beta_1|_{I_\mathfrak{p}}$, for every $s_0\in K_\mathfrak{p}^\times$ with $v_3(s_0)>15/2$. Theorem 4.1 is therefore equivalent to $\beta_1=1$.

4.4. **The limit at $s=0$.** Let $\mathbb{V}_{\vec t}$ be the fiber of $\mathbb{V}$ at the tangential base point $\vec t=\partial/\partial s$ at $s=0$, defined over K [43, §15], with its actions of G_K and of the local inertia group $I_0\cong\hat{\mathbb{Z}}(1)$ at 0, through the local monodromy γ_0. Let $\beta^{\lim}\colon G_K\to\overline{\mathbb{Q}}_\ell^\times$ be the character by which G_K acts on the line $\mathbb{V}_{\vec t}^{I_0}=\ker(\gamma_0-1)$.

Lemma 4.15. *The character $\beta^{\lim}$ has the following properties.*

(a) $\beta_1 = \beta^{\lim}|_{G_{K_\mathfrak{p}}}$.

(b) *For every prime $\mathfrak{q} \nmid 3\ell$ of K, $\beta^{\lim}$ is unramified at $\mathfrak{q}$ and $\beta^{\lim}(\mathrm{Frob}_\mathfrak{q}) = \alpha_0(\mathfrak{q})$, the eigenvalue of $\mathrm{Frob}_\mathfrak{q}$ on the stalk at 0 of $j_*\mathbb{V}$ over $\overline{\mathbb{F}}_q$.*

(c) *$\alpha_0(\mathfrak{q})$ is the unique root of weight 0 of the polynomial $\Omega_\mathfrak{q}(T)$ of Proposition 3.9, and $\alpha_0(\mathfrak{q}) \in \mu_6$.*

Proof. (a) Let $x \in D(K_\mathfrak{p})$, $\Pi_D = \Pi_D(F_{\bar{x}})$, and $\delta\colon F_{\bar{x}} \Rightarrow F_{\vec{t}}$ as in Lemma 4.13. By Lemma 4.13 (c), $\delta^{-1} I_0 \delta \subset \Pi_D$, so $\delta^{-1}(\mathbb{V}_{\vec{t}}^{I_0}) = \mathbb{V}_{\bar{x}}^{\delta^{-1} I_0 \delta}$ contains $\mathbb{V}_{\bar{x}}^{\Pi_D}$. Both are lines (a single Jordan block, and Proposition 4.14 (a)), so they are equal. For $\sigma \in G_{K_\mathfrak{p}}$, $\beta^{\lim}(\sigma)$ is the scalar by which $s_{\vec{t}}(\sigma)$ acts on $\mathbb{V}_{\vec{t}}^{I_0}$, that is, by which $\delta^{-1} s_{\vec{t}}(\sigma) \delta = h\, s_x(\sigma)$, with $h \in \Pi_D$ (Lemma 4.13 (b)), acts on $\mathbb{V}_{\bar{x}}^{\Pi_D}$. As h acts trivially on $\mathbb{V}_{\bar{x}}^{\Pi_D}$, this scalar is $\beta_1(\sigma)$.

(b) The geometric point $\operatorname{Spec} \Omega_K$ at which $\mathbb{V}_{\vec{t}}$ is the fiber (Section 4.3) lies over $\operatorname{Spec} \overline{K}\{s\}[1/s]$, where $\overline{K}\{s\} \subset \overline{K}[[s]]$ is the strict henselization of $\mathbb{P}^1_K$ at 0. The fundamental group of $\operatorname{Spec} \overline{K}\{s\}[1/s]$ is I_0, and G_K acts on $\overline{K}\{s\}$ and on Ω_K through the coefficients; so $\mathbb{V}_{\vec{t}}^{I_0} = \Gamma(\operatorname{Spec} \overline{K}\{s\}[1/s], \mathbb{V})$ is the stalk at 0 of $j_*\mathbb{V}$ over $\overline{K}$, with its natural action of G_K. Let $R \subset \overline{K}$ be the valuation ring, for the place of $\overline{K}$ that defines $G_{K_\mathfrak{q}}$, of the field fixed by $I_\mathfrak{q}$, a strict henselization of $\mathcal{O}$ at $\mathfrak{q}$; let A be the henselization of $R[s]$ at $(\mathfrak{m}_R, s)$, a strict henselization of $\mathbb{P}^1_{\mathcal{O}[1/3\ell]}$ at the point $s = 0$ of the fiber at $\mathfrak{q}$; and let $U_A = \operatorname{Spec} A[1/s]$. The group $G_{K_\mathfrak{q}}$ acts on A through its action on R, and $I_\mathfrak{q}$ acts trivially. By Abhyankar's lemma [68, Exposé XIII, Proposition 5.2 and Corollary 5.3], applied to the regular strictly local scheme $\operatorname{Spec} A$ and the divisor $s = 0$ (the tameness it assumes at the generic point of this divisor holds because the residue field there has characteristic 0), every finite étale cover of U_A becomes trivial over $A[s^{1/n}]$ for some n prime to q. So $\pi_1(U_A) \cong \varprojlim_{(n,q)=1} \mu_n$, and both I_0, through the strict localization of $\operatorname{Spec} A$ at the generic point of $s = 0$, and the inertia group at 0 of $\mathbb{P}^1_{\overline{\mathbb{F}}_q}$, through the special fiber, map onto it. As $\mathbb{V}$ is lisse on $\mathcal{S}$ over $\mathcal{O}[1/3\ell]$ (Proposition 3.4), restriction gives $G_{K_\mathfrak{q}}$-equivariant isomorphisms from $\Gamma(U_A, \mathbb{V})$ onto the stalks at 0 of $j_*\mathbb{V}$ over $\overline{K}$ and over $\overline{\mathbb{F}}_q$, where $G_{K_\mathfrak{q}}$ acts on the latter through $\mathrm{Gal}(\overline{\mathbb{F}}_q/\mathbb{F}_q)$. Hence $I_\mathfrak{q}$ acts trivially on $\mathbb{V}_{\vec{t}}^{I_0}$, and $\mathrm{Frob}_\mathfrak{q}$ acts on it as on the stalk at 0 of $j_*\mathbb{V}$ over $\overline{\mathbb{F}}_q$.

(c) Over $\overline{\mathbb{F}}_q$, $j_*\mathbb{V}$ is irreducible on $\mathbb{P}^1$ with stalks of dimensions $1, 2, 0$ at $0, 1, \infty$ (Proposition 3.3). Its Euler characteristic is $3 \cdot (-1) + 1 + 2 + 0 = 0$, and H^0 and H^2 vanish, so $H^*(\mathbb{P}^1, j_*\mathbb{V}) = 0$ and the sequence $0 \to j_!\mathbb{V} \to j_*\mathbb{V} \to \bigoplus_x (j_*\mathbb{V})_x \to 0$ gives $H^1_c(\mathcal{S}, \mathbb{V}) \cong (j_*\mathbb{V})_0 \oplus (j_*\mathbb{V})_1$. By Deligne's theory of weights [41, 1.8.4], since $\mathbb{V}$ is pure of weight 2 and γ_0 has a single Jordan block of length three, $(j_*\mathbb{V})_0$ is pure of weight 0; and $(j_*\mathbb{V})_1$, the invariants of a monodromy of finite order, is pure of weight 2. So $\alpha_0(\mathfrak{q})$ is the unique root of $\Omega_\mathfrak{q}$ of weight 0, that is, of absolute value 1 in every complex embedding. The coefficients of $\Omega_\mathfrak{q}$ lie in K (Lemma 3.7 and Newton's identities), and the roots of weight 0 are permuted by G_K, so $\alpha_0(\mathfrak{q}) \in K$. It is an algebraic integer, being an eigenvalue of Frobenius on $H^1_c(\mathcal{S}, \mathbb{V})$, which is the χ^m-part of H^3_c of the variety X over $\mathbb{F}_q$ [44, Exposé XXI, 5.5.3]. An algebraic integer of K all of whose conjugates have absolute value 1 is a root of unity, so $\alpha_0(\mathfrak{q}) \in \mu_6$. □

Proposition 4.16. *The character $\beta^{\lim}$ is trivial. Hence $\beta_1 = 1$, and Theorem 4.1 holds.*

Proof. By Lemma 4.15 (b)–(c), $\beta^{\lim}(\mathrm{Frob}_\mathfrak{q}) \in \mu_6$ for a set of primes $\mathfrak{q}$ of density one, so $(\beta^{\lim})^6 = 1$ by the Chebotarev density theorem. The values $\alpha_0(\mathfrak{q})$ do not depend on ℓ (they

are determined by the traces of Lemma 3.7), so for two primes ℓ,ℓ' the characters $\beta_\ell^{\lim}$ and $\beta_{\ell'}^{\lim}$, both of finite order, agree on almost all Frobenius elements and are equal. Hence $\beta^{\lim}$ is unramified outside $\mathfrak{p}$. The Galois group of the maximal abelian extension of K unramified outside $\mathfrak{p}$ is the inverse limit of the ray class groups $\mathrm{Cl}_{\mathfrak{p}^k}(K)$, which have order 3^{k-2} for $k\geq 2$ (the class number is one, $|(\mathcal{O}/\mathfrak{p}^k)^\times|=2\cdot 3^{k-1}$, and μ_6 injects); so it is a pro-3 group, and $\beta^{\lim}$ has order dividing 3. A cubic character of $K_\mathfrak{p}^\times$ is trivial on $1+\mathfrak{p}^4$, because the binomial series of $(1+x)^{1/3}$ converges for $v_3(x)>3/2$, that is for $x\in\mathfrak{p}^4$. So $\beta^{\lim}$ factors through $\mathrm{Cl}_{\mathfrak{p}^4}(K)\cong(\mathbb{Z}/3)^2$. This group is generated by the classes of $\mathfrak{l}$ and $\bar{\mathfrak{l}}$ (Appendix A, item C3). If $\ell\neq 7$, then $\mathfrak{l},\bar{\mathfrak{l}}\nmid 3\ell$, and Lemma 4.15 (b), (c) and Proposition 3.9 (b) give $\beta^{\lim}(\mathrm{Frob}_\mathfrak{l})=\alpha_0(\mathfrak{l})=1$ and $\beta^{\lim}(\mathrm{Frob}_{\bar{\mathfrak{l}}})=\alpha_0(\bar{\mathfrak{l}})=1$, so $\beta^{\lim}=1$. If $\ell=7$, then $\beta_7^{\lim}=\beta_5^{\lim}$, as shown above, and $\beta_5^{\lim}=1$ by the case $\ell=5$. Then $\beta_1=1$ by Lemma 4.15 (a). Finally, given $s_0\in K_\mathfrak{p}^\times$ with $v_3(s_0)>15/2$, choose d with $15/2<d<v_3(s_0)$; then $s_0\in D(K_\mathfrak{p})$, and Proposition 4.14 (b) with $\beta_1=1$ is Theorem 4.1. □

Remark 4.17 (the radius). We do not know whether 15/2 is optimal, but it is the natural constant for this argument. The holomorphic solution at $s=0$ of the hypergeometric differential equation underlying $\mathbb{V}$ is ${}_3F_2(a_0,a_1,a_2;1,1;s)$ with $\{a_0,a_1,a_2\}=\{1/9,4/9,7/9\}$ or $\{2/9,5/9,8/9\}$ (see the proof of Proposition 3.3). Its nth coefficient $\prod_j((a_j)_n/n!)$ is, up to sign, the product of the three binomial coefficients $\binom{-a_j}{n}$, each of the kind in Lemma 4.3; so its 3-adic valuation is $-(15n-3s_3(n))/2$, and the series converges exactly on $v_3(s)>15/2$. The same argument applied to a convolution of two Kummer sheaves gives, for the Legendre family $y^2=x(x-1)(x-\lambda)$ (two quadratic characters, at the prime 2, each trivial on $v_2(x)>2$), the disc $v_2(\lambda)>4$, and for the Hesse family $x^3+y^3+z^3=3\mu xyz$ with $s=\mu^{-3}$ (two cubic characters, at the prime 3, each trivial on $v_3(x)>3/2$), the disc $v_3(s)>3$. Since $v_2(j)=8-2v_2(\lambda)$ and $v_3(j)=3-v_3(s)$ when these valuations are positive, these discs are exactly the parts in $v_2(\lambda)>0$, resp. $v_3(s)>0$, of the loci $v(j)<0$ of potentially multiplicative reduction.

Remark 4.18 (a numerical check). For $s_0\in\mathbb{Z}\smallsetminus\{0,1\}$ let $L(s)$ be the L-function of $\mathrm{Ind}_K^{\mathbb{Q}}\mathbb{V}_{s_0}$, of degree 6, with gamma factor $\Gamma_{\mathbb{C}}(s)^2\Gamma_{\mathbb{C}}(s-1)$ (Lemma 3.5) and conductor $27\cdot 3^f N'$, where f is the conductor exponent of $\mathbb{V}_{s_0}$ at $\mathfrak{p}$ and N', prime to 3, is the product of $\mathrm{N}\,\mathfrak{q}^2$ over the primes $\mathfrak{q}\nmid 3$ of K dividing s_0 and of $\mathrm{N}\,\mathfrak{q}$ over those dividing s_0-1 to a power prime to 3 (Proposition 3.3 (c) and the proof of Lemma 5.3). Assume that $\Lambda(s)=\pm\Lambda(3-s)$ for the completed L-function. We computed the Euler factors at the primes $q\leq X$ other than 3, taking at the primes dividing $s_0(s_0-1)$ the factors given by specialization, and tested the functional equation numerically, with both signs: for $f\leq 2$, with a list of candidate Euler factors at 3 that contains every factor allowed by Theorem 4.1, and, at the points outside the disc, also for larger f. The Supplement, item S25, gives the details. For the choice of f, Euler factor at 3 and sign in the table, the functional equation holds to within about $2^{-66}\approx 10^{-20}$; every other choice tested misses it by at least $2^{-17}\approx 10^{-5}$.

s_0	$v_3(s_0)$	X	local data at $\mathfrak{p}$ singled out
3^8, 3^{10}	8, 10	$5\cdot 10^5$, $5.2\cdot 10^5$	$f=2$, Euler factor $1-3^{-s}$, sign $+1$
9	2	$5\cdot 10^5$	$f=14$, Euler factor 1, sign $+1$
-27	3	10^5	$f=6$, Euler factor 1, sign $+1$
$-2\cdot 3^7$	7	$3\cdot 10^5$	$f=4$, Euler factor 1, sign $+1$
-9, 27, 81, 243, 729	2–6	10^5	none with $f\leq 2$ (nor with the larger f tested)

Unipotent inertia forces $f \leq 2$ (the Swan conductor vanishes and there are nonzero invariants). So at $s_0 = 3^8$ and 3^{10} the data agree with Theorem 4.1, and the factor $1 - 3^{-s}$ suggests moreover that the monodromy operator is a single Jordan block. At the point $s_0 = 9$ of the Catalan solution, at $s_0 = -27$, and at $s_0 = -2 \cdot 3^7$ (where $v_3(s_0) = 7$, just outside the disc), the data indicate that inertia does not act unipotently. These computations are numerical and conditional on the functional equation and on the Euler factors at the primes dividing $s_0(s_0 - 1)$.

Remark 4.19. The arithmetic input at the primes above 7 in the proof of Proposition 4.16 cannot be replaced by geometry. For the Legendre family $y^2 = x(x-1)(x-\lambda)$ the character on the invariant line of the limit at $\lambda = 0$ is the quadratic character of -1, which is nontrivial. The analogous character for a twist of a family is changed by the twist, and only an arithmetic computation, here the one at the primes above 7, decides it.

5. The Frey representation of a solution

Parts II and III use the local properties of the Frey representation of a solution and its Frobenius data at the primes above 7 (Proposition 5.5), together with its irreducibility (Section 6).

5.1. **Inputs from Kraus.** Kraus [80, §6] writes a solution with the even variable first and normalizes its sign. His results for $p \geq 17$ assume that $E_{a,b}$ is modular, which is now known [25]; his note added in proof observes that it follows from the work of Conrad, Diamond and Taylor. We only need the following consequences, which do not depend on the normalization.

Proposition 5.1. *Let $p \geq 17$ be prime and let (a, b, c) be a solution of $x^3 + y^3 = z^p$ in coprime nonzero integers. Then*

(a) $3 \mid c$;
(b) $p \nmid c$;
(c) $7 \nmid abc$;
(d) *exactly one of a, b is even.*

Proof. Replacing (a, b, c) by (b, a, c) or by $(-a, -b, -c)$ we may assume that we are in Kraus's normalization. Then (a) and (d) are part of [80, Théorème 6.1] and (b) is [80, Lemme 6.4]. For (c), [80, Proposition 6.3 (ii)] gives $\bar{\rho}_{E_{a,b},p} \cong \bar{\rho}_{W,p}$, where $W\colon Y^2 = X^3 + 6X - 7$ has good reduction at 7 with $a_7(W) = 0$ (it reduces to $Y^2 = X^3 - X$, and $7 \equiv 3 \pmod 4$). The discriminant of $E_{a,b}$ is $-432c^{2p}$ and $c_4(E_{a,b}) = -144ab$, where ab is prime to c. If $7 \mid c$, then $E_{a,b}$ has multiplicative reduction at 7 and the congruence forces $a_7(W) \equiv \pm(7+1) \pmod p$, that is $p \mid 8$. If $7 \mid ab$, then $7 \nmid c$, $E_{a,b}$ has good reduction at 7, and modulo 7 it is $Y^2 = X^3 \pm (\text{a unit})^3$, a quadratic twist of $y^2 = x^3 + 1$, which has $a_7 = -4$; the congruence then gives $0 \equiv \pm 4 \pmod p$. Both are impossible for $p \geq 17$. □

5.2. **The parameter.** Let $p \geq 17$ and let (a, b, c) be a solution in coprime nonzero integers. As a, b are coprime, $p \nmid a$ or $p \nmid b$. Choose $(u, w) \in \{(a, b), (b, a)\}$ with $p \nmid u$ (when both choices are possible, nothing depends on which is made; see Remark 5.10), and put

$$s_0 = \frac{c^p}{u^3} = 1 + \left(\frac{w}{u}\right)^3 \in \mathbb{Q} \smallsetminus \{0, 1\}.$$

Lemma 5.2. *We have $v_3(s_0) = p\, v_3(c) \geq p$, and $s_0 \equiv 2 \pmod 7$ (in $\mathbb{Z}_{(7)}$).*

Proof. By Proposition 5.1 (a), $3 \mid c$, and $3 \nmid u$ by coprimality. By Proposition 5.1 (c), u, w, c are prime to 7; the cube of a unit modulo 7 is ± 1, and $(w/u)^3 \equiv -1$ would give $7 \mid c$; so $(w/u)^3 \equiv 1$ and $s_0 \equiv 2 \pmod 7$. □

5.3. **Tame specialization.**

Lemma 5.3. *Let $\mathfrak{q} \nmid 3\ell$ be a prime of K and $s_0 \in K \smallsetminus \{0, 1\}$.*

(a) *If $v_\mathfrak{q}(s_0) = 0$ and $v_\mathfrak{q}(s_0 - 1) = 0$, then $\mathbb{V}_{s_0}$ is unramified at $\mathfrak{q}$.*
(b) *If $v_\mathfrak{q}(s_0) > 0$, then there is a G_K-stable lattice in $\mathbb{V}_{s_0}$ on which $I_\mathfrak{q}$ acts through $\sigma \mapsto \gamma_0^{v_\mathfrak{q}(s_0) t_\ell(\sigma)}$, where $t_\ell \colon I_\mathfrak{q} \to \mathbb{Z}_\ell(1)$ is the ℓ-adic tame character (Section 2) and γ_0 is a unipotent automorphism of the lattice with $(\gamma_0 - 1)^3 = 0$.*
(c) *If $v_\mathfrak{q}(s_0 - 1) > 0$ and $3 \mid v_\mathfrak{q}(s_0 - 1)$, then $I_\mathfrak{q}$ acts trivially on $\mathbb{V}_{s_0}$.*
(d) *If $s_0 = z_0/u^3$ with $z_0, u \in \mathcal{O}$, $\mathfrak{q} \mid u$ and $\mathfrak{q} \nmid z_0$, then $I_\mathfrak{q}$ acts on $\mathbb{V}_{s_0}$ by the scalar character $\kappa_u^{n_\infty}|_{I_\mathfrak{q}}$.*

Proof. $\mathbb{V}$ is lisse on $\mathcal{S}$ over $\mathcal{O}[1/3\ell]$ and tamely ramified along $0, 1, \infty$ (Propositions 3.3 and 3.4); fix a lattice $\mathbb{V}^\circ$. In (a) the point s_0 extends to a point of $\mathcal{S}$ over the local ring at $\mathfrak{q}$, so $\mathbb{V}_{s_0}$ is unramified. Otherwise s_0 reduces modulo $\mathfrak{q}$ to one of the points $0, 1, \infty$; let z be the local coordinate s, $s - 1$ or $1/s$ there. By Abhyankar's lemma [68, Exposé XIII, 5.3], étale locally near that point a finite étale cover of $\mathcal{S}$ trivializing $\mathbb{V}^\circ/\ell^n$ is a disjoint union of Kummer covers, each obtained by extracting an ith root of z times a unit, with i prime to the residue characteristic. Pulling back along s_0 shows that $I_\mathfrak{q}$ acts on $\mathbb{V}^\circ_{s_0}$ through the composite of the tame Kummer map $\sigma \mapsto (\sigma(z(s_0)^{1/i})/z(s_0)^{1/i})_i \in \hat{\mathbb{Z}}'(1)$ with the local monodromy of $\mathbb{V}^\circ$ at that point, since the value of the unit at s_0 contributes nothing on inertia. Now use Proposition 3.3 (c). In (b) the point is 0 and the monodromy is the unipotent γ_0 on $\mathbb{V}^\circ$, with $(\gamma_0 - 1)^3 = 0$ (one Jordan block of length three). In (c) the point is 1 and the monodromy factors through μ_3; the image of $\sigma \in I_\mathfrak{q}$ in μ_3 is $\sigma((s_0 - 1)^{1/3})/(s_0 - 1)^{1/3}$, which is 1 because $s_0 - 1$ is a unit times a cube in $K_\mathfrak{q}$ and $\mathfrak{q} \nmid 3$. In (d) the point is ∞ and the monodromy factors through μ_9; the image of $\sigma \in I_\mathfrak{q}$ is $\sigma((1/s_0)^{1/9})/(1/s_0)^{1/9} = \sigma(u^{1/3})/u^{1/3} \cdot \sigma(z_0^{-1/9})/z_0^{-1/9}$, and the second factor is 1 on $I_\mathfrak{q}$ since $\mathfrak{q} \nmid 9z_0$. So the image is $\kappa_u(\sigma) \in \mu_3$, which acts by the scalar $\iota_\ell(\kappa_u(\sigma))^{n_\infty}$ (Proposition 3.3). □

5.4. **The Frey representation.** Fix a prime $p \geq 17$ with $p \equiv 1 \pmod 3$ and a solution, with u, w, s_0 as above. Take $\ell = p$.

Definition 5.4. The *Frey representation* of the solution is

$$\rho = \mathbb{V}_{s_0} \otimes \kappa_u^{-n_\infty} \colon G_K \to \mathrm{GL}_3(\overline{\mathbb{Q}}_p),$$

where $n_\infty \in \{1, 2\}$ is as in Proposition 3.3, and $\bar\rho \colon G_K \to \mathrm{GL}_3(\overline{\mathbb{F}}_p)$ is its reduction (Section 2).

Proposition 5.5. *The representation ρ has the following properties.*

(a) *ρ is unramified at every prime $\mathfrak{q} \nmid 3pc$. For every prime $\mathfrak{q} \nmid 3pcuw$ the characteristic polynomial of $\rho(\mathrm{Frob}_\mathfrak{q})$ has coefficients in $\mathcal{O}$, so ρ has coefficients in K.*
(b) *$\bar\rho$ is unramified at every prime $\mathfrak{q} \nmid 3p$.*
(c) *$\rho^\mathsf{c} \cong \rho^\vee \otimes \varepsilon_p^{-2}$, and hence $\bar\rho^\mathsf{c} \cong \bar\rho^\vee \otimes \bar\varepsilon_p^{-2}$.*
(d) *$I_\mathfrak{p}$ acts on ρ through $\kappa_u^{-n_\infty}|_{I_\mathfrak{p}}$ times a unipotent representation, so every constituent of $\bar\rho|_{I_\mathfrak{p}}$ is $\bar\kappa_u^{-n_\infty}|_{I_\mathfrak{p}}$.*

(e) *ρ is unramified at $\mathfrak{l}$ and $\bar{\mathfrak{l}}$, and the characteristic polynomial of $\rho(\mathrm{Frob}_\mathfrak{q})$, $\mathfrak{q} \in \{\mathfrak{l}, \bar{\mathfrak{l}}\}$, is $P_\mathfrak{q}(\xi_\mathfrak{q}^{-1}T)$ with $\xi_\mathfrak{q} = \kappa_u(\mathrm{Frob}_\mathfrak{q})^{-n_\infty} \in \mu_3$ and $P_\mathfrak{q}$ as in Proposition 3.9.*

(f) *For each prime $v \mid p$ of K, $\rho|_{G_{K_v}}$ is crystalline with Hodge–Tate weights $\{0,1,2\}$.*

Proof. (a) If $\mathfrak{q} \nmid 3pcuw$, then s_0 and $s_0 - 1 = (w/u)^3$ are $\mathfrak{q}$-units, so $\mathbb{V}_{s_0}$ is unramified at $\mathfrak{q}$ by Lemma 5.3 (a); if $\mathfrak{q} \mid w$, it is unramified at $\mathfrak{q}$ by Lemma 5.3 (c) ($v_\mathfrak{q}(s_0 - 1) = 3v_\mathfrak{q}(w)$); if $\mathfrak{q} \mid u$, then $I_\mathfrak{q}$ acts on $\mathbb{V}_{s_0}$ by $\kappa_u^{n_\infty}$ by Lemma 5.3 (d) (with $z_0 = c^p$), which the twist cancels. The character κ_u is unramified outside $3u$. For $\mathfrak{q} \nmid 3pcuw$ the coefficients lie in $\mathcal{O}$ by Lemma 3.7, which applies because s_0 reduces to a point of $\mathcal{S}$ modulo $\mathfrak{q}$, and because κ_u takes values in $\mu_3 \subset \mathcal{O}^\times$.

(b) By (a) it remains to treat $\mathfrak{q} \mid c$, $\mathfrak{q} \nmid 3$ (note $p \nmid c$). By Lemma 5.3 (b), on a G_K-stable lattice $I_\mathfrak{q}$ acts through powers of $\gamma_0^{p\, v_\mathfrak{q}(c)}$, since $v_\mathfrak{q}(s_0) = p\, v_\mathfrak{q}(c)$ and κ_u is unramified at $\mathfrak{q}$. As $(\gamma_0 - 1)^3 = 0$ and $p \geq 3$, $\gamma_0^p = 1 + p(\gamma_0 - 1) + \binom{p}{2}(\gamma_0 - 1)^2 \equiv 1 \pmod{p}$; so $I_\mathfrak{q}$ acts trivially on the reduction of this lattice, hence on $\bar{\rho}$.

(c) By Lemma 3.6 (as $s_0 \in \mathbb{Q}$), $\mathbb{V}_{s_0}^\mathsf{c} \cong \mathbb{V}_{s_0}^\vee \otimes \varepsilon_p^{-2}$, and $(\kappa_u^{-n_\infty})^\mathsf{c} = \kappa_u^{n_\infty}$ because $u \in \mathbb{Z}$.

(d) By Lemma 5.2, $v_3(s_0) \geq 17 > 15/2$, so $I_\mathfrak{p}$ acts unipotently on $\mathbb{V}_{s_0}$ by Theorem 4.1.

(e) By Lemma 5.2, s_0 reduces modulo $\mathfrak{l}$ and $\bar{\mathfrak{l}}$ to $2 \in \mathcal{S}(\mathbb{F}_7)$, so $\mathbb{V}_{s_0}$ is unramified there and $\mathrm{Frob}_\mathfrak{q}$ has characteristic polynomial $P_\mathfrak{q}$ on it; κ_u is unramified at $\mathfrak{q}$ since $7 \nmid 3u$.

(f) This is Proposition 5.6 below. □

5.5. **Crystallinity at p.**

Proposition 5.6. *Let $p \geq 5$, $p \equiv 1 \pmod 3$, let $v \mid p$ be a prime of K (so $K_v = \mathbb{Q}_p$), and let $s_0 \in \mathbb{Q} \smallsetminus \{0,1\}$ with $v_p(s_0) = 0$. Suppose that either $s_0 \not\equiv 1 \pmod p$, or $s_0 - 1 = t_1^3$ with $t_1 \in p\mathbb{Z}_{(p)}$. Then $\mathbb{V}_{s_0}|_{G_{K_v}}$ (with $\ell = p$) is crystalline with Hodge–Tate weights $\{0,1,2\}$.*

For the Frey representation, $v_p(s_0) = 0$ by Proposition 5.1 (b) and $p \nmid u$; if $p \nmid w$ then $s_0 \not\equiv 1 \pmod p$, and if $p \mid w$ then $s_0 - 1 = (w/u)^3$ with $w/u \in p\mathbb{Z}_{(p)}$. Since κ_u is unramified at v and of finite order, Proposition 5.5 (f) follows.

For a finite extension L of $\mathbb{Q}_p$ let $L_0 = W(k_L)[1/p]$ be its maximal subfield unramified over $\mathbb{Q}_p$, and for a p-adic representation V' of G_L, with coefficients in a finite extension E of $\mathbb{Q}_p$, let $D_{\mathrm{st},L}(V') = (B_\mathrm{st} \otimes_{\mathbb{Q}_p} V')^{G_L}$, a module over $L_0 \otimes_{\mathbb{Q}_p} E$ with a Frobenius φ and a monodromy operator N. Since $B_\mathrm{st}^{G_L} = L_0$ and $B_\mathrm{st}^{N=0} = B_\mathrm{cris}$ [113, §2.1, $(4)_\mathrm{st}$ and $(6)_\mathrm{st}$], V' is semistable when $\dim_{L_0} D_{\mathrm{st},L}(V') = \dim_{\mathbb{Q}_p} V'$, and crystalline when moreover $N = 0$ on $D_{\mathrm{st},L}(V')$ [113, Definition 2.2.7].

Lemma 5.7. *Let L/F be a finite Galois extension of finite extensions of $\mathbb{Q}_p$, with inertia subgroup $I(L/F)$, and let V' be a p-adic representation of G_F whose restriction to G_L is semistable. Then $\mathrm{Gal}(L/F)$ acts on $D_{\mathrm{st},L}(V')$, through $g \otimes g$ for $g \in G_F$, semilinearly with respect to its action on L_0 and commuting with N. If $N = 0$ on $D_{\mathrm{st},L}(V')$ and $I(L/F)$ acts trivially on it, then V' is crystalline.*

Proof. Since G_L is normal in G_F, the action $g \otimes g$ preserves $D = D_{\mathrm{st},L}(V')$ and factors through $\mathrm{Gal}(L/F)$; it commutes with N because N commutes with G_F on B_st. The group $\mathrm{Gal}(L/F)$ acts on L_0 through $\mathrm{Gal}(L/F)/I(L/F) \cong \mathrm{Gal}(L_0F/F) \cong \mathrm{Gal}(L_0/F_0)$. If $I(L/F)$ acts trivially on D, then D is an L_0-vector space with a semilinear action of $\mathrm{Gal}(L_0/F_0)$, so $D = L_0 \otimes_{F_0} D^{\mathrm{Gal}(L/F)}$ by Galois descent for vector spaces (Hilbert's Theorem 90). As $(B_\mathrm{st} \otimes V')^{G_F} = D^{\mathrm{Gal}(L/F)}$, this gives $\dim_{F_0} D_{\mathrm{st},F}(V') = \dim_{L_0} D = \dim_{\mathbb{Q}_p} V'$, so V' is semistable; and $N = 0$ on $D_{\mathrm{st},F}(V') \subset D$, so V' is crystalline. □

For the rest of this subsection let $p \geq 5$, let v be a prime of K above p (so K_v is unramified over $\mathbb{Q}_p$ and contains μ_3; $K_v = \mathbb{Q}_p$ if $p \equiv 1 \pmod 3$), let $\bar{F} = \overline{K}_v$, and let $F = K_v(\zeta_9) \subset \bar{F}$, where ζ_9 is the image of $\tau_0(\zeta_9)$ under an embedding $\overline{K} \hookrightarrow \overline{K}_v$ over K that defines the decomposition group $G_{K_v} \subset G_K$ (Section 2); F is an unramified extension of K_v. Over F the twisted forms of Section 3.1 split: $X_s \otimes_K F = \{\prod_j (1 - y_j^9) = s\}$, $H = \mu_9^3$ acting coordinatewise, and G_F acts trivially on $H(\overline{K})$; we use the model $\tilde{X}^\flat \otimes \mathcal{O}_F$ of Proposition 3.4 (a) in this split form. Let $t_1 \in \mathfrak{m}_F \smallsetminus \{0\}$, $s_0 = 1 + t_1^3$, let $t_0 \in \bar{F}$ with $t_0^3 = t_1$, and $K' = F(t_0)$; as $\mu_3 \subset F$, the extension K'/F is Galois of degree 1 or 3 and tamely ramified. Let k' be the residue field of K', π a uniformizer, and $e = v_{K'}(t_0) \geq 1$. For $\lambda \in \mu_9$ let $\delta(\lambda) = (\lambda, \lambda, \lambda) \in \mu_9^3$.

The case $s_0 \equiv 1 \pmod p$ of Proposition 5.6, where s_0 reduces to the point 1, over which the model of Proposition 3.4 is not smooth, needs the following semistable model. It is used through parts (c) and (d): the diagonal μ_9 fixes the double curves pointwise and χ^m is nontrivial on it, so the χ^m-part of the cohomology of the special fiber comes only from the components, which forces $N = 0$; and inertia acts on each component through the diagonal μ_3, on which χ^m is trivial, so it acts trivially on that part (proof of Proposition 5.6).

Lemma 5.8. *There is a regular scheme $\mathcal{X}$, projective and flat over $\mathcal{O}_{K'}$, with the following properties.*

(a) *Its generic fiber is $\tilde{X}_{s_0} \otimes_F K'$.*

(b) *Its special fiber Y is a reduced divisor with strict normal crossings and without triple points. Its components are Z', Ξ and, if $e \geq 2$, $E_1, \dots, E_{e-1}$, where Ξ is the Fermat surface $y_0^9 + y_1^9 + y_2^9 + t^9 = 0$ in $\mathbb{P}^3_{k'}$, Z' is the blow-up of $\tilde{X}_1^\flat \otimes k'$ at its singular point $y = 0$, and each E_r is a $\mathbb{P}^1$-bundle over the Fermat curve $C\colon y_0^9 + y_1^9 + y_2^9 = 0$ in $\mathbb{P}^2_{k'}$. The components form a chain $Z', E_1, \dots, E_{e-1}, \Xi$, and each double curve maps isomorphically to C.*

(c) *$H = \mu_9^3$ acts on $\mathcal{X}$ by $\mathcal{O}_{K'}$-automorphisms, extending its action on the generic fiber and mapping every component of Y to itself. The diagonal $\mu_9 \subset H$ fixes every point of every double curve.*

(d) *For each $\gamma \in \mathrm{Gal}(K'/F)$ there is an automorphism $\gamma_{\mathcal{X}}$ of the scheme $\mathcal{X}$ over $\mathrm{Spec}(\gamma)$ which extends $1 \times \mathrm{Spec}(\gamma)$ on $\tilde{X}_{s_0} \times_F K'$ and commutes with H. If γ lies in the inertia subgroup, then $\gamma_{\mathcal{X}}$ maps every component Y_a of Y to itself, and its restriction to Y_a is the restriction of an element δ_a of the diagonal $\mu_3 \subset H$.*

Proof. The family over the t-line. Let $B = \mathrm{Spec}\, \mathcal{O}_F[t, (1+t^9)^{-1}]$, mapped to $\bar{\mathcal{S}}$ by $s = 1 + t^9$, and $\mathcal{Y} = \tilde{X}^\flat \times_{\bar{\mathcal{S}}} B$, projective over B, with H acting over B. By Proposition 3.4 (a), $\mathcal{Y} \to B$ is smooth outside the closed subset $\Sigma = \{y = 0,\ t = 0\}$, a section of $\mathcal{Y}$ over $\mathcal{O}_F$; so $\mathcal{Y}$ is smooth over $\mathcal{O}_F$ outside Σ. Near Σ, $\mathcal{Y}$ is the hypersurface $\Phi = 0$ in $\mathbb{A}^4_{\mathcal{O}_F}$, with coordinates y_0, y_1, y_2, t and

$$\Phi = \textstyle\prod_j (1 - y_j^9) - 1 - t^9 = -(y_0^9 + y_1^9 + y_2^9 + t^9) + \sum_{i<j} y_i^9 y_j^9 - y_0^9 y_1^9 y_2^9.$$

For $\zeta \in \mu_3$, $\phi_\zeta(x, t) = (x, \zeta t)$ is an automorphism of $\mathcal{Y}$ over the automorphism $t \mapsto \zeta t$ of B (which preserves $s = 1 + t^9$); it commutes with H and fixes the fiber $t = 0$ pointwise.

One blow-up. Let $\mathcal{Y}'$ be the blow-up of $\mathcal{Y}$ along Σ. Near Σ it is the strict transform of $\mathcal{Y}$ in the blow-up of $\mathbb{A}^4_{\mathcal{O}_F}$ along the zero section, and H and ϕ_ζ act on it. In the chart $y_1 = y_0\eta_1$, $y_2 = y_0\eta_2$, $t = y_0\tau$ we have $\Phi = y_0^9 G$ with

$$G = -(1 + \eta_1^9 + \eta_2^9 + \tau^9) + y_0^9(\eta_1^9 + \eta_2^9 + \eta_1^9\eta_2^9) - y_0^{18}\eta_1^9\eta_2^9,$$

so $\mathcal{Y}' = \{G = 0\}$ there, and $\partial G/\partial\tau = -9\tau^8$, $\partial G/\partial\eta_1 = -9\eta_1^8(1-y_0^9)(1-y_0^9\eta_2^9)$, $\partial G/\partial\eta_2 = -9\eta_2^8(1-y_0^9)(1-y_0^9\eta_1^9)$. On the exceptional divisor $y_0 = 0$ these do not vanish simultaneously on $G = 0$ (otherwise $G = -1$), and off it $\mathcal{Y}' = \mathcal{Y} \smallsetminus \Sigma$. The charts of y_1 and y_2 are symmetric, and in the chart $y_j = t\eta_j$ ($j = 0, 1, 2$) we have $\Phi = t^9 G_t$ with $G_t \equiv -(1+\eta_0^9+\eta_1^9+\eta_2^9) \pmod t$, whose partial derivatives $-9\eta_j^8$ at $t = 0$ do not all vanish on $G_t = 0$. Hence $\mathcal{Y}'$ is smooth over $\mathcal{O}_F$; its exceptional divisor Ξ is the Fermat surface $y_0^9 + y_1^9 + y_2^9 + t^9 = 0$ in $\mathbb{P}^3_{\mathcal{O}_F}$, smooth over $\mathcal{O}_F$ as $p \neq 3$; and the divisor of the function $t = y_0\tau$ near $t = 0$ is $Z' + \Xi$, where Z', the strict transform of the fiber $\tilde{X}_1^\flat \otimes \mathcal{O}_F$ of $\mathcal{Y}$ over $t = 0$, is $\{\tau = 0\}$ in the chart above. Its fibers are irreducible: over an algebraically closed field of characteristic $\neq 3$ the surface $\prod_j(1-y_j^9) = 1$ is a hypersurface whose open part $y_0y_1y_2 \neq 0$ is an étale μ_9^3-cover, $y_j^9 = 1-x_j$, of an open part of the torus $x_0x_1x_2 = 1$, connected because the functions $1 - x_j$ have the distinct prime divisors $\{x_j = 1\}$ on the torus, so that they are independent modulo ninth powers; and the open part is dense, the complement having dimension 1. The intersection $C = Z' \cap \Xi = \{y_0 = \tau = 0,\ 1 + \eta_1^9 + \eta_2^9 = 0\}$ is the Fermat curve $y_0^9 + y_1^9 + y_2^9 = 0$ in the plane $t = 0$ of $\mathbb{P}^3$, and along C one of $\partial G/\partial\eta_1$, $\partial G/\partial\eta_2$ is a unit. So near each point of C there are étale coordinates (ξ, τ, η) of $\mathcal{Y}'$ over $\mathcal{O}_F$ (in the chart of a coordinate y_j that does not vanish at the point; we write it for $j = 0$), with $\xi = y_0$ and $\eta \in \{\eta_1, \eta_2\}$, in which $Z' = \{\tau = 0\}$, $\Xi = \{\xi = 0\}$ and $t = \xi\tau$; and Z', Ξ and C are smooth over $\mathcal{O}_F$. Off C, near $t = 0$, the morphism $\mathcal{Y}' \to B$ is smooth (on $Z' \smallsetminus C$ because $\mathcal{Y} \to B$ is smooth off Σ; on $\Xi \smallsetminus C$ because τ is a unit there, so that t is a coordinate). In these coordinates $\delta(\lambda)$ acts by $(\xi, \tau, \eta) \mapsto (\lambda\xi, \lambda^{-1}\tau, \eta)$ and ϕ_ζ by $(\xi, \tau, \eta) \mapsto (\xi, \zeta\tau, \eta)$. Globally, ϕ_ζ is the identity on Z' and acts on $\Xi \subset \mathbb{P}^3$ by $[y : t] \mapsto [y : \zeta t] = [\zeta^{-1}y : t]$, as $\delta(\zeta^{-1})$ does; and $\delta(\lambda)$ fixes C pointwise, since it acts on the plane $t = 0$ by $[y : 0] \mapsto [\lambda y : 0]$.

Base change and resolution. Since $t_0 \in \mathfrak{m}_{K'}$ and $1 + t_0^9 = s_0$ is a unit, $t \mapsto t_0$ is an $\mathcal{O}_{K'}$-point of B. Let $\mathcal{X}_0 = \mathcal{Y}' \times_B \operatorname{Spec}\mathcal{O}_{K'}$, projective over $\mathcal{O}_{K'}$, with generic fiber $\tilde{X}_{s_0}^\flat \otimes_F K'$ (the center Σ lies over $t = 0$). Its special fiber is $(Z' + \Xi) \otimes k'$. Off C, $\mathcal{X}_0$ is smooth over $\mathcal{O}_{K'}$; near a point of C it is étale over $\operatorname{Spec}\mathcal{O}_{K'}[\xi, \tau, \eta]/(\xi\tau - \pi^e u)$ with $u \in \mathcal{O}_{K'}^\times$, which is flat over $\mathcal{O}_{K'}$. So $\mathcal{X}_0$ is flat. If $e = 1$ it is regular with reduced normal-crossings special fiber, and we put $\mathcal{X} = \mathcal{X}_0$. If $e \geq 2$, blow up $e - 1$ times the ideal of the strict transform of $\Xi \otimes k'$ (locally (ξ, π) at the first step). For the ring $\mathcal{O}_{K'}[\xi, \tau]/(\xi\tau - \pi^e u)$ the blow-up of (ξ, π) has two charts: $\xi = \pi\xi_1$, with equation $\xi_1\tau = \pi^{e-1}u$; and $\pi = \xi\pi_1$, with $\tau = \xi^{e-1}\pi_1^e u$, which is regular with special fiber $\xi\pi_1 = 0$, reduced with normal crossings. In the first chart the special fiber $\xi_1\tau = 0$ consists of the strict transform $\{\xi_1 = 0\}$ of $\Xi \otimes k'$ and of a new component $E_1 = \{\tau = 0\}$, mapping to C with fiber coordinate ξ_1; the strict transform of $Z' \otimes k'$ lies in the second chart. By induction the result $\mathcal{X}$ is regular, and its special fiber is $Y = Z' \cup E_1 \cup \cdots \cup E_{e-1} \cup \Xi$, where E_r is the $\mathbb{P}^1$-bundle over C that in the chart after r blow-ups is $\{\tau = \pi = 0\}$, with fiber coordinate $\xi_r = \xi/\pi^r$; consecutive components meet transversally along sections isomorphic to C, and there are no triple points. Off C the ideal blown up is invertible, so nothing changes there. This proves (a) and (b).

The actions. H acts on $\mathcal{Y}'$ over B, hence on $\mathcal{X}_0$ over $\mathcal{O}_{K'}$; it preserves $\Xi \otimes k'$, so it acts on $\mathcal{X}$, and it maps every component to itself. Since $\delta(\lambda)$ fixes C pointwise and commutes with the projections of the double curves to C, which are isomorphisms, the diagonal μ_9 fixes every double curve pointwise. This proves (c). Let $\gamma \in \operatorname{Gal}(K'/F)$ and $\zeta = \gamma(t_0)/t_0 \in \mu_3$. The morphisms $\phi_\zeta \circ \operatorname{pr}_1 \colon \mathcal{X}_0 \to \mathcal{Y}'$ and $\operatorname{Spec}(\gamma) \circ \operatorname{pr}_2 \colon \mathcal{X}_0 \to \operatorname{Spec}\mathcal{O}_{K'}$ induce the same morphism to B (both pull t back to $\zeta t_0 = \gamma(t_0)$), so they define an automorphism $\gamma_{\mathcal{X}_0}$ of $\mathcal{X}_0$ over $\operatorname{Spec}(\gamma)$. On the generic fiber it is $1 \times \operatorname{Spec}(\gamma)$ on $\tilde{X}_{s_0}^\flat \times_F K'$, because ϕ_ζ does not move the point of $\tilde{X}^\flat$; it commutes with H; and it preserves $\Xi \otimes k'$, so it lifts to an

automorphism $\gamma_{\mathcal{X}}$ of $\mathcal{X}$. Now let γ be in the inertia subgroup. Then γ acts trivially on k', and $\gamma(\pi)/\pi \equiv \lambda \pmod{\pi}$ for some $\lambda \in \mu_3$ (the value of the tame character). On the components Z' and Ξ the claim is global: there $\gamma_{\mathcal{X}}$ restricts to the base change of ϕ_ζ (as γ is trivial on k'), which is the identity on Z' and equals $\delta(\zeta^{-1})$ on Ξ. Let $1 \le r \le e-1$. In the model obtained after r blow-ups, let U_r be the affine chart lying over the chart of y_0 in which, at each of the r steps, the ideal blown up is generated by π; so $y_0 = \pi^r \xi_r$ on U_r, the coordinate ring of U_r is generated over $\mathcal{O}_{K'}$ by ξ_r, τ, η_1, η_2, and $\xi_r\tau = \pi^{e-r}u$ there. Let $U = U_r \smallsetminus \{\xi_r = 0\}$. The centers of the later blow-ups lie in $\{\xi_r = 0\}$, so U is an open subscheme of $\mathcal{X}$; its coordinate ring is generated over $\mathcal{O}_{K'}$ by $\xi_r^{\pm 1}$, τ, η_1 and η_2; and $E_r \cap U = \{\tau = \pi = 0\}$ is a nonempty, hence dense, open subscheme of the irreducible scheme E_r, with coordinate ring generated over k' by $\xi_r^{\pm 1}$, η_1 and η_2. Both $\gamma_{\mathcal{X}}$ and every $\delta(\lambda')$ map U to itself, since they multiply y_0, y_1, y_2, t, π and each $\xi_i = y_0/\pi^i$ by units. Both pull-backs fix η_1 and η_2; pull-back by $\gamma_{\mathcal{X}}$ is $\xi_r \mapsto (\pi/\gamma(\pi))^r \xi_r$, $\tau \mapsto \zeta\tau$, together with γ on $\mathcal{O}_{K'}$, and pull-back by $\delta(\lambda')$ is $\xi_r \mapsto \lambda'\xi_r$, $\tau \mapsto \lambda'^{-1}\tau$, and the identity on $\mathcal{O}_{K'}$. On the coordinate ring of $E_r \cap U$ both are k'-algebra maps, and they agree when $\lambda' = \lambda^{-r}$. So $\gamma_{\mathcal{X}}$ and $\delta(\lambda^{-r})$ agree on the dense open subscheme $E_r \cap U$ of the reduced scheme E_r, hence on E_r, as $\mathcal{X}$ is separated. This proves (d). □

Lemma 5.9. *Let $\mathcal{X}$ and Y be as in Lemma 5.8, and let $D = H^2_{\text{log-crys}}(Y/W(k')) \otimes \mathbb{Q}$ be the log-crystalline (Hyodo–Kato) cohomology of Y (with the log structure induced by $\mathcal{X}$) over $W(k')$ (with the log structure $\mathbb{N} \to W(k')$, $1 \mapsto 0$). It is a K_0'-vector space with φ and N.*

(a) *The restriction of $H^2(\tilde{X}_{s_0} \otimes \bar{F}, \mathbb{Q}_p)$ to $G_{K'}$ is semistable, and there is an isomorphism $D_{\text{st},K'}(H^2(\tilde{X}_{s_0} \otimes \bar{F}, \mathbb{Q}_p)) \cong D$ compatible with φ, with N up to a nonzero rational factor depending on the normalizations, with the actions of H, and with the action of the inertia subgroup $I(K'/F)$, in which each $\gamma \in I(K'/F)$ acts on D through the automorphism of the log scheme Y induced by $\gamma_{\mathcal{X}}$ (Lemma 5.8 (d)), lying over the Teichmüller lift to $W(k')$ of the automorphism that γ induces on the log point* $\operatorname{Spec} k'$ *(with the log structure induced by $\mathcal{O}_{K'}$).*

(b) *There is a finite increasing filtration $P_\bullet$ of D, stable under H and under $\gamma_{\mathcal{X}}$ for γ in the inertia subgroup $I(K'/F)$, such that $N(P_r) \subset P_{r-2}$ and $\operatorname{gr}^P_r D$ is, compatibly with these actions, a subquotient of*

$$E_1^{-r,2+r} = \bigoplus_{j \ge \max(0,-r)} H^{2-r-2j}_{\text{crys}}\big(Y^{(2j+r+1)}/W(k')\big)(-j-r) \otimes \mathbb{Q},$$

where $Y^{(q)}$ is the disjoint union of the q-fold intersections of components of Y, and H and $\gamma_{\mathcal{X}}$, $\gamma \in I(K'/F)$, act on $E_1^{-r,2+r}$ by pull-back along their restrictions to the strata $Y^{(q)}$.

Proof. (a) Let $\tilde{X}_{\bar{F}} = \tilde{X}_{s_0} \otimes_F \bar{F}$, on which G_F acts through the second factor, and let F^{nr} be the maximal unramified extension of F in $\bar{F}$ (Beilinson's K_0^{nr}; his K_0 is our F). We use, with base field F, the semistable comparison isomorphism constructed by Beilinson [11] (the comparison theorem is due to Tsuji [112]), which involves no choice of a uniformizer: the base log structures are the canonical ones, generated by all nonzero elements of $\mathcal{O}_{K'}$ and of $W(k')$ [11, 1.16]. Beilinson attaches to $\tilde{X}_{\bar{F}}$ its Hyodo–Kato cohomology $H^2_{\text{HK}}(\tilde{X}_{\bar{F}})$, an F^{nr}-vector space with φ and N on which G_F acts by transport of structure [11, 2.4, 2.5], and constructs a canonical isomorphism

$$\rho_{\text{HK}} \colon H^2_{\text{HK}}(\tilde{X}_{\bar{F}}) \otimes_{F^{\text{nr}}} B_{\text{st}} \xrightarrow{\sim} H^2(\tilde{X}_{\bar{F}}, \mathbb{Q}_p) \otimes_{\mathbb{Q}_p} B_{\text{st}},$$

compatible with φ, N and the action of G_F [11, (3.3.1)]; here B_{st} is Fontaine's ring, with its φ and N [11, 1.17, last paragraph].

The scheme $\mathcal{X}$, with the log structure defined by its special fiber, is log smooth over $\mathcal{O}_{K'}$, its special fiber is of Cartier type over the log point [113, §4.3], its reduction modulo p is of Cartier type by the same computation in the charts of Lemma 5.8, and its log structure is trivial on the generic fiber. So [11, Proposition in 2.6] gives a canonical isomorphism

$$\iota\colon H^2_{\mathrm{HK}}(Y)\otimes_{K'_0} F^{\mathrm{nr}} \xrightarrow{\sim} H^2_{\mathrm{HK}}(\tilde{X}_{\bar{F}}),$$

where $H^2_{\mathrm{HK}}(Y)$ is the Hyodo–Kato cohomology [11, (1.16.1)] of the special fiber with its log structure, and $G_{K'}$ acts on the source through the second factor [11, 3.3 (ii)]. By [11, Remark (i) in 1.16 and Remark (iv) in 1.15], $H^2_{\mathrm{HK}}(Y)$ is the log-crystalline cohomology of Y over $W(k')$ with the log structure obtained from that of the log point $\operatorname{Spec} k'$ through Teichmüller representatives; choosing the class of a uniformizer as a generator identifies it with D, with its φ, and with its N up to the factor $e(K'/\mathbb{Q}_p)$ by which the two normalizations differ [11, Remark (ii) in 1.16 and Theorem-construction (ii) in 1.15]. We use only the vanishing of N and the property $N(P_r)\subset P_{r-2}$ of (b), which do not depend on this factor. Taking $G_{K'}$-invariants of $\rho_{\mathrm{HK}}\circ(\iota\otimes 1)$ and using $B_{\mathrm{st}}^{G_{K'}}=K'_0$ gives $D_{\mathrm{st},K'}(H^2)\cong D$, compatible with φ, and with N up to a nonzero rational factor; as $\dim_{K'_0} D=\dim_{\mathbb{Q}_p} H^2$ [11, Proposition in 2.5 (ii)], H^2 is semistable over K'.

The Hyodo–Kato complex of the model is functorial for automorphisms of the log scheme $\mathcal{X}$ lying over automorphisms of $\operatorname{Spec}\mathcal{O}_{K'}$ with its canonical log structure, by the compatibility with base change of the functor from (φ,N)-modules to F-crystals through which that complex is defined [11, Theorem-construction (ii) in 1.15, and (1.16.1)]; [11, 3.3 (ii)] is the case $\gamma=1$ of the naturality used below. All these constructions are canonical, so they are compatible with every automorphism of their input (transport of structure, which is also how the action of G_F is defined [11, 2.4]): with H, which acts on $\mathcal{X}$ over $\mathcal{O}_{K'}$ and on $\tilde{X}_{\bar{F}}$; and, for $g\in G_F$ with image $\gamma\in I(K'/F)$, with the automorphism $\gamma_{\mathcal{X}}\otimes g$ of $\mathcal{X}\otimes_{\mathcal{O}_{K'}}\mathcal{O}_{\bar{F}}$, which is g on $\tilde{X}_{\bar{F}}$ and lies over the automorphism γ of $\operatorname{Spec}\mathcal{O}_{K'}$ with its canonical log structure. Since γ fixes K'_0, the element g acts on $H^2_{\mathrm{HK}}(Y)$ through the automorphism of the log scheme Y induced by $\gamma_{\mathcal{X}}$, which lies over the automorphism of the log point induced by γ (and its Teichmüller lift to $W(k')$); under the identification with D this is the action of $\gamma_{\mathcal{X}}$ used in (b).

(b) This is the p-adic weight spectral sequence of Mokrane [87, 3.23], in the corrected form of Nakkajima [90, (9.9.4), (9.10.2) and Definition 9.11 (2)]. It is the spectral sequence of the p-adic Steenbrink complex WA_Y, the total complex of $WA_Y^{ij}=W\Lambda_Y^{i+j+1}/P_jW\Lambda_Y^{i+j+1}$ [87, 3.8], [90, proof of Theorem 4.1], filtered by the weight filtration P [90, (4.1.4)], whose graded pieces are identified with the de Rham–Witt complexes of the strata by Poincaré residues [90, (9.9.3)]. Its E_1-terms are as displayed and its abutment is D, so $\mathrm{gr}^P_r D=E_\infty^{-r,2+r}$ is a subquotient of $E_1^{-r,2+r}$. Under this identification, the monodromy operator N of Hyodo and Kato is induced by the operator ν [90, Proposition 11.10 and Corollary 11.5 (2)], which is defined by the projections $WA_Y^{ij}\to WA_Y^{i-1,j+1}$ [90, Definition 11.6 (2)]; by the definition of the filtration [90, (4.1.4)] it maps P_r into P_{r-2}.

Every step of the construction is functorial for the automorphisms used here. The complex $W\Lambda_Y$ above is the complex $W\widetilde{\Lambda}_Y$ of [90, proof of Theorem 4.1], which is presented, level by level, in terms of $W_n(\mathcal{O}_Y)$ and of M_Y^{gp} modulo the units coming from k', where M_Y is the log structure of Y [90, (11.0.2) and Theorem 11.1 (1)]; so every automorphism g of the log scheme Y lying over an automorphism of the log point acts on it and preserves its filtration

P [87, 3.5], which counts logarithmic factors. The section θ is the $d\log$ of the image in M_Y of a generator of the log structure of the log point, and it does not depend on the choice of the generator [90, the paragraph before Theorem 11.1, and Theorem 11.1 (1)]; so $g^*\theta=\theta$, and g acts on the filtered complex (WA_Y,P) [90, (2.2.1; $\star$), (4.1.3), (4.1.4)], on the spectral sequence and on ν. On the abutment this is the action of g on the log-crystalline cohomology of Y over the canonical lift of the log point [90, beginning of §7, (7.12.3) and Proposition 7.13], whose log structure comes from the Teichmüller section, that is, the action on D of (a): the quasi-isomorphism $\theta\wedge$ [90, (4.1.2)] commutes with g, and so does the comparison isomorphism [90, Theorem 7.19], by transport of structure: it does not depend on the embedding system used to construct it (loc. cit., proof), g carries an embedding system to another one, and the maps into the log-crystalline cohomology sheaves of Y from which it is built are compatible with g [90, Lemma 9.1 (1)]. If g maps every component of Y to itself, it acts on the E_1-terms by pull-back along its restrictions to the strata, since multiplying a local equation of a component by a unit changes a logarithmic form only by a form of lower weight, which does not affect the Poincaré residue. The elements of H (over the identity of the log point) and the automorphisms $\gamma_{\mathcal{X}}$, $\gamma\in I(K'/F)$ (over the automorphism of the log point that multiplies its generator by the unit $\gamma(\pi)/\pi$) are of this kind, by Lemma 5.8 (c), (d); this is the compatibility used in [97, §8, after (8.6)]. □

Proof of Proposition 5.6. In both cases the Hodge–Tate weights are $\{0,1,2\}$, by Lemma 3.5 and the de Rham comparison theorem [113, Theorem A1]. The comparison theorem is functorial [113, (A1.1)], hence compatible with the action of H, and Lemma 3.5 holds with χ^m replaced by any of the six characters $\chi^{m'}$, $m'\in(\mathbb{Z}/9)^\times$, so the choice of embeddings of E does not matter. By Lemma 5.7 for the unramified extension F/K_v, it suffices to show that $V=\mathbb{V}_{s_0}$ is crystalline as a representation of G_F. By Proposition 3.4, $V=(H^2(\tilde{X}_{s_0}\otimes\bar{F},\mathbb{Q}_p)\otimes_{\mathbb{Q}_p}E)^{\chi^m}$, where $E\subset\overline{\mathbb{Q}}_p$ is a finite extension of $\mathbb{Q}_p$ containing $\iota_p(\zeta_9)$.

The case $s_0\not\equiv 0,1 \pmod p$. The pull-back of $\tilde{f}$ along $s_0\in\mathcal{S}(\mathcal{O}_{K_v})$ is a smooth projective model of $\tilde{X}_{s_0}$ over $\mathcal{O}_{K_v}$, so $H^2(\tilde{X}_{s_0}\otimes\bar{F},\mathbb{Q}_p)$ is crystalline [113, Theorem 1.1 and the remarks before it] (in the good reduction case the monodromy operator vanishes), and so is its direct summand V, cut out by the idempotent attached to χ^m, which commutes with G_{K_v}.

The case $s_0-1=t_1^3$ with $v_p(t_1)>0$. Let $\mathcal{X}$, Y, D and $P_\bullet$ be as in Lemmas 5.8 and 5.9, and $D_E=D\otimes_{\mathbb{Q}_p}E$. Taking χ^m-parts is exact and commutes with taking $G_{K'}$-invariants, so by Lemma 5.9 (a) the restriction of V to $G_{K'}$ is semistable and $D_{\mathrm{st},K'}(V)\cong D_E^{\chi^m}$, compatibly with N up to a nonzero factor and with the inertia subgroup $I(K'/F)$. By Lemma 5.7 it remains to show that N and the inertia subgroup $I(K'/F)$ act trivially on $D_E^{\chi^m}$.

The χ^m-part has a single weight. Since Y has no triple points, the term $E_1^{-r,2+r}$ of Lemma 5.9 (b) vanishes for $|r|\ge 2$, and for $r=1$ and $r=-1$ it is $H^1_{\mathrm{crys}}(Y^{(2)}/W(k'))(-1)\otimes\mathbb{Q}$ and $H^1_{\mathrm{crys}}(Y^{(2)}/W(k'))\otimes\mathbb{Q}$. The diagonal μ_9 fixes every point of $Y^{(2)}$ (Lemma 5.8 (c)), so it acts trivially on these terms, while χ^m is nontrivial on it (Lemma 3.1). Hence $(\mathrm{gr}_r^P D_E)^{\chi^m}=0$ for $r\ne 0$, that is, $(P_{-1}D_E)^{\chi^m}=0$ and $(P_0D_E)^{\chi^m}=D_E^{\chi^m}$.

$N=0$. $N(D_E^{\chi^m})=N((P_0D_E)^{\chi^m})\subset(P_{-2}D_E)^{\chi^m}=0$.

The inertial type is trivial. By the previous step $D_E^{\chi^m}=(\mathrm{gr}_0^P D_E)^{\chi^m}$, which by Lemma 5.9 (b) is, compatibly with $I(K'/F)$, a subquotient of the χ^m-part of $E_1^{0,2}\otimes E=\bigoplus_a H^2_{\mathrm{crys}}(Y_a/W(k'))\otimes_{\mathbb{Q}_p}E$, the sum over the components Y_a of Y (the other summand, from $Y^{(3)}$, is zero). Let $\gamma\in I(K'/F)$. By Lemma 5.8 (d) the restriction of $\gamma_{\mathcal{X}}$ to Y_a equals that of an element δ_a of the diagonal μ_3, so γ acts on $(H^2_{\mathrm{crys}}(Y_a/W(k'))\otimes E)^{\chi^m}$ as δ_a^* does,

that is, by $\chi^m(\delta_a) = 1$ (Lemma 3.1). So γ acts trivially on the χ^m-part of $E_1^{0,2} \otimes E$, hence on its subquotient $D_E^{\chi^m}$. Thus V is crystalline over F, and therefore over K_v. □

Remark 5.10. When $p \mid a$ the choice $(u, w) = (b, a)$ puts the variable divisible by p at the point $s = 1$, where Proposition 5.6 applies. With $(u, w) = (a, b)$ the parameter would be close to ∞ at p. The two choices of (u, w) give the same local data at $\mathfrak{p}$: since $3 \mid c$, $a \equiv -b \pmod 9$, and -1 and $1 + 9\mathbb{Z}_3$ are cubes in $\mathbb{Q}_3$, so $\kappa_a = \kappa_b$ on $G_{K_\mathfrak{p}}$. Apart from the requirement $p \nmid u$, nothing below depends on which of a, b is called u, and the parity of u plays no role.

6. Irreducibility

Suppose that the residual Frey representation had a one-dimensional constituent. Such a constituent would be the reduction of one of five algebraic Hecke characters of conductor dividing $\mathfrak{p}^2$, and the Frobenius data at the primes above 7 exclude all five (Theorem 6.2).

6.1. Cubic characters at $\mathfrak{p}$.

Lemma 6.1. *Let $u \in \mathbb{Z}$ with $3 \nmid u$, and let $\mathrm{Art}_\mathfrak{p} \colon K_\mathfrak{p}^\times \to G_{K_\mathfrak{p}}^{\mathrm{ab}}$ be the local Artin map.*

(a) *$\kappa_u \circ \mathrm{Art}_\mathfrak{p}$ is trivial on $\mathbb{Q}_3^\times$.*
(b) *If $u \equiv \pm 1 \pmod 9$, then κ_u is trivial on $G_{K_\mathfrak{p}}$.*
(c) *If $u \not\equiv \pm 1 \pmod 9$, then $\kappa_u|_{G_{K_\mathfrak{p}}}$ has conductor $\mathfrak{p}^2$ and $\kappa_u(\mathrm{Art}_\mathfrak{p}(\omega)) \neq 1$.*

In all cases $\kappa_u \circ \mathrm{Art}_\mathfrak{p}$ is trivial on $1 + \mathfrak{p}^2$.

Proof. (a) $\kappa_u(\mathrm{Art}_\mathfrak{p}(x))$ is the cubic Hilbert symbol $(u, x)_\mathfrak{p}$ (up to inversion, depending on normalizations). Let $u, x \in \mathbb{Q}_3^\times$, and let g be the nontrivial automorphism of $K_\mathfrak{p}/\mathbb{Q}_3$. By Galois equivariance $g((u, x)_\mathfrak{p}) = (gu, gx)_\mathfrak{p} = (u, x)_\mathfrak{p}$, and g inverts μ_3; so the symbol is 1.

(b), (c) The group $\mathbb{Z}_3^\times/(\mathbb{Z}_3^\times)^3$ has order 3: -1 is a cube and $1 + 9\mathbb{Z}_3 = (1 + 3\mathbb{Z}_3)^3$, while 2 is not a cube in $\mathbb{Q}_3$. So u is a cube in $\mathbb{Q}_3$ if and only if $u \equiv \pm 1 \pmod 9$, and otherwise $\kappa_u = \kappa_2^{\pm 1}$ on $G_{K_\mathfrak{p}}$ (a cube in $K_\mathfrak{p}$ that lies in $\mathbb{Q}_3$ is a cube in $\mathbb{Q}_3$, as $[K_\mathfrak{p} : \mathbb{Q}_3] = 2$). It remains to treat $u = 2$. The discriminant of $\mathbb{Q}(\sqrt[3]{2})$ is -108, so $\mathbb{Q}_3(\sqrt[3]{2})/\mathbb{Q}_3$ is totally ramified of degree 3 with discriminant exponent 3; the quadratic extension $K_\mathfrak{p}(\sqrt[3]{2})/\mathbb{Q}_3(\sqrt[3]{2})$ is tamely ramified, so $K_\mathfrak{p}(\sqrt[3]{2})/\mathbb{Q}_3$ has discriminant exponent $2 \cdot 3 + 1 = 7$. Computed through the tower $K_\mathfrak{p}(\sqrt[3]{2}) \supset K_\mathfrak{p} \supset \mathbb{Q}_3$, the same exponent is $3 \cdot 1 + 2f$, where f is the conductor exponent of κ_2 at $\mathfrak{p}$ (both nontrivial characters of $\mathrm{Gal}(K_\mathfrak{p}(\sqrt[3]{2})/K_\mathfrak{p})$ have conductor $\mathfrak{p}^f$). So $f = 2$. A character of conductor $\mathfrak{p}^2$ factors through $(\mathcal{O}/\mathfrak{p}^2)^\times \cong \mu_6$ nontrivially, and, being cubic, is nontrivial on ω. The final assertion of the lemma follows from (b) and $f = 2$. □

6.2. The theorem.

Theorem 6.2. *Let $p \geq 17$ be a prime with $p \equiv 1 \pmod 3$, and let $\bar\rho$ be the residual Frey representation of a solution of $x^3 + y^3 = z^p$ in coprime nonzero integers (Definition 5.4). Then $\bar\rho$ is absolutely irreducible.*

Proof. Suppose not. Since $\dim \bar\rho = 3$, $\bar\rho$ has a one-dimensional constituent $\theta \colon G_K \to \overline{\mathbb{F}}_p^\times$.

Step 1: ramification. By Proposition 5.5 (b), θ is unramified outside $\{\mathfrak{p}, v, \bar v\}$. By Proposition 5.5 (d), $\theta|_{I_\mathfrak{p}} = \bar\kappa_u^{-n_\infty}|_{I_\mathfrak{p}}$, which by Lemma 6.1 has order dividing 3 and conductor dividing $\mathfrak{p}^2$. By Proposition 5.5 (f) and Fontaine–Laffaille theory [57] ($p \geq 5$, weights in $[0, 2]$), $\bar\rho|_{G_{K_v}}$ is the reduction of a crystalline representation with Hodge–Tate weights

$\{0,1,2\}$, and every one-dimensional subquotient restricts to inertia as $\bar\varepsilon_p^{-k}$ with $k\in\{0,1,2\}$. So $\theta|_{I_v}=\bar\varepsilon_p^{-k_v}|_{I_v}$ and $\theta|_{I_{\bar v}}=\bar\varepsilon_p^{-k_{\bar v}}|_{I_{\bar v}}$ with $k_v,k_{\bar v}\in\{0,1,2\}$.

Step 2: the type. By class field theory θ is a character of the idele group of K, trivial on $K^\times$ and on the connected component at infinity, and unramified outside $\mathfrak{p},v,\bar v$. Evaluate it at the global unit -1: through the local Artin maps its components at v and $\bar v$ contribute $(-1)^{k_v}$ and $(-1)^{k_{\bar v}}$, its component at $\mathfrak{p}$ contributes the value at -1 of the cubic character $\bar\kappa_u^{-n_\infty}$, which is 1, and the other components contribute 1; so $(-1)^{k_v+k_{\bar v}}=1$. So the *type* $(k_v,k_{\bar v})$ lies in $\mathcal{T}=\{(0,0),(1,1),(2,2),(0,2),(2,0)\}$.

Step 3: θ is the reduction of an algebraic Hecke character. For $x\in K^\times$ prime to $\mathfrak{p}$ let $\zeta_x\in\mu_6$ be the unit with $x\equiv\zeta_x \pmod{\mathfrak{p}^2}$. The algebraic Hecke characters

$$\psi_{(k,k)}((x))=(x\bar x)^k\ (k=0,1,2),\qquad \psi'((x))=(\zeta_x\bar x)^2,\qquad \psi''((x))=(\bar\zeta_x x)^2$$

are well defined on ideals prime to $\mathfrak{p}$ and have conductor dividing $\mathfrak{p}^2$. Their p-adic realizations (through ι_p, with values $\psi(\mathfrak{q})$ on $\mathrm{Frob}_\mathfrak{q}$) restrict to $I_v\times I_{\bar v}$ as $(\varepsilon_p^{-k},\varepsilon_p^{-k})$, and, for ψ' and ψ'', as $(\varepsilon_p^{-2},1)$ and $(1,\varepsilon_p^{-2})$ in some order. So there is $\psi\in\{\psi_{(0,0)},\psi_{(1,1)},\psi_{(2,2)},\psi',\psi''\}$ whose reduction $\bar\psi$ has the same restrictions to I_v and $I_{\bar v}$ as θ. Then $\theta\bar\psi^{-1}$ is unramified outside $\mathfrak{p}$ and its restriction to $I_\mathfrak{p}$ has conductor dividing $\mathfrak{p}^2$: it is a character of the ray class group $\mathrm{Cl}_{\mathfrak{p}^2}(K)$, which is trivial because $\mathcal{O}$ is principal and $\mu_6\to(\mathcal{O}/\mathfrak{p}^2)^\times$ is onto. Hence $\theta=\bar\psi$.

Step 4: the primes above 7. By Proposition 5.5 (e), $\theta(\mathrm{Frob}_\mathfrak{q})$ is a root of the reduction of $P_\mathfrak{q}(\xi_\mathfrak{q}^{-1}T)$ for $\mathfrak{q}\in\{\mathfrak{l},\bar{\mathfrak{l}}\}$, with $\xi_\mathfrak{q}=\kappa_u(\mathrm{Frob}_\mathfrak{q})^{-n_\infty}\in\mu_3$. Let $\mathfrak{P}$ be the prime of $\mathcal{O}$ above p defined by ι_p, so that $\mathfrak{P}$ is v or $\bar v$ (the coefficients of the characteristic polynomials lie in $\mathcal{O}$). Write $\varpi=2-\omega$, so $\mathfrak{l}=(\varpi)$ and $\bar{\mathfrak{l}}=(\bar\varpi)$. The value $\psi(\mathfrak{l})$ is $\varpi^k\bar\varpi^{k'}$ times an element of μ_3, and $\psi(\bar{\mathfrak{l}})$ is $\bar\varpi^k\varpi^{k'}$ times an element of μ_3, where $(k,k')\in\mathcal{T}$ is the infinity type of ψ (for ψ' and ψ'' the units $\zeta_\varpi^2,\bar\zeta_\varpi^2$ lie in μ_3). Absorbing these roots of unity and $\xi_\mathfrak{q}$ into $\zeta_1,\zeta_2\in\mu_3$, we find $(k,k')\in\mathcal{T}$ and $\zeta_1,\zeta_2\in\mu_3$ with

$$P_\mathfrak{l}(\zeta_1\varpi^k\bar\varpi^{k'})\in\mathfrak{P}\quad\text{and}\quad P_{\bar{\mathfrak{l}}}(\zeta_2\bar\varpi^k\varpi^{k'})\in\mathfrak{P}. \tag{6.1}$$

This test does not depend on the normalization of Section 2: with arithmetic Frobenius elements, the roots of $P_\mathfrak{q}$ and the values $\psi(\mathfrak{q})$ are both replaced by their inverses.

Step 5: computation. By Proposition 3.9 (a), $(P_\mathfrak{l},P_{\bar{\mathfrak{l}}})$ is (P^+,P^-) or (P^-,P^+). For both assignments, each $(k,k')\in\mathcal{T}$ and each $(\zeta_1,\zeta_2)\in\mu_3^2$, the two elements above are nonzero, and the ideal of $\mathcal{O}$ they generate has all its prime factors above 2, 3, 7 or 13 (Appendix A, item C2). Since $\mathfrak{P}$ lies above $p\ge19$, this is a contradiction. □

Remark 6.3. Requiring the *same* prime $\mathfrak{P}$ at $\mathfrak{l}$ and $\bar{\mathfrak{l}}$ matters: without that requirement, the rational primes dividing the norms of both elements include 67, 103 and 523 for the types $(0,0)$ and $(2,2)$, and these primes divide the two norms through different primes of K. The computation of Step 5 also allows the values of κ_u at $\mathfrak{l}$ and $\bar{\mathfrak{l}}$ to vary independently in μ_3, although they are complex conjugate. So it covers every solution, both sheaves $\mathbb{V}_{\chi^{\pm1}}$ and both choices of u.

Part II: a compatible system and its members above 5

7. A compatible system of minimal ramification

Throughout Part II, $p\ge17$ is a prime with $p\equiv1 \pmod 3$, (a,b,c) is a solution of $x^3+y^3=z^p$ in coprime nonzero integers, u, w, s_0 are as in Section 5, and ρ, $\bar\rho$ are the Frey representation and its reduction (Definition 5.4). We replace ρ, which is ramified at the

primes of c, by a lift of $\bar\rho$ that is unramified outside $3p$ and belongs to a compatible system [27]. In Part II, representations over finite fields and over ℓ-adic fields are considered over an algebraic closure where convenient, and *irreducible* means absolutely irreducible.

7.1. **Properties of the Frey representation.** Put

$$\kappa := \kappa_u^{-n_\infty},$$

a character of G_K with values in $\mu_3 \subset \mathcal{O}^\times$. We shall use the following six properties of ρ.

(F1) $\bar\rho$ is unramified outside $\{\mathfrak{p}, v, \bar v\}$ (Proposition 5.5 (b)).

(F2) $\rho|_{G_{K_v}}$ and $\rho|_{G_{K_{\bar v}}}$ are crystalline with Hodge–Tate weights $\{0,1,2\}$ (Proposition 5.5 (f)).

(F3) $\rho|_{I_\mathfrak{p}}$ is $\kappa|_{I_\mathfrak{p}}$ times a unipotent representation (Proposition 5.5 (d)). Moreover $\kappa^{\mathsf{c}} = \kappa^{-1}$ (Section 2), and $\kappa|_{G_{K_\mathfrak{p}}}$ is trivial if $u \equiv \pm 1 \pmod 9$ and has conductor $\mathfrak{p}^2$ otherwise (Lemma 6.1).

(F4) $\rho^{\mathsf{c}} \cong \rho^\vee \otimes \varepsilon_p^{-2}$ (Proposition 5.5 (c)).

(F5) ρ is unramified at $\mathfrak{l}$ and $\bar{\mathfrak{l}}$, and for $\mathfrak{q} \in \{\mathfrak{l}, \bar{\mathfrak{l}}\}$ the eigenvalues of $\rho(\mathrm{Frob}_\mathfrak{q})$ are the products of $\xi_\mathfrak{q} = \kappa(\mathrm{Frob}_\mathfrak{q}) \in \mu_3$ with the roots of $P_\mathfrak{q}$, where $(P_\mathfrak{l}, P_{\bar{\mathfrak{l}}})$ is (P^+, P^-) or (P^-, P^+) (Proposition 5.5 (e), Proposition 3.9).

(F6) $\bar\rho$ is absolutely irreducible (Theorem 6.2).

We say that we are in the *unramified case* if κ is unramified at $\mathfrak{p}$ (that is, $u \equiv \pm 1 \pmod 9$), and in the *ramified case* otherwise. By Remark 5.10 this is independent of the choice of u.

The image of ρ is compact, so ρ is defined over a finite extension of $\mathbb{Q}_p$ and stabilizes a lattice. By (F6) the lattice is unique up to homothety and its reduction is $\bar\rho$. We therefore regard ρ as a homomorphism $G_K \to \mathrm{GL}_3(\overline{\mathbb{Z}}_p)$, where $\overline{\mathbb{Z}}_p$ is the ring of integers of $\overline{\mathbb{Q}}_p$, with reduction $\bar\rho\colon G_K \to \mathrm{GL}_3(\overline{\mathbb{F}}_p)$. Since $\rho|_{I_\mathfrak{p}} \otimes \kappa^{-1}$ is unipotent, every constituent of $(\bar\rho \otimes \bar\kappa^{-1})|_{I_\mathfrak{p}}$ is trivial, and therefore

$$\bar\rho|_{I_\mathfrak{p}} \text{ is } \bar\kappa|_{I_\mathfrak{p}} \text{ times a unipotent representation.} \tag{7.1}$$

7.2. **Polarizations.** Let $\delta_{K/\mathbb{Q}}\colon G_\mathbb{Q} \to \{\pm 1\}$ be the quadratic character of $K/\mathbb{Q}$. Let ℓ be a prime and let A be $\overline{\mathbb{Q}}_\ell$, $\overline{\mathbb{F}}_\ell$, or the ring of integers of a finite extension of $\mathbb{Q}_\ell$. A continuous action of G_K on A^3 is called *polarized* (with multiplier $\varepsilon_\ell^{-2}\delta_{K/\mathbb{Q}}$) if there is a perfect symmetric A-bilinear pairing Ψ on A^3 such that

$$\Psi(\sigma x, (\tilde{\mathsf{c}}\sigma\tilde{\mathsf{c}})y) = \varepsilon_\ell(\sigma)^{-2}\,\Psi(x,y) \qquad (\sigma \in G_K,\ x, y \in A^3). \tag{7.2}$$

This is the notion of a polarized and odd pair of [27, §1.5.1] and [10, §2.1], for the field K, the representation of G_K on A^3 and the character $\varepsilon_\ell^{-2}\delta_{K/\mathbb{Q}}$ of $G_\mathbb{Q}$: taking $\tilde{\mathsf{c}}$ as the element of $G_\mathbb{Q} \smallsetminus G_K$ fixed in [27, §1.5.1] (denoted γ_0 there), the two conditions there are (7.2) and $\Psi(y,x) = -(\varepsilon_\ell^{-2}\delta_{K/\mathbb{Q}})(\tilde{\mathsf{c}})\Psi(x,y) = \Psi(x,y)$, and oddness is $(\varepsilon_\ell^{-2}\delta_{K/\mathbb{Q}})(\tilde{\mathsf{c}}) = -1$.

Let $\mathcal{G}_3$ be the group scheme of Clozel, Harris and Taylor [31, §2.1]: the semidirect product of $\mathcal{G}_3^0 = \mathrm{GL}_3 \times \mathrm{GL}_1$ by a group $\{1, \jmath\}$ of order two, with $\jmath(g,t)\jmath^{-1} = (t \cdot {}^t g^{-1}, t)$, and let $\mathrm{mult}\colon \mathcal{G}_3 \to \mathrm{GL}_1$ be the character with $\mathrm{mult}(g,t) = t$ and $\mathrm{mult}(\jmath) = -1$. By [31, Lemma 2.1.1], a polarized action of G_K on A^3 together with a pairing Ψ is the same as a continuous homomorphism $G_\mathbb{Q} \to \mathcal{G}_3(A)$ that maps G_K to $\mathcal{G}_3^0(A)$ by $\sigma \mapsto (\sigma|_{A^3}, \varepsilon_\ell(\sigma)^{-2})$, induces an isomorphism of $G_\mathbb{Q}/G_K$ with $\mathcal{G}_3/\mathcal{G}_3^0$, and has *multiplier* $\varepsilon_\ell^{-2}\delta_{K/\mathbb{Q}}$, where the multiplier of a homomorphism to $\mathcal{G}_3$ is its composite with mult. It is called a *prolongation*. Changing Ψ by a scalar conjugates it by an element of $\{1\} \times \mathrm{GL}_1(A)$ [27, §1.5.1].

Lemma 7.1. *There is a perfect symmetric $\overline{\mathbb{Z}}_p$-bilinear pairing Ψ_ρ on $\overline{\mathbb{Z}}_p^3$ satisfying (7.2) for ρ (with $\ell = p$); it is unique up to a unit. In particular ρ and $\bar\rho$ are polarized, and the prolongation of ρ defined by Ψ_ρ lifts the prolongation of $\bar\rho$ defined by the reduction of Ψ_ρ.*

Proof. By (F4) there is a nondegenerate $\overline{\mathbb{Q}}_p$-bilinear pairing Ψ_ρ with (7.2): an isomorphism $\rho^{\mathsf{c}} \to \rho^\vee \otimes \varepsilon_p^{-2}$ sends y to the linear form $\Psi_\rho(\,\cdot\,, y)$. This isomorphism maps the lattice $\overline{\mathbb{Z}}_p^3$ onto a stable lattice of the dual, which by (F6) is a multiple of the dual lattice, and after scaling Ψ_ρ is perfect on $\overline{\mathbb{Z}}_p^3$. By Schur's lemma it is unique up to a scalar. The pairing $(x, y) \mapsto \Psi_\rho(y, x)$ also satisfies (7.2): replacing σ by $\tilde{\mathsf{c}}\sigma\tilde{\mathsf{c}}$ in (7.2) and using $\tilde{\mathsf{c}}^2 = 1$ and $\varepsilon_p(\tilde{\mathsf{c}}\sigma\tilde{\mathsf{c}}) = \varepsilon_p(\sigma)$ gives $\Psi_\rho((\tilde{\mathsf{c}}\sigma\tilde{\mathsf{c}})y, \sigma x) = \varepsilon_p(\sigma)^{-2}\Psi_\rho(y, x)$. So $\Psi_\rho(y, x) = \pm\Psi_\rho(x, y)$, and the sign is $+$ because a nondegenerate alternating form does not exist in odd dimension. (This is the argument of the proof of [27, Lemma 1.5.3].) □

7.3. **The residual representation is reasonable.** Calegari, Emerton and Gee call a representation $G_K \to \mathrm{GL}_3(\overline{\mathbb{F}}_p)$ *reasonable* if it is polarizable and odd, its restriction to $G_{K(\zeta_p)}$ is irreducible, $\zeta_p \notin K$, and $p > 2(3 + 1) = 8$ [27, Definition 2.1.6].

Proposition 7.2. *The representation $\bar\rho$ is reasonable.*

Proof. It is polarized by Lemma 7.1; $p \geq 17$; and $\zeta_p \notin K$. It remains to prove that $\bar\rho|_{G_{K(\zeta_p)}}$ is irreducible. The extension $K(\zeta_p)/K$ is cyclic of degree $p - 1$, since $K \cap \mathbb{Q}(\zeta_p) = \mathbb{Q}$. Suppose that $\bar\rho|_{G_{K(\zeta_p)}}$ is reducible. By Clifford's theorem it is a direct sum of irreducible representations that are conjugate under G_K; each occurs with multiplicity one, because the quotient $G_K/G_{K(\zeta_p)}$ is cyclic (a constituent extends to its stabilizer). As the dimension is 3, there are three distinct conjugate characters, and $\bar\rho$ is induced from a character of the subgroup of index 3 containing $G_{K(\zeta_p)}$, that is, of $G_{K'}$ with K' the cubic subfield of $K(\zeta_p)/K$. Hence $\bar\rho \cong \bar\rho \otimes \eta$ for a character η of order 3 of $\mathrm{Gal}(K'/K)$. The extension K'/K is totally ramified at v, so $\eta|_{I_v} = \bar\varepsilon_p^{\pm(p-1)/3}|_{I_v}$.

For $d \geq 1$ let $\bar\varepsilon_{p,d}\colon I_v \to \overline{\mathbb{F}}_p^\times$ be a fundamental character of level d; so $\bar\varepsilon_{p,1} = \bar\varepsilon_p|_{I_v}$, and $\bar\varepsilon_{p,d}^{(p^d-1)/(p-1)} = \bar\varepsilon_{p,1}$. By (F2) and Fontaine–Laffaille theory [57, Théorème 5.3] ($K_v = \mathbb{Q}_p$, weights $\{0, 1, 2\}$, $p > 3$), the semisimplification of $\bar\rho|_{I_v}$ is, up to replacing every character by its inverse, one of

(i) $1 \oplus \bar\varepsilon_{p,1} \oplus \bar\varepsilon_{p,1}^2$;

(ii) $\bar\varepsilon_{p,1}^{k_1} \oplus \bar\varepsilon_{p,2}^{k_2+pk_3} \oplus \bar\varepsilon_{p,2}^{k_3+pk_2}$ with $\{k_1, k_2, k_3\} = \{0, 1, 2\}$;

(iii) $\bar\varepsilon_{p,3}^{x} \oplus \bar\varepsilon_{p,3}^{px} \oplus \bar\varepsilon_{p,3}^{p^2x}$ with $x = k_1 + k_2p + k_3p^2$ and $\{k_1, k_2, k_3\} = \{0, 1, 2\}$.

This multiset of characters is stable under multiplication by $\eta|_{I_v}$, which has order 3.

In case (i), $\eta\cdot 1 \in \{1, \bar\varepsilon_{p,1}, \bar\varepsilon_{p,1}^2\}$ forces $(p-1)/3 \equiv 0, \pm1$ or $\pm2 \pmod{p-1}$, which is false for $p \geq 13$. In case (ii), $\bar\varepsilon_{p,2}^{k_2+pk_3}$ is not a power of $\bar\varepsilon_{p,1}$, because $k_2+pk_3 \equiv k_2-k_3 \not\equiv 0 \pmod{p+1}$; so $\bar\varepsilon_{p,1}^{k_1}$ is the only character of level 1 in the multiset, and $\eta\bar\varepsilon_{p,1}^{k_1} = \bar\varepsilon_{p,1}^{k_1}$, which is false. In case (iii), $\eta = \bar\varepsilon_{p,3}^{\pm(p^3-1)/3}$ on I_v permutes the three characters cyclically, so $(p - 1)x$ or $(p^2 - 1)x$ is congruent to $\pm(p^3 - 1)/3$ modulo $p^3 - 1$. Put $D = p^2 + p + 1$. The first congruence says $x \equiv \pm D/3 \pmod D$. The second says $(p + 1)x \equiv \pm D/3 \pmod D$; since $(p + 1)(-p) \equiv 1 \pmod D$ and $p \cdot D/3 \equiv D/3 \pmod D$ (as $3 \mid p - 1$), it also gives $x \equiv \pm D/3 \pmod D$. But $x \equiv (k_1 - k_3) + (k_2 - k_3)p \pmod D$, a nonzero integer of absolute value at most $2p + 2 < D/3$. This is a contradiction. □

7.4. **Compatible systems.** We recall the terminology of [27, §1.5.4] and [10, §5.1] for the field K and rank 3. A *compatible system* $\mathcal{R}$ of three-dimensional representations of G_K with coefficients in a number field M consists of a finite set of primes of K (the *bad* primes), a monic cubic polynomial $Q_{\mathfrak{q}}(X) \in M[X]$ for each prime $\mathfrak{q}$ of K that is not bad, a continuous semisimple representation

$$R_\lambda \colon G_K \to \mathrm{GL}_3(\overline{M}_\lambda)$$

for each prime λ of M, and a multiset H_τ of three integers for each embedding $\tau \colon K \to \overline{M}$, such that, if ℓ is the residue characteristic of λ: for every $\mathfrak{q} \nmid \ell$ that is not bad, R_λ is unramified at $\mathfrak{q}$ and $R_\lambda(\mathrm{Frob}_{\mathfrak{q}})$ has characteristic polynomial $Q_{\mathfrak{q}}$; for $\mathfrak{q} \mid \ell$, $R_\lambda|_{G_{K_{\mathfrak{q}}}}$ is de Rham, and crystalline if $\mathfrak{q}$ is not bad, and the Hodge–Tate weights of R_λ with respect to τ are H_τ. The system is *regular* if each H_τ consists of three distinct integers, and *polarized* (and odd, with multiplier $\varepsilon_\ell^{-2}\delta_{K/\mathbb{Q}}$) if every R_λ is polarized in the sense of Section 7.2. It is *weakly irreducible* if there is a set of rational primes ℓ of positive Dirichlet density such that R_λ is irreducible for all $\lambda \mid \ell$ [27, Definition 1.5.10]. We regard M as a subfield of $\overline{\mathbb{Q}}$, with $\overline{M} = \overline{\mathbb{Q}}$, in such a way that the *p-adic member* R_p of the system is the member at the prime of M induced by ι_p, viewed over $\overline{\mathbb{Q}}_p$ through ι_p.

Let $\bar{\rho}_{\mathcal{G}} \colon G_{\mathbb{Q}} \to \mathcal{G}_3(\overline{\mathbb{F}}_p)$ be the prolongation of $\bar{\rho}$ given by the reduction of Ψ_ρ. A *polarized component at* 3 is an irreducible component of the generic fiber of the universal ring of framed liftings of $\bar{\rho}_{\mathcal{G}}|_{G_{\mathbb{Q}_3}}$ to $\mathcal{G}_3$ with multiplier $\varepsilon_p^{-2}\delta_{K/\mathbb{Q}}$ and a fixed inertial type. The prime 3 is ramified in K, and this is the case for which [27, §1.5.19] works with $\mathcal{G}_3$-valued liftings. A *polarized component at p* is an irreducible component of the generic fiber of the universal ring of framed potentially semistable liftings of $\bar{\rho}|_{G_{K_v}}$ of a fixed inertial type and fixed Hodge–Tate weights. As p splits in K, this is the same as a component for the $\mathcal{G}_3$-valued liftings at p [27, Lemma 1.5.20]. A polarized component $\mathcal{C}$ at p with distinct Hodge–Tate weights is *globally realizable* [27, Definition 2.1.9] if there are a CM field F, a regular, polarized and odd, weakly irreducible compatible system of representations of G_F whose residual representation at p is reasonable, and a place of the maximal totally real subfield of F with completion $\mathbb{Q}_p$ at which the prolongation of the p-adic member of the system has residual representation isomorphic to $\bar{\rho}_{\mathcal{G}}|_{G_{\mathbb{Q}_p}}$ and defines a point of $\mathcal{C}$.

Theorem 7.3 (Calegari–Emerton–Gee)**.** *Let $\mathcal{C}_3$ be a polarized component at 3, and let $\mathcal{C}_p$ be a polarized component at p with Hodge–Tate weights $\{0,1,2\}$ which is globally realizable. Then there is a regular, polarized and odd, weakly irreducible compatible system $\mathcal{R} = \{R_\lambda\}$ of three-dimensional representations of G_K such that:*

1. *the p-adic member R_p is a lift of $\bar{\rho}$, and it is unramified outside $\{\mathfrak{p}, v, \bar{v}\}$;*
2. *the prolongation of R_p, restricted to $G_{\mathbb{Q}_3}$, defines a point of $\mathcal{C}_3$, and $R_p|_{G_{K_v}}$ defines a point of $\mathcal{C}_p$.*

Proof. This is [27, Theorem 4.2.11] (for components at places of the maximal totally real subfield that are ramified in the CM field, see [27, §1.5.19 and Convention 1.5.22]) for the CM field K, with maximal totally real subfield $\mathbb{Q}$, in dimension $n = 3$ (the theorem requires n odd or $n = 2$), for the residual representation $\bar{\rho}$ with the character $\bar{\varepsilon}_p^{-2}\bar{\delta}_{K/\mathbb{Q}}$, the set of places $\{3, p\}$ of $\mathbb{Q}$, and the lift $\varepsilon_p^{-2}\delta_{K/\mathbb{Q}}$ of that character. Its hypotheses hold: $\bar{\rho}$ is polarized and reasonable (Lemma 7.1, Proposition 7.2); the set $\{3, p\}$ contains p and the primes at which $\bar{\rho}$ or $\bar{\varepsilon}_p^{-2}\bar{\delta}_{K/\mathbb{Q}}$ is ramified, by (F1); the character $\varepsilon_p^{-2}\delta_{K/\mathbb{Q}}$ is de Rham and unramified outside $\{3, p\}$; a polarized component is given at each of the two places; and the component at the place p is globally realizable, by hypothesis (in all uses below this is Lemma 7.5, with the field of [27, Definition 2.1.9] equal to K).

The place 3. At a place not above p of the set S of [27, Theorem 4.2.11], here $\{3, p\}$, that theorem asks only for a polarized component in the sense of [27, §1.5.19], where such components are defined, following Bellovin and Gee, at every finite place of the maximal totally real subfield, including the places that are inert or ramified in the CM field; global realizability is asked only at the places above p. So $\mathcal{C}_3$ may be any polarized component at 3 (Section 7.4).

In the proof of [27, Theorem 4.2.11], a component at a place of S not above p is imposed on auxiliary compatible systems by [27, Lemmas 4.2.3 and 4.2.4], and kept through the component swapping and descent of [27, Lemmas 4.1.8, 4.2.1 and 4.2.9]. For such a component these steps use two results of Bellovin and Gee, which allow at a place prime to p any component of a $\mathcal{G}_3$-valued lifting ring of fixed inertial type, also when the place is inert or ramified in the CM field [13, §5.1]: global deformation rings with given components at all places of S have Krull dimension at least one [13, Corollary 5.1.1], which is [27, Proposition 1.5.24]; and, given a suitable potentially diagonalizably automorphic lift over a CM extension, there is a lift on the given components [13, Theorem 5.2.1], which gives the lift in [27, Lemma 4.2.3]. The latter result asks for potential diagonalizability, a notion defined for GL_n-valued liftings [10, §1.4], only at the places above p, which split in the CM field in [27, Lemma 4.2.3]; and the finiteness of the deformation rings rests on [27, Lemma 1.5.27], which passes to a base change in which every place of S splits [10, Lemma 1.2.3].

The theorem gives a regular, polarized and odd, weakly irreducible compatible system together with a compatible system of characters of $G_{\mathbb{Q}}$ whose p-adic member is $\varepsilon_p^{-2}\delta_{K/\mathbb{Q}}$. A compatible system of characters is determined by one member, so its member at $\lambda \mid \ell$ is $\varepsilon_\ell^{-2}\delta_{K/\mathbb{Q}}$, and every R_λ is polarized in the sense of Section 7.2. Conclusions (1) and (2) are those of [27, Theorem 4.2.11], read with [27, Convention 1.5.22 and Lemma 1.5.20]: the p-adic member lifts $\bar\rho$, is unramified outside the places above 3 and p, that is, outside $\{\mathfrak{p}, v, \bar v\}$, and lies on the given components.

A second proof. For the component $\mathcal{C}_p$ of Section 7.5, the only one used below, the theorem also holds without the component swapping of [27, §4.2]. As p splits in K and the points of $\mathcal{C}_p$ are potentially diagonalizable [10, Lemma 1.4.3 (2)], it follows from the lifting argument of Bellovin and Gee [13, Theorem 5.2.1], written out in Lemma 12.21 for $p \equiv 2 \pmod 3$, together with the proof of Lemma 7.4, as Remark 12.23 shows. □

7.5. **The two components.** *At p.* By (F2), $\rho|_{G_{K_v}}$ is a point of the generic fiber of the universal ring of framed crystalline liftings of $\bar\rho|_{G_{K_v}}$ with Hodge–Tate weights $\{0, 1, 2\}$. This generic fiber is regular, and it is a union of irreducible components of the generic fiber of the ring of semistable liftings with the same weights, namely those on which the monodromy operator vanishes identically [13, Theorem 3.3.7 and the paragraph before it] (see also [78]). Let $\mathcal{C}_p$ be its irreducible component through $\rho|_{G_{K_v}}$. It is a polarized component at p, with trivial inertial type, and every point of $\mathcal{C}_p$ is crystalline. To show that $\mathcal{C}_p$ is globally realizable (Lemma 7.5), we first put ρ itself in a compatible system.

Lemma 7.4. *The representation ρ is the p-adic member of a compatible system $\{\rho_\lambda\}$ of three-dimensional representations of G_K, with coefficient field $M_\rho \subset \overline{\mathbb{Q}}$, which is regular, weakly irreducible, and polarized and odd with the multipliers $\varepsilon_\ell^{-2}\delta_{K/\mathbb{Q}}$: every ρ_λ is polarized in the sense of Section 7.2.*

Proof. (1) *The system.* We apply [10, Theorem 5.5.1] to $(\rho, \varepsilon_p^{-2}\delta_{K/\mathbb{Q}})$. Its hypotheses hold. The field K is an imaginary CM field, $\zeta_p \notin K$, and $p \geq 17 \geq 2(3+1)$. The pair $(\rho, \varepsilon_p^{-2}\delta_{K/\mathbb{Q}})$ is a totally odd, regular algebraic, polarized p-adic representation in the sense of [10, §2.1]:

the pairing Ψ_ρ of Lemma 7.1 is symmetric and satisfies (7.2), and $(\varepsilon_p^{-2}\delta_{K/\mathbb{Q}})(\tilde{\mathsf{c}}) = -1$; ρ is unramified outside the primes dividing $3pc$, and de Rham with distinct Hodge–Tate weights at v and $\bar{v}$ by (F2). It is potentially diagonalizable at v and $\bar{v}$ by [10, Lemma 1.4.3 (2)], because $K_v = K_{\bar{v}} = \mathbb{Q}_p$, ρ is crystalline there and its weights lie in $[0, p-2]$. And $\bar{\rho}|_{G_{K(\zeta_p)}}$ is irreducible (Proposition 7.2). The theorem puts ρ in a compatible system $\{\rho_\lambda\}$ of representations of G_K, with coefficient field $M_\rho \subset \overline{\mathbb{Q}}$, which we embed so that ρ is the member at the prime of M_ρ induced by ι_p: each $\rho_\lambda \colon G_K \to \mathrm{GL}_3(\overline{M}_\lambda)$ is semisimple, and there are a finite set S of primes of K, which we take stable under c and containing the primes above $3p$, and polynomials $Q_\mathfrak{q} \in M_\rho[X]$ for $\mathfrak{q} \notin S$, such that ρ_λ is unramified at every $\mathfrak{q} \notin S$ prime to λ and $\rho_\lambda(\mathrm{Frob}_\mathfrak{q})$ has characteristic polynomial $Q_\mathfrak{q}$. Its Hodge–Tate weights are those of ρ, $\{0,1,2\}$ at both embeddings, so it is regular.

(2) *Duality.* For $\mathfrak{q} \notin S$ let $Q_\mathfrak{q}^*(X) \in M_\rho[X]$ be the monic polynomial whose roots are the $\mathrm{N}\,\mathfrak{q}^2/\alpha$, α running over the roots of $Q_\mathfrak{q}$. Since $\tilde{\mathsf{c}}\,\mathrm{Frob}_\mathfrak{q}\,\tilde{\mathsf{c}}$ is a Frobenius element at $\bar{\mathfrak{q}}$ and $\varepsilon_\ell(\mathrm{Frob}_\mathfrak{q}) = \mathrm{N}\,\mathfrak{q}^{-1}$, the characteristic polynomials of $\rho_\lambda^{\mathsf{c}}(\mathrm{Frob}_\mathfrak{q})$ and of $(\rho_\lambda^\vee \otimes \varepsilon_\ell^{-2})(\mathrm{Frob}_\mathfrak{q})$ are $Q_{\bar{\mathfrak{q}}}$ and $Q_{\bar{\mathfrak{q}}}^*$. For λ the prime of ρ they are equal, because $\rho^{\mathsf{c}} \cong \rho^\vee \otimes \varepsilon_p^{-2}$ (F4); so $Q_{\bar{\mathfrak{q}}} = Q_{\bar{\mathfrak{q}}}^*$ in $M_\rho[X]$, and by the Chebotarev density theorem and the Brauer–Nesbitt theorem $\rho_\lambda^{\mathsf{c}} \cong \rho_\lambda^\vee \otimes \varepsilon_\ell^{-2}$ for every λ, ℓ being the residue characteristic of λ.

(3) *Constituents.* Fix λ and write $\rho_\lambda = \bigoplus_{\alpha \in \mathcal{A}} V_\alpha$ with V_α irreducible. The V_α are pairwise non-isomorphic, since the Hodge–Tate weights of ρ_λ at each embedding are distinct. By (2) there is an involution $\alpha \mapsto \alpha^*$ of $\mathcal{A}$ with $V_\alpha^{\mathsf{c}} \cong V_{\alpha^*}^\vee \otimes \varepsilon_\ell^{-2}$.

(4) *An automorphic restriction.* By [10, Lemma 5.3.1 (1)] there is a finite Galois extension K^1/K such that, for every λ, $\sigma \mapsto \rho_\lambda(\sigma)$ induces an isomorphism of $\mathrm{Gal}(K^1/K)$ with G_λ/G_λ^0, where G_λ is the Zariski closure of $\rho_\lambda(G_K)$ and G_λ^0 its identity component. Apply [10, Theorem 4.5.1] with $F = F_0 = K$, the single representation $(\rho, \varepsilon_p^{-2}\delta_{K/\mathbb{Q}})$ (its hypotheses were checked in (1)), an isomorphism $\imath \colon \overline{\mathbb{Q}}_p \to \mathbb{C}$, and $F^{(\mathrm{avoid})} = K^1$: there are a finite CM extension F'/K, Galois and linearly disjoint from K^1 over K, and a regular algebraic, cuspidal, polarized automorphic representation (π, χ) of $\mathrm{GL}_3(\mathbb{A}_{F'})$ in the sense of [10, §2.1] with $(r_{p,\imath}(\pi), r_{p,\imath}(\chi)\varepsilon_p^{-2}) \cong (\rho|_{G_{F'}}, \varepsilon_p^{-2}\delta_{K/\mathbb{Q}}|_{G_{(F')^+}})$. For each λ fix an isomorphism $j_\lambda \colon \overline{M}_\lambda \to \mathbb{C}$ inducing $\imath \circ \iota_p$ on M_ρ. Both $\rho_\lambda|_{G_{F'}}$ (as F'/K is Galois) and $r_{\ell,j_\lambda}(\pi)$ are semisimple. At a prime w of F' at which π is unramified, above a prime $\mathfrak{q} \notin S$ of K prime to ℓp, both $\rho_\lambda(\mathrm{Frob}_w)$ and $r_{\ell,j_\lambda}(\pi)(\mathrm{Frob}_w)$ have as characteristic polynomial the image under j_λ^{-1} of that of $\mathrm{rec}(\pi_w \otimes |\det|^{-1})(\mathrm{Frob}_w)$: for $r_{\ell,j_\lambda}(\pi)$ by [10, Theorem 2.1.1 (2)], and for ρ_λ because its characteristic polynomial is given by the same polynomial over M_ρ as that of $\rho(\mathrm{Frob}_w) = r_{p,\imath}(\pi)(\mathrm{Frob}_w)$. So $\rho_\lambda|_{G_{F'}} \cong r_{\ell,j_\lambda}(\pi)$ by the Chebotarev density and Brauer–Nesbitt theorems. Likewise $r_{\ell,j_\lambda}(\chi) = \delta_{K/\mathbb{Q}}|_{G_{(F')^+}}$: this holds for $\ell = p$, so χ has finite order, and the $r_{\ell,j}(\chi)$ form a compatible system of characters.

The Zariski closure H_λ of $\rho_\lambda(G_{F'})$ has finite index in G_λ, so it contains G_λ^0; and $G_{F'}$ maps onto $\mathrm{Gal}(K^1/K) = G_\lambda/G_\lambda^0$. So $H_\lambda = G_\lambda$. Hence each V_α is irreducible as a representation of $G_{F'}$, and $V_\alpha \not\cong V_\beta$ as representations of $G_{F'}$ for $\alpha \neq \beta$ (a map commuting with $\rho_\lambda(G_{F'})$ commutes with $H_\lambda = G_\lambda$). As F' is a CM field, $\tilde{\mathsf{c}}$ normalizes $G_{F'}$, so the same holds for the V_α^{c} and the $V_\beta^\vee \otimes \varepsilon_\ell^{-2}$.

(5) *The pairing.* For a closed subgroup $H \subset G_K$ normalized by $\tilde{\mathsf{c}}$, let $\mathcal{B}_H$ be the space of bilinear forms Ψ on the space of ρ_λ with $\Psi(\sigma x, (\tilde{\mathsf{c}}\sigma\tilde{\mathsf{c}})y) = \varepsilon_\ell(\sigma)^{-2}\Psi(x,y)$ for $\sigma \in H$; sending Ψ to $y \mapsto \Psi(\cdot, y)$ identifies $\mathcal{B}_H$ with $\mathrm{Hom}_H(\rho_\lambda^{\mathsf{c}}, \rho_\lambda^\vee \otimes \varepsilon_\ell^{-2})$. By (3), (4) and Schur's lemma, $\mathrm{Hom}_H(V_\alpha^{\mathsf{c}}, V_\beta^\vee \otimes \varepsilon_\ell^{-2})$ has dimension 1 if $\beta = \alpha^*$ and 0 otherwise, both for $H = G_K$ and for $H = G_{F'}$. So $\mathcal{B}_{G_K} \subset \mathcal{B}_{G_{F'}}$ have the same dimension $|\mathcal{A}|$, and they are equal. By [10,

Theorem 2.1.1 (1)] and the definitions of [10, §2.1], $(\rho_\lambda|_{G_{F'}}, \varepsilon_\ell^{-2}\delta_{K/\mathbb{Q}}|_{G_{(F')^+}})$ is a totally odd polarized representation: taking for the complex conjugation at an infinite place of $(F')^+$ the element $\tilde{\mathsf{c}}$, which lies in $G_{(F')^+}$, there is a nondegenerate symmetric $\Phi \in \mathcal{B}_{G_{F'}}$. As $\mathcal{B}_{G_{F'}} = \mathcal{B}_{G_K}$, Φ satisfies (7.2) for all $\sigma \in G_K$, and ρ_λ is polarized.

(6) *Weak irreducibility.* By [92, Theorem 1.7] there is a set L' of rational primes of positive Dirichlet density such that $r_{\ell,j}(\pi)$ is irreducible for every $\ell \in L'$ and every j. For λ above $\ell \in L'$, $\rho_\lambda|_{G_{F'}}$ is irreducible, hence so is ρ_λ. □

Lemma 7.5. *The component $\mathcal{C}_p$ is globally realizable.*

Proof. By Lemma 7.4, $(\{\rho_\lambda\}, \{\varepsilon_\ell^{-2}\delta_{K/\mathbb{Q}}\})$ is a regular, polarized and odd, weakly irreducible compatible system of representations of G_K. Its residual representation at p is $\bar\rho$, which is reasonable (Proposition 7.2); the prolongation of ρ defined by Ψ_ρ (Lemma 7.1) has multiplier $\varepsilon_p^{-2}\delta_{K/\mathbb{Q}}$, whose restriction to $G_{\mathbb{Q}_p}$ is the multiplier of $\mathcal{C}_p$; and the restriction of this prolongation to $G_{\mathbb{Q}_p}$, at the place p of $\mathbb{Q}$, lies on $\mathcal{C}_p$ by the definition of $\mathcal{C}_p$ ([27, Lemma 1.5.20], as p splits in K). These are the conditions of [27, Definition 2.1.9] with $F = K$. □

At 3. The prolongation of ρ defined by Ψ_ρ (Lemma 7.1), restricted to $G_{\mathbb{Q}_3}$, is a lifting of $\bar\rho_{\mathcal{G}}|_{G_{\mathbb{Q}_3}}$ with multiplier $\varepsilon_p^{-2}\delta_{K/\mathbb{Q}}$. Let $\mathcal{C}_3$ be any irreducible component through it of the generic fiber of the lifting ring of its inertial type.

Lemma 7.6. *Let $\rho'\colon G_{K_\mathfrak{p}} \to \mathrm{GL}_3(\overline{\mathbb{Z}}_p)$ be a continuous representation whose reduction, restricted to $I_\mathfrak{p}$, is $\bar\kappa|_{I_\mathfrak{p}}$ times a unipotent representation. Then there is a nilpotent matrix N such that $\rho'(\sigma) = \kappa(\sigma)\exp(t_p(\sigma)N)$ for all $\sigma \in I_\mathfrak{p}$. In other words, $\mathrm{WD}(\rho') = (\phi, N)$ with $\phi|_{I_\mathfrak{p}} = \kappa|_{I_\mathfrak{p}}$, a scalar. (The proof uses only that $p \notin \{2, 3, 13\}$.)*

Proof. Let $I_\mathfrak{p}^{\mathrm{w}} \subset I_\mathfrak{p}$ be the wild inertia subgroup, a pro-3 group. The kernel of reduction is a pro-p group and $p \neq 3$, so $\rho'(I_\mathfrak{p}^{\mathrm{w}})$ maps isomorphically onto its reduction $\bar\kappa(I_\mathfrak{p}^{\mathrm{w}})$, of order 1 or 3 (a unipotent representation over $\overline{\mathbb{F}}_p$ is trivial on a pro-3 group). An element of order dividing 3 of $\mathrm{GL}_3(\overline{\mathbb{Z}}_p)$ whose reduction is a scalar is a scalar, since its eigenvalues lie in μ_3, which injects into the residue field. So $\rho' \otimes \kappa^{-1}$ is trivial on $I_\mathfrak{p}^{\mathrm{w}}$. Let g be the image under $\rho' \otimes \kappa^{-1}$ of a topological generator of the tame inertia group. Its reduction is unipotent, so its eigenvalues are congruent to 1. The residue field of $K_\mathfrak{p}$ has three elements, so a Frobenius element conjugates the tame inertia group by $\sigma \mapsto \sigma^{3^{\pm 1}}$; hence g is conjugate to g^3, the multiset of eigenvalues of g is stable under $t \mapsto t^3$, and each eigenvalue satisfies $t^{3^j-1} = 1$ for some $j \in \{1, 2, 3\}$: its order divides 2, 8 or 26. A root of unity congruent to 1 has p-power order, and $p \nmid 2 \cdot 8 \cdot 26 = 2^5 \cdot 13$ (this is where $p \neq 2, 13$ is used). So g is unipotent, the closure of the group generated by g is $\{\exp(xN) : x \in \mathbb{Z}_p\}$ with $N = \log g$, and the tame inertia group acts through its quotient $\mathbb{Z}_p(1)$. □

7.6. **The system and its p-adic member.** From now on, $\mathcal{R} = \{R_\lambda\}$ denotes a compatible system given by Theorem 7.3 for the component $\mathcal{C}_p$ of Section 7.5 (Lemma 7.5) and some polarized component at 3. Unless said otherwise the component at 3 is $\mathcal{C}_3$. Let $M \subset \overline{\mathbb{Q}}$ be its field of coefficients. Its p-adic member R_p has the following properties.

(P1) R_p is a lift of $\bar\rho$ and is unramified outside $\{\mathfrak{p}, v, \bar v\}$.

(P2) R_p is crystalline at v and $\bar v$ with Hodge–Tate weights $\{0, 1, 2\}$. Hence $H_\tau = \{0, 1, 2\}$ for both embeddings τ of K.

(P3) $R_p|_{I_\mathfrak{p}} \cong \kappa \otimes \exp(t_p N)$ for a nilpotent matrix N.

Indeed (P1) is Theorem 7.3 (1). For (P2): $R_p|_{G_{K_v}}$ defines a point of $\mathcal{C}_p$, all of whose points are crystalline with weights $\{0,1,2\}$; and $R_p^{\mathsf{c}} \cong R_p^\vee \otimes \varepsilon_p^{-2}$, which turns the weights h at v into the weights $2-h$ at $\bar{v}$. For (P3): apply Lemma 7.6 to $R_p|_{G_{K_\mathfrak{p}}}$, using (7.1). (P3) holds for *every* lift of $\bar{\rho}|_{G_{K_\mathfrak{p}}}$; the choice of the component at 3 only decides whether N can be zero (Proposition 9.5).

7.7. **What the other members inherit.**

Lemma 7.7. *Let $\mathcal{R} = \{R_\lambda\}$ be a regular, polarized and odd, weakly irreducible compatible system of three-dimensional representations of G_K, with coefficient field M (for instance a system given by Theorem 7.3), and let $\mathfrak{q}$ be a prime of K. There are an embedding $\imath_\mathfrak{q}\colon M \to \mathbb{C}$ and a Weil–Deligne representation $W_\mathfrak{q}$ of $W_{K_\mathfrak{q}}$ over $\mathbb{C}$ such that*

$$j\ \mathrm{WD}\left(R_\lambda|_{G_{K_\mathfrak{q}}}\right)^{F\text{-ss}} \cong W_\mathfrak{q}$$

for every prime λ of M, including those above the residue characteristic of $\mathfrak{q}$, and every isomorphism $j\colon \overline{M}_\lambda \to \mathbb{C}$ that restricts to $\imath_\mathfrak{q}$ on M. (For λ above the residue characteristic of $\mathfrak{q}$, WD is Fontaine's Weil–Deligne representation of the de Rham representation $R_\lambda|_{G_{K_\mathfrak{q}}}$.) In particular:

(a) *if R_{λ_0} is unramified at $\mathfrak{q}$ for some prime λ_0 of M not above the residue characteristic of $\mathfrak{q}$, or crystalline at $\mathfrak{q}$ for some λ_0 above it, then R_λ is unramified at $\mathfrak{q}$ for every λ not above the residue characteristic of $\mathfrak{q}$, and crystalline at $\mathfrak{q}$ for every λ above it;*

(b) *the restrictions to $I_\mathfrak{q}$ of the Weil–Deligne representations of the $R_\lambda|_{G_{K_\mathfrak{q}}}$ correspond to one another under isomorphisms of their coefficient fields that are the identity on M, and their monodromy operators have the same Jordan type.*

Proof. Let r be the residue characteristic of $\mathfrak{q}$. By [27, Theorem 2.1.16], applied to $\mathcal{R}$, its compatible system of multipliers $\{\varepsilon_\ell^{-2}\delta_{K/\mathbb{Q}}\}$ and the set $\{r\}$ of places of $\mathbb{Q}$, there is a finite Galois extension F'/K of CM fields such that r splits completely in its maximal totally real subfield $(F')^+$ and the restriction of $\mathcal{R}$ to $G_{F'}$ is automorphic [27, §1.5.4]: there are a regular algebraic, cuspidal, polarized automorphic representation (Π', χ') of $\mathrm{GL}_3(\mathbb{A}_{F'})$ in the sense of [10, §2.1] and an embedding $\imath_\mathfrak{q}\colon M \to \mathbb{C}$ such that, at almost all primes w of F', Π'_w is unramified and $\mathrm{rec}(\Pi'_w \otimes |\det|^{-1})(\mathrm{Frob}_w)$ has as characteristic polynomial the image under $\imath_\mathfrak{q}$ of that of the $R_\lambda(\mathrm{Frob}_w)$ [10, §5.1]. Let λ be a prime of M, ℓ its residue characteristic, and $j\colon \overline{M}_\lambda \to \mathbb{C}$ an isomorphism restricting to $\imath_\mathfrak{q}$ on M. Both $R_\lambda|_{G_{F'}}$ (as F'/K is Galois) and the representation $r_{\ell,j}(\Pi')$ of [10, Theorem 2.1.1] are semisimple, with the same characteristic polynomials of Frobenius at almost all primes, by [10, Theorem 2.1.1 (2)]; so $R_\lambda|_{G_{F'}} \cong r_{\ell,j}(\Pi')$ by the Chebotarev density and Brauer–Nesbitt theorems. Let y be a place of F' above $\mathfrak{q}$, and y^+ the place of $(F')^+$ below y. As r splits completely in $(F')^+$, the completion of $(F')^+$ at y^+ is $\mathbb{Q}_r$; as $F' = (F')^+K$, the completion F'_y is generated over it by $K_\mathfrak{q}$, so $F'_y = K_\mathfrak{q}$, for every choice of y. Hence y^+ is split, inert or ramified in F' as $\mathfrak{q}$ is over r; for $\mathfrak{q} = \mathfrak{p}$ it is ramified. Put $W_\mathfrak{q} = \mathrm{rec}(\Pi'_y \otimes |\det|^{-1})$.

If $\ell \neq r$, then $j\,\mathrm{WD}(R_\lambda|_{G_{F'_y}})^{F\text{-ss}} \cong W_\mathfrak{q}$ by [10, Theorem 2.1.1 (2)], which is stated for a regular algebraic, cuspidal, polarized pair in the sense of [10, §2.1] over a CM field, and for every place of that field not above ℓ. If $\ell = r$, the same isomorphism, monodromy operators included, is the second assertion of [9, Theorem 1.1], applied to F', (Π', χ'), j and the place y.

That theorem concerns an imaginary CM field F, a RAECSDC (regular algebraic, essentially conjugate self-dual, cuspidal) pair (Π, χ) of $\mathrm{GL}_m(\mathbb{A}_F)$, an isomorphism $j\colon \overline{\mathbb{Q}}_\ell \to \mathbb{C}$,

and every place $x \mid \ell$ of F, with no condition on the behavior of x in F/F^+. For every weight it gives $j\,\mathrm{WD}(r_{\ell,j}(\Pi)|_{G_{F_x}})^{F\text{-ss}} \prec \mathrm{rec}(\Pi_x \otimes |\det|^{(1-m)/2})$: the two sides have isomorphic semisimplifications, but the Jordan type of the monodromy operator of the left side may be smaller, in the dominance order, than that of the right side. For Shin-regular weight it gives $j\,\mathrm{WD}(r_{\ell,j}(\Pi)|_{G_{F_x}})^{F\text{-ss}} \cong \mathrm{rec}(\Pi_x \otimes |\det|^{(1-m)/2})$, monodromy operators included. By the definition in [9, §1], every weight is Shin-regular when m is odd (when m is even, a condition on the weight is required), so for $m = 3$ the isomorphism holds. For every $m \geq 2$, every CM field and every place above ℓ, the isomorphism with no condition on the weight is [28, Theorem 1.1], stated for cohomological conjugate self-dual Π (one reduces to these by a twist, as in the proof of [9, Theorem 2.1]); that paper proves the case of even m and refers to [8, 9] for odd m [28, §1], so for $m = 3$ it is not an independent source. The monodromy operator is needed when (a) is applied at the primes above p (Propositions 7.8 and 10.4), where that of $W_{\mathfrak{q}}$ must vanish, and when (b) is applied at $\mathfrak{p}$ to the members above 3 (Proposition 10.5), where it must be regular.

A regular algebraic, cuspidal, polarized pair in the sense of [10, §2.1], such as (Π', χ'), is RAECSDC (the definition of a polarized pair asks in addition that $\chi_x(-1) = (-1)^m$ for $x \mid \infty$), and the two papers attach to it the same representation $r_{\ell,j}(\Pi')$, both being semisimple with the characteristic polynomials of Frobenius given by Π' at almost all places. The proof of [9, Theorem 1.1] treats a place that does not split over the maximal totally real subfield by passing to a solvable CM extension in which the place splits completely, so that its completion does not change, and in which the places above ℓ of the maximal totally real subfield split [9, proof of Theorem 3.1 and Corollary 3.2], [8, §7]. As $F'_y = K_{\mathfrak{q}}$, this gives the isomorphism when $\ell = r$, whether $\mathfrak{q}$ is split, inert or ramified in K; all three cases occur ($\mathfrak{q} \in \{v, \bar{v}\}$, $\mathfrak{q} = 5\mathcal{O}$, $\mathfrak{q} = \mathfrak{p}$).

For (a): a representation of $G_{K_{\mathfrak{q}}}$ over $\overline{M}_\lambda$, with $\ell \neq r$, is unramified if and only if its Weil–Deligne representation is unramified with zero monodromy, and a de Rham representation of $G_{K_{\mathfrak{q}}}$, with $\ell = r$, is crystalline if and only if its Weil–Deligne representation is unramified with zero monodromy [55]. For (b): Frobenius semisimplification changes neither the restriction to inertia nor the monodromy operator. □

Proposition 7.8. *Let λ be a prime of M of residue characteristic $\ell \notin \{3, p\}$.*

(M1) *R_λ is unramified outside $\mathfrak{p}$ and the primes of K above ℓ.*

(M2) *R_λ is crystalline at the primes of K above ℓ, with Hodge–Tate weights $\{0, 1, 2\}$ for each embedding of K.*

(M3) *$R_\lambda|_{I_{\mathfrak{p}}} \cong \kappa_\lambda \otimes \exp(t_\ell N_\lambda)$, where $\kappa_\lambda \colon I_{\mathfrak{p}} \to \mu_3 \subset \overline{M}_\lambda^\times$ is $\kappa|_{I_{\mathfrak{p}}}$ or its inverse (after an identification of the groups μ_3 of the two coefficient fields), and N_λ is a nilpotent matrix of the same rank as the matrix N of* (P3).

Moreover, for every prime $\mathfrak{q} \nmid 3p\ell$ of K, the characteristic polynomials of $R_\lambda(\mathrm{Frob}_{\mathfrak{q}})$ and of $R_p(\mathrm{Frob}_{\mathfrak{q}})$ are the images of the same polynomial $Q_{\mathfrak{q}} \in M[X]$.

Proof. Apply Lemma 7.7, comparing R_λ with R_p.

(M1) and the last assertion: at a prime $\mathfrak{q} \nmid 3p\ell$, R_p is unramified by (P1), so R_λ is unramified at $\mathfrak{q}$. For every isomorphism $j \colon \overline{M}_\lambda \to \mathbb{C}$ restricting to $\imath_{\mathfrak{q}}$ on M, j maps the characteristic polynomial of $R_\lambda(\mathrm{Frob}_{\mathfrak{q}})$ to that of $W_{\mathfrak{q}}(\mathrm{Frob}_{\mathfrak{q}})$. Composing j with the automorphisms of $\mathbb{C}$ that fix $\imath_{\mathfrak{q}}(M)$ shows that the coefficients of the latter lie in $\imath_{\mathfrak{q}}(M)$ (the fixed field in $\mathbb{C}$ of the automorphisms fixing a subfield k is k); so the characteristic polynomial of $R_\lambda(\mathrm{Frob}_{\mathfrak{q}})$ is the image of $Q_{\mathfrak{q}} = \imath_{\mathfrak{q}}^{-1}(\mathrm{char}\, W_{\mathfrak{q}}(\mathrm{Frob}_{\mathfrak{q}})) \in M[X]$, the same polynomial for every λ. So $\mathfrak{q}$

may be removed from the bad primes, which gives the last assertion; the same argument applies to R_p. At $\mathfrak{q} \in \{v, \bar{v}\}$, R_p is crystalline by (P2), so R_λ is unramified at $\mathfrak{q}$.

(M2): at $\mathfrak{q} \mid \ell$, R_p is unramified by (P1), so R_λ is crystalline at $\mathfrak{q}$, with the weights H_τ of (P2).

(M3): take $\mathfrak{q} = \mathfrak{p}$. By (P3), the Weil–Deligne representation of $R_p|_{G_{K_\mathfrak{p}}}$ restricted to $I_\mathfrak{p}$ is the scalar character κ, with values in μ_3, and its monodromy operator is conjugate to N; so by Lemma 7.7 (b) the same holds for R_λ, with κ replaced by its image κ_λ and N by a nilpotent matrix N_λ of the same Jordan type. For an ℓ-adic representation the restriction to inertia is recovered from the Weil–Deligne representation (ϕ, N_λ) as $\sigma \mapsto \phi(\sigma)\exp(t_\ell(\sigma)N_\lambda)$ (Section 2). □

7.8. **Irreducibility of the members.** Weak irreducibility says nothing about a given member. The test at the primes above 7 that gave the irreducibility of $\bar{\rho}$ does.

Proposition 7.9. *Let λ be a prime of M of residue characteristic $\ell \notin \{3, 7, p\}$. Then R_λ is irreducible.*

Proof. R_λ is semisimple. If it is reducible, it has a one-dimensional summand $\theta\colon G_K \to \overline{M}_\lambda^\times$. By Proposition 7.8, θ is unramified outside $\mathfrak{p}$ and the primes above ℓ; $\theta|_{I_\mathfrak{p}} = \kappa_\lambda$ (a unipotent element acts trivially on a stable line), which has order dividing 3 and is trivial on $1 + \mathfrak{p}^2$ by (F3); and θ is crystalline at the primes above ℓ, with Hodge–Tate weights $k, k' \in \{0, 1, 2\}$ at the two embeddings of K. A crystalline character of G_K is the λ-adic realization of an algebraic Hecke character [100, Chapter III, Appendix and §2.3, Theorem 2; Chapter II, §2], here of conductor dividing $\mathfrak{p}^2$ and of infinity type (k, k'): there are an embedding $\tau\colon K \to \overline{M}_\lambda$ and a character η_0 of $(\mathcal{O}/\mathfrak{p}^2)^\times$, of order dividing 3, with

$$\theta(\mathrm{Frob}_{(x)}) = \tau\big(\eta_0(x)\, x^k\, \bar{x}^{k'}\big) \qquad \text{for all } x \in \mathcal{O} \text{ prime to } 3\ell.$$

(Here $\mathrm{Frob}_{(x)}$ denotes the product of the $\mathrm{Frob}_\mathfrak{q}^{v_\mathfrak{q}(x)}$ over the primes $\mathfrak{q}$ dividing x, in the abelianized Galois group, and we regard η_0 as a character with values in $\mu_3 \subset K$.) The right side must be 1 for $x \in \mu_6$. As $\mu_6 \to (\mathcal{O}/\mathfrak{p}^2)^\times$ is an isomorphism, this gives $\eta_0(\zeta) = \zeta^{k'-k}$ for $\zeta \in \mu_6$; since $\eta_0(-1) = 1$, $k \equiv k' \pmod 2$, so (k, k') lies in the set $\mathcal{T}$ of the proof of Theorem 6.2, and $x \mapsto \eta_0(x)x^k\bar{x}^{k'}$ is one of the five Hecke characters $\psi_{(0,0)}, \psi_{(1,1)}, \psi_{(2,2)}, \psi', \psi''$ of that proof. Complex conjugation of the values permutes these five characters, and replacing τ by $\tau \circ \mathsf{c}$ in the display replaces the character by its complex conjugate. So we may take for τ the restriction to K of an embedding $\overline{M} \to \overline{M}_\lambda$ that is the identity on M, and there is ψ among the five such that, for every prime $\mathfrak{q} \nmid 3\ell$ of K, the element $\psi(\mathfrak{q}) \in K \subset \overline{\mathbb{Q}} = \overline{M}$ is a root of the polynomial $Q_\mathfrak{q}$ of $\mathcal{R}$.

Take $\mathfrak{q} \in \{\mathfrak{l}, \bar{\mathfrak{l}}\}$; this is allowed because $\ell \neq 7$. By Proposition 7.8, $\iota_p(\psi(\mathfrak{q}))$ is an eigenvalue of $R_p(\mathrm{Frob}_\mathfrak{q})$, so its reduction is an eigenvalue of $\bar{\rho}(\mathrm{Frob}_\mathfrak{q})$, because R_p lifts $\bar{\rho}$ (P1). By (F5), $P_\mathfrak{q}(\xi_\mathfrak{q}^{-1}\psi(\mathfrak{q}))$ lies in the prime $\mathfrak{P}$ of $\mathcal{O}$ induced by ι_p, for both $\mathfrak{q} = \mathfrak{l}$ and $\mathfrak{q} = \bar{\mathfrak{l}}$. As in Step 4 of the proof of Theorem 6.2, this gives $(k, k') \in \mathcal{T}$ and $\zeta_1, \zeta_2 \in \mu_3$ with (6.1), which Step 5 of that proof excludes for $p \geq 17$. □

Remark 7.10. Properties (M1)–(M3) alone do not exclude a reducible system: in the unramified case with $N = 0$ they are satisfied by the system with members $1 \oplus \varepsilon_\ell^{-1} \oplus \varepsilon_\ell^{-2}$. The proof excludes such systems using only that $\psi(\mathfrak{q})$ is an eigenvalue of Frobenius at the two primes above 7, that is, the congruence with $\bar{\rho}$ there.

8. The member at 5: ramification, discriminants, groups and fields

The members above 5 of a compatible system as in Section 7.6 are crystalline at 5 with Hodge–Tate weights in the Fontaine–Laffaille range, which bounds the ramification of their reductions modulo 5 (Proposition 8.2). With this bound, the lower bounds for discriminants, the facts on finite groups and the class numbers given below, Section 9 shows that their monodromy at $\mathfrak{p}$ is not zero (step (1) of Section 1.5). The *root discriminant* of a number field L of degree n and discriminant d_L is $\mathrm{rd}(L) = |d_L|^{1/n}$. Upper ramification groups G^y ($y \geq -1$ real) are numbered as in [101, Chapitre IV]; so $G^y = 1$ for $y > 0$ in a tamely ramified extension.

8.1. **Notation.** From now on in this part, λ is a prime of M above 5 and $R = R_\lambda$. The prime 5 is inert in K. The completion of K at 5 is $\mathbb{Q}_{25}$, the unramified quadratic extension of $\mathbb{Q}_5$, and $G_{\mathbb{Q}_{25}} \subset G_K$ is a decomposition group at 5. Let $E \subset \overline{M}_\lambda$ be a finite extension of $\mathbb{Q}_5$ over which R is defined, with ring of integers $\mathcal{O}_E$, maximal ideal $\mathfrak{m}_E$ and residue field $\mathbb{F}_E$. A *stable lattice* is a G_K-stable $\mathcal{O}_E$-lattice Λ in the space of R, and its reduction is $\overline{R}_\Lambda = \Lambda/\mathfrak{m}_E\Lambda$, a representation of G_K over $\mathbb{F}_E$. The semisimplification $\overline{R}^{\mathrm{ss}}$ of $\overline{R}_\Lambda$ is independent of Λ. We enlarge E when needed, so that every constituent of $\overline{R}^{\mathrm{ss}}$ is absolutely irreducible and E contains $\mathbb{Q}_{25}$.

As $5 \notin \{3, 7, p\}$, Propositions 7.8 and 7.9 apply: R is irreducible, and it has the properties (M1)–(M3). By (M3) there is a unipotent automorphism U of the space of R, the image under $R \otimes \kappa_\lambda^{-1}$ of a topological generator of the tame inertia group at $\mathfrak{p}$, such that every $\sigma \in I_\mathfrak{p}$ acts by $\kappa_\lambda(\sigma)U^{t_5(\sigma)}$, where $t_5(\sigma) \in \mathbb{Z}_5$ is defined by that generator. The representation R is polarized (Section 7.2): there is a nondegenerate symmetric pairing Ψ on its space with $\Psi(\sigma x, (\tilde{\mathsf{c}}\sigma\tilde{\mathsf{c}})y) = \varepsilon_5(\sigma)^{-2}\Psi(x, y)$; in particular $R^{\mathsf{c}} \cong R^\vee \otimes \varepsilon_5^{-2}$.

8.2. **Ramification.**

Theorem 8.1 (Fontaine; Abrashkin)**.** *Let ℓ be a prime, F a finite unramified extension of $\mathbb{Q}_\ell$, and h an integer with $0 \leq h \leq \ell - 2$. Let V be a crystalline representation of G_F on a finite-dimensional $\mathbb{Q}_\ell$-vector space with Hodge–Tate weights in $[0, h]$, and let $T' \subset T$ be G_F-stable $\mathbb{Z}_\ell$-lattices in V with $\ell T \subset T'$. Then the ramification groups G_F^y, $y > h/(\ell - 1)$, act trivially on T/T'.*

This is [1, §2, 8.1] (generalized in [2, Theorem 2.3]); for $h = 1$ it is Fontaine's theorem on finite flat group schemes [53]. It is also established in the course of the proof of [54, Théorème 2], and [69, Theorem 2.19, Corollary 2.13 and §4.4] gives a proof (there $G^{(j)} = G^{j-1}$). The convention for the sign of the weights does not matter, and the interval $[0, h]$ may be replaced by any interval of length h: twisting V by a power of ε_ℓ twists T/T' by a power of $\bar{\varepsilon}_\ell$, which is tamely ramified and so trivial on G_F^y for $y > 0$.

Proposition 8.2. *Let Λ be a stable lattice and Θ a subquotient of the $\mathbb{F}_E[G_K]$-module $\overline{R}_\Lambda$.*

(a) *The ramification groups $G^y_{\mathbb{Q}_{25}}$, $y > 1/2$, act trivially on Θ.*

(b) *U stabilizes Λ; let $\bar{U}_\Theta$ be the automorphism of Θ that it induces. It is unipotent, of order 1 or 5, and $\sigma \in I_\mathfrak{p}$ acts on Θ by $\bar{\kappa}_\lambda(\sigma)\bar{U}_\Theta^{t_5(\sigma)}$. So the image of $I_\mathfrak{p}$ in the projective linear group of Θ is generated by the image of $\bar{U}_\Theta$; it is tame, of order 1 or 5.*

(c) *Θ is unramified outside $\{\mathfrak{p}, 5\}$.*

(d) *Let L/K be a finite Galois extension contained in the field cut out by the projective representation attached to Θ, let $e_{\mathfrak{p}} \in \{1,5\}$ be the order of its inertia groups at $\mathfrak{p}$, and let 5^m be the order of its wild inertia groups at 5. Then*

$$\operatorname{rd}(L) < 3^{\,1-1/(2e_{\mathfrak{p}})} \cdot 5^{\,1+(1-5^{-m})/2}.$$

In particular $\operatorname{rd}(L) < 3^{1/2}\cdot 5^{3/2}$ *if* $e_{\mathfrak{p}} = 1$; $\operatorname{rd}(L) < 3^{1/2}\cdot 5^{7/5}$ *if* $e_{\mathfrak{p}} = 1$ *and* $25 \nmid [L:K]$; *and* $\operatorname{rd}(L) < 3^{1/2}\cdot 5$ *if* $e_{\mathfrak{p}} = 1$ *and* $5 \nmid [L:K]$.

Proof. (a) By (M2), $R|_{G_{\mathbb{Q}_{25}}}$, viewed as a representation over $\mathbb{Q}_5$, is crystalline with Hodge–Tate weights in $[0,2]$, and $\Lambda \supset \mathfrak{m}_E\Lambda \supset 5\Lambda$ are $G_{\mathbb{Q}_{25}}$-stable $\mathbb{Z}_5$-lattices in it. Apply Theorem 8.1 with $\ell = 5$, $F = \mathbb{Q}_{25}$ and $h = 2 \le \ell - 2$: the groups $G^y_{\mathbb{Q}_{25}}$ with $y > 2/4$ act trivially on $\Lambda/\mathfrak{m}_E\Lambda$, hence on Θ.

(b) $U = R(\sigma_0)\kappa_\lambda(\sigma_0)^{-1}$ for some $\sigma_0 \in I_{\mathfrak{p}}$, so U stabilizes Λ; as $(U-1)^3 = 0$, its reduction satisfies $(\bar{U}-1)^5 = \bar{U}^5 - 1 = 0$. The character $\bar{\kappa}_\lambda$ is a scalar, and the wild inertia group at $\mathfrak{p}$, a pro-3 group, acts through it.

(c) is (M1).

(d) By (c), L is unramified outside $\{3,5\}$. The primes of L above 3 are conjugate, and so are those above 5. At 3, $L/\mathbb{Q}$ is tamely ramified with ramification index $2e_{\mathfrak{p}}$, which contributes $3^{1-1/(2e_{\mathfrak{p}})}$ to $\operatorname{rd}(L)$. At 5, let $\Delta_5 \subset \operatorname{Gal}(L/K)$ be a decomposition group, with ramification groups Δ_5^y in the upper numbering. Since $\mathbb{Q}_{25}/\mathbb{Q}_5$ is unramified, the exponent of 5 in $\operatorname{rd}(L)$ is the valuation, normalized by $v(5) = 1$, of the different of the corresponding extension of $\mathbb{Q}_{25}$, which is

$$\int_{-1}^{\infty} \Big(1 - \frac{1}{|\Delta_5^y|}\Big)\, dy$$

([101, Chapitre IV, §1, Proposition 4] and the definition of the upper numbering). By (a), $\Delta_5^y = 1$ for $y > 1/2$; for $y > 0$, Δ_5^y is contained in the wild inertia subgroup, of order 5^m; and for $-1 < y \le 0$ it is the inertia subgroup Δ_5^0. So the exponent is at most $(1 - 1/|\Delta_5^0|) + \frac{1}{2}(1-5^{-m}) < 1 + \frac{1}{2}(1-5^{-m})$. If $25 \nmid [L:K]$ then $m \le 1$, and if $5 \nmid [L:K]$ then $m = 0$. □

8.3. **Lower bounds for root discriminants.** Let L be a number field of degree n with r_1 real places, and let $\Phi\colon \mathbb{R} \to \mathbb{R}$ be an even, twice continuously differentiable function with compact support and $\Phi(0) = 1$. Put

$$I_1(\Phi) = \int_0^\infty \frac{1-\Phi(x)}{2\sinh(x/2)}\, dx, \qquad I_1'(\Phi) = \int_0^\infty \frac{1-\Phi(x)}{2\cosh(x/2)}\, dx,$$
$$I_2(\Phi) = \int_0^\infty \Phi(x)\cosh(x/2)\, dx,$$

and $\widehat{\Phi}(s) = \int_{-\infty}^{\infty} \Phi(x) e^{(s-1/2)x}\, dx$. Weil's explicit formula, in the form given by Poitou [93, pp. 6-06 and 6-07, formula (6)] (see also [91, §2]), reads

$$\log|d_L| = n(\gamma + \log 8\pi) + r_1\frac{\pi}{2} - nI_1(\Phi) - r_1 I_1'(\Phi) - 4I_2(\Phi) + \sum_{\varrho} \widehat{\Phi}(\varrho) + 2\sum_{\mathfrak{r}} \sum_{m\ge 1} \frac{\log \mathrm{N}\,\mathfrak{r}}{\mathrm{N}\,\mathfrak{r}^{m/2}}\, \Phi(m \log \mathrm{N}\,\mathfrak{r}), \quad (8.1)$$

where γ is Euler's constant, ϱ runs over the zeros of the Dedekind zeta function ζ_L with $0 < \operatorname{Re}\varrho < 1$ (the sum being the limit of the sums over $|\operatorname{Im}\varrho| < x$ as $x \to \infty$), and $\mathfrak{r}$

runs over the prime ideals of L. If $\Phi \geq 0$ the last sum is nonnegative, and if moreover $\sum_\varrho \operatorname{Re}\widehat{\Phi}(\varrho) \geq 0$ we get

$$\log \operatorname{rd}(L) \;\geq\; \gamma + \log 8\pi + \frac{r_1}{n}\Big(\frac{\pi}{2} - I_1'(\Phi)\Big) - I_1(\Phi) - \frac{4}{n}\, I_2(\Phi). \tag{8.2}$$

Let $\Phi_0(x) = (1-|x|)\cos(\pi x) + \frac{1}{\pi}\sin(\pi|x|)$ for $|x| \leq 1$ and $\Phi_0(x) = 0$ for $|x| > 1$ [93, (9)]. It is twice continuously differentiable and nonnegative, and it is twice the convolution square of the function equal to $\cos(\pi x)$ on $[-\frac{1}{2}, \frac{1}{2}]$ and to 0 elsewhere, so its Fourier transform is nonnegative. For $b > 0$ we use the test function $\Phi(x) = \Phi_0(x/b)/\cosh(x/2)$. For a zero $\varrho = \beta + it$, $\operatorname{Re}\widehat{\Phi}(\varrho)$ is the Fourier transform at t of $\Phi_0(x/b)\cosh((\beta - \frac{1}{2})x)/\cosh(x/2)$, a product of two functions with nonnegative Fourier transforms (that of $\cosh(\alpha x)/\cosh(x/2)$, for $|\alpha| < \frac{1}{2}$, is $4\pi\cosh(\pi t)\cos(\pi\alpha)/(\cosh 2\pi t + \cos 2\pi\alpha)$); so it is nonnegative, and (8.2) holds unconditionally [93, Proposition 5]. Here $I_2(\Phi) = 4b/\pi^2$. For fixed b, and for $r_1 = 0$ or $r_1 = n$, the right side of (8.2) increases with n. This is the method of Odlyzko. For totally complex fields the supremum over b and n of these bounds is $4\pi e^\gamma < 22.39$.

Proposition 8.3. *Let L be a totally complex number field of degree n. If $n \geq 18$ then $\operatorname{rd}(L) > 9.2709$; if $n \geq 120$ then $\operatorname{rd}(L) > 16.9886$; if $n \geq 2002$ then $\operatorname{rd}(L) > 21.4136$. On the other hand*

$$3^{1/2}\cdot 5 < 8.6603, \qquad 3^{1/2}\cdot 5^{7/5} < 16.4862, \qquad 3^{1/2}\cdot 5^{3/2} < 19.3650.$$

Proof. The right side of (8.2), with $r_1 = 0$, was evaluated with certified error bounds (Appendix A, item C4) at $(n, b) = (18, \frac{23}{4})$, $(120, 13)$ and $(2002, 36)$; any $b > 0$ is admissible, and these values of b are close to optimal. The exponential of each value exceeds the number stated, and the bounds increase with n. □

The proof of Theorem 9.3 needs these bounds for $[L : \mathbb{Q}] \geq 18$, $[L : \mathbb{Q}] \geq 120$ and $[L : \mathbb{Q}] \geq 7200$; in the last case any degree up to 7200 at which the bound exceeds 19.3650 would serve, and 2002 is one.

The exponent $3/2$ at 5 in Proposition 8.2 (d) is what makes the method work: $3^{1/2}\cdot 5^{3/2} < 19.37$ lies below the supremum $4\pi e^\gamma$ of these bounds. A crystalline representation with Hodge–Tate weights in an interval of length 3 is still covered by Theorem 8.1 at $\ell = 5$, since $3 \leq \ell - 2$, but only for $y > 3/4$. The argument of Proposition 8.2 (d) then gives the exponent $1 + \frac{3}{4} = \frac{7}{4}$ at 5 in place of $\frac{3}{2}$, and $3^{1/2}\cdot 5^{7/4} > 28.9$, far above that supremum.

8.4. **Finite groups.** For a finite group Δ, $O_5(\Delta)$ is its largest normal 5-subgroup.

Lemma 8.4. *Let $d \in \{2, 3\}$ and let $\Delta \subset \mathrm{PGL}_d(\overline{\mathbb{F}}_5)$ be a finite subgroup whose preimage in $\mathrm{GL}_d(\overline{\mathbb{F}}_5)$ acts irreducibly on $\overline{\mathbb{F}}_5^d$. If 5 divides $|\Delta|$, then Δ has no nontrivial abelian normal subgroup. In particular Δ is not solvable, $|\Delta| \geq 60$, and $O_5(\Delta) = 1$.*

Proof. Let $\tilde{\Delta} \subset \mathrm{SL}_d(\overline{\mathbb{F}}_5)$ be the preimage of Δ; it is finite and irreducible. Let $A \neq 1$ be an abelian normal subgroup of Δ and $\tilde{A}$ its preimage, a normal subgroup of $\tilde{\Delta}$ whose commutator subgroup lies in the center μ_d; so $\tilde{A}$ is nilpotent. By Clifford's theorem the restriction of $\overline{\mathbb{F}}_5^d$ to $\tilde{A}$ is semisimple and $\tilde{\Delta}$ permutes its isotypic components transitively. As d is prime there are three cases.

(i) There are d components. They are lines, $\tilde{\Delta}$ permutes them, and the kernel of $\tilde{\Delta} \to S_d$ consists of diagonal matrices, so its order is prime to 5; as $|S_d|$ divides 6, $5 \nmid |\Delta|$.

(ii) There is one component, a multiple of a character. Then $\tilde{A}$ consists of scalars and $A = 1$.

(iii) $\tilde{A}$ acts irreducibly. The Sylow 5-subgroup of the nilpotent group $\tilde{A}$ is normal in $\tilde{\Delta}$; its fixed vectors form a nonzero $\tilde{\Delta}$-stable subspace, which is therefore the whole space, so this Sylow subgroup is trivial. An irreducible representation of a nilpotent group of order prime to 5 is a tensor product of irreducible representations of its Sylow subgroups, whose degrees are powers of the corresponding primes. As d is prime, the Sylow d-subgroup acts irreducibly and the other Sylow subgroups act by scalars. Scalars of order prime to d in SL_d are trivial, so $\tilde{A}$ is a d-group. Its center consists of scalars, so it is μ_d, and $\tilde{A}/\mu_d = A$ is abelian. The character of a faithful irreducible representation of such a group vanishes outside the center, so $d^2 = [\tilde{A} : \mu_d] = |A|$; and A is not cyclic, since otherwise $\tilde{A}$ would be abelian. So $A \cong (\mathbb{Z}/d)^2$. An element x of $\mathrm{GL}_d(\overline{\mathbb{F}}_5)$ whose image commutes with A satisfies $xqx^{-1} = \eta(q)q$ for $q \in \tilde{A}$, with η a character of A with values in μ_d; the commutator pairing identifies A with the group of such characters, so x differs from an element of $\tilde{A}$ by an element commuting with $\tilde{A}$, a scalar. Hence A is its own centralizer in $\mathrm{PGL}_d(\overline{\mathbb{F}}_5)$, and Δ/A embeds in $\mathrm{Aut}(A) = \mathrm{GL}_2(\mathbb{Z}/d)$, of order 6 or 48. So $|\Delta|$ divides 24 or 432, and $5 \nmid |\Delta|$.

Each case contradicts $5 \mid |\Delta|$ or $A \neq 1$. A nontrivial solvable group has a nontrivial abelian normal subgroup (the last nontrivial term of its derived series), and the smallest non-solvable group has order 60. Finally, if $O_5(\Delta) \neq 1$ its center would be a nontrivial abelian normal subgroup. □

Lemma 8.5. *The following statements on finite groups hold.*

(a) *A finite group with no nontrivial abelian normal subgroup and of order divisible by* 25 *has order at least* 3600*.*

(b) *A finite subgroup of* $\mathrm{PGL}_3(\overline{\mathbb{F}}_5)$ *whose preimage in* $\mathrm{GL}_3(\overline{\mathbb{F}}_5)$ *is irreducible has order at least* 9*.*

(c) *A finite subgroup of* $\mathrm{PGL}_2(\overline{\mathbb{F}}_5)$ *of order prime to* 5 *whose preimage in* $\mathrm{GL}_2(\overline{\mathbb{F}}_5)$ *is irreducible is dihedral of order* $2m \geq 4$*, or isomorphic to* A_4 *or* S_4*.*

Proof. We use two standard facts. First, if a finite group Δ has no nontrivial abelian normal subgroup, then its socle is a direct product of non-abelian simple groups and has trivial centralizer, so Δ embeds in the automorphism group of its socle. Second, the non-abelian simple groups of order less than 3600 are A_5, $\mathrm{PSL}_2(\mathbb{F}_7)$, A_6, $\mathrm{PSL}_2(\mathbb{F}_8)$, $\mathrm{PSL}_2(\mathbb{F}_{11})$, $\mathrm{PSL}_2(\mathbb{F}_{13})$, $\mathrm{PSL}_2(\mathbb{F}_{17})$, A_7, $\mathrm{PSL}_2(\mathbb{F}_{19})$, of orders 60, 168, 360, 504, 660, 1092, 2448, 2520, 3420, and their automorphism groups have orders 120, 336, 1440, 1512, 1320, 2184, 4896, 5040, 6840 [34]; none of these is divisible by 25.

(a) If the socle has at least two simple factors, its order is at least 60^2; if it is a simple group S of order less than 3600, then $|\Delta|$ divides $|\mathrm{Aut}(S)|$, which is not divisible by 25.

(b) If the order of the group is prime to 5, the representation of its preimage $\tilde{\Delta}$ in $\mathrm{SL}_3(\overline{\mathbb{F}}_5)$ lifts to an irreducible representation in characteristic 0, of degree 3, and $9 \leq [\tilde{\Delta} : \mu_3]$. Otherwise Lemma 8.4 gives order at least 60.

(c) The preimage in $\mathrm{SL}_2(\overline{\mathbb{F}}_5)$ has order prime to 5, so it lifts to characteristic 0, and the group is isomorphic to a finite subgroup of $\mathrm{PGL}_2(\mathbb{C})$: cyclic, dihedral, A_4, S_4 or A_5. A cyclic group has an abelian, hence reducible, preimage, and $|A_5|$ is divisible by 5. □

8.5. **Class numbers and abelian extensions.**

Lemma 8.6. *The following statements hold.*

(a) *The fields* K*,* $K(\sqrt{5})$ *and* $K(\zeta_5) = \mathbb{Q}(\zeta_{15})$ *have class number one.*

(b) *The abelian extensions of K of degree prime to 5 that are unramified outside 5 are K, $K(\sqrt{5})$ and $K(\zeta_5)$; and* $\mathrm{Gal}(K(\zeta_5)/K) \cong \mathbb{Z}/4$.

(c) *An abelian extension of $K(\sqrt{5})$ of degree prime to 5 that is unramified outside 5 has degree at most 2 over $K(\sqrt{5})$.*

Proof. (a) The three fields are totally complex, of degrees 2, 4, 8 and discriminants -3, $3^2 \cdot 5^2$, $3^4 \cdot 5^6$, so their Minkowski bounds are smaller than 1.11, 2.28 and 7.11. No prime ideal has norm below the bound: in $K(\sqrt{5})$ the primes above 2 have norm 4 (2 is inert in K and in $\mathbb{Q}(\sqrt{5})$); in $\mathbb{Q}(\zeta_{15})$ the primes above 2, 3, 5, 7 have norms 16, 81, 25, 2401. So every ideal class contains the unit ideal.

(b) Such an extension is tamely ramified at the prime $5\mathcal{O}$, so its conductor divides $5\mathcal{O}$. As K has class number one, no real place and unit group μ_6, the ray class group of conductor $5\mathcal{O}$ is $\mathbb{F}_{25}^\times/\mu_6 \cong \mathbb{Z}/4$. The extension $K(\zeta_5)/K$ is abelian of degree 4, unramified outside 5 and tamely ramified, so it is the ray class field, and its subextensions are the three fields named.

(c) The field $K(\sqrt{5})$ has one prime $\mathfrak{Q}$ above 5, with residue field $\mathbb{F}_{25}$, and the conductor of the extension divides $\mathfrak{Q}$. By (a) the ray class group of conductor $\mathfrak{Q}$ is the quotient of $\mathbb{F}_{25}^\times$ by the image of the units. The image of $-\omega$ has order 6, and the image of $(1+\sqrt{5})/2$ is $1/2 = 3$, of order 4; together they generate a subgroup of order 12 of the cyclic group $\mathbb{F}_{25}^\times$. The image of the full unit group contains this subgroup, so the quotient has order at most 2. □

9. The reductions modulo 5

In the notation of Section 8.1, this section carries out step (1) of Section 1.5: the monodromy at $\mathfrak{p}$ of every member above 5 of a compatible system as in Section 7.6 is not zero (Theorem 9.3), and so $\bar\rho(I_\mathfrak{p})$ is not contained in the scalar matrices (Proposition 9.5).

9.1. **Constituents.** We use Fontaine–Laffaille theory [57] in the normalization of [10, §1.4], for the unramified extension $\mathbb{Q}_{25}/\mathbb{Q}_5$ with ring of integers $\mathbb{Z}_{25}$. Let $\mathcal{MF}$ be the category of finite $\mathbb{Z}_{25} \otimes_{\mathbb{Z}_5} \mathcal{O}_E$-modules $\mathcal{D}$ with a decreasing filtration by submodules $\mathrm{Fil}^i \mathcal{D}$ that are direct summands over $\mathbb{Z}_{25}$, with $\mathrm{Fil}^0 \mathcal{D} = \mathcal{D}$ and $\mathrm{Fil}^4 \mathcal{D} = 0$, and with Frobenius-semilinear maps $\varphi_i \colon \mathrm{Fil}^i \mathcal{D} \to \mathcal{D}$ such that $\varphi_i|_{\mathrm{Fil}^{i+1}\mathcal{D}} = 5\varphi_{i+1}$ and $\sum_i \varphi_i(\mathrm{Fil}^i \mathcal{D}) = \mathcal{D}$. There is an exact, fully faithful, covariant, $\mathcal{O}_E$-linear functor $\mathbf{T}$ from $\mathcal{MF}$ to the category of finite $\mathcal{O}_E$-modules with a continuous action of $G_{\mathbb{Q}_{25}}$, whose essential image is closed under subobjects and quotients. For an object $\mathcal{D}$ killed by $\mathfrak{m}_E$ and an embedding $\tau \colon \mathbb{Q}_{25} \to E$, the *jumps* of $\mathcal{D}$ at τ are the integers i such that the τ-component of $\mathrm{Fil}^i \mathcal{D}/\mathrm{Fil}^{i+1}\mathcal{D}$ is nonzero, counted with its dimension over $\mathbb{F}_E$. If $\mathcal{D}$ is torsion-free, then $\mathbf{T}(\mathcal{D}) \otimes \mathbb{Q}_5$ is crystalline and its Hodge–Tate weights at τ are the jumps of $\mathcal{D}/\mathfrak{m}_E\mathcal{D}$ at τ; and every $G_{\mathbb{Q}_{25}}$-stable lattice in a crystalline representation with Hodge–Tate weights in $[0,3]$ is in the image of $\mathbf{T}$. An object killed by $\mathfrak{m}_E$ that has a filtration by subobjects with graded pieces of rank one over $\mathbb{F}_{25} \otimes \mathbb{F}_E$ is the reduction of a torsion-free object with a filtration lifting the given one [10, Lemma 1.4.2]. Let τ, τ' be the two embeddings of $\mathbb{Q}_{25}$ in E.

Recall the set of types $\mathcal{T} = \{(0,0), (1,1), (2,2), (0,2), (2,0)\}$ of Section 6.

Lemma 9.1. *Let Λ be a stable lattice.*

(i) *$\overline{R}_\Lambda|_{G_{\mathbb{Q}_{25}}} = \mathbf{T}(\bar{\mathcal{D}})$ for an object $\bar{\mathcal{D}}$ whose jumps are $\{0,1,2\}$ at τ and at τ'. Every subquotient of $\overline{R}_\Lambda|_{G_{\mathbb{Q}_{25}}}$ is the image under $\mathbf{T}$ of a subquotient of $\bar{\mathcal{D}}$, and jumps are additive in exact sequences.*

(ii) *Let $\theta\colon G_K \to \mathbb{F}_E^\times$ be a one-dimensional constituent of $\overline{R}^{\mathrm{ss}}$, and let (k,k') be its jumps at (τ,τ'). Then $(k,k') \in \mathcal{T}$. In the unramified case, $k = k'$ and $\theta = \bar{\varepsilon}_5^{-k}$. In the ramified case, either $(k,k') = (0,2)$ for all such θ, or $(k,k') = (2,0)$ for all such θ.*

(iii) *$\overline{R}^{\mathrm{ss}}$ is a sum of three characters only in the unramified case, and then $\overline{R}^{\mathrm{ss}} = 1 \oplus \bar{\varepsilon}_5^{-1} \oplus \bar{\varepsilon}_5^{-2}$, three distinct characters.*

(iv) *Let Θ be a subquotient of $\overline{R}_\Lambda$ that is an extension of $\bar{\varepsilon}_5^{-j}$, $j \in \{0,1\}$, by a subrepresentation isomorphic to $\bar{\varepsilon}_5^{-2}$. Then Θ is split as a representation of $G_{\mathbb{Q}_{25}}$.*

Proof. (i) By (M2), Λ is a lattice in a crystalline representation with Hodge–Tate weights $\{0,1,2\}$ at both embeddings, so $\Lambda = \mathbf{T}(\mathcal{D})$; by exactness and full faithfulness $\mathcal{D}$ is torsion-free, $\overline{R}_\Lambda = \mathbf{T}(\mathcal{D}/\mathfrak{m}_E\mathcal{D})$, and the jumps of $\bar{\mathcal{D}} = \mathcal{D}/\mathfrak{m}_E\mathcal{D}$ are the Hodge–Tate weights. The rest follows from the properties of $\mathbf{T}$ and the strictness of morphisms in $\mathcal{MF}$ with respect to the filtrations.

(ii) By (i), $\theta|_{G_{\mathbb{Q}_{25}}}$ is the image of an object of rank one with jumps $k,k' \in \{0,1,2\}$, which lifts to a torsion-free object, so $\theta|_{G_{\mathbb{Q}_{25}}}$ is the reduction of a crystalline character with Hodge–Tate weights (k,k'). On the inertia group, identified with $\mathbb{Z}_{25}^\times$ by local class field theory, such a character is $x \mapsto \tau(x)^{\pm k}\tau'(x)^{\pm k'}$, so θ is $x \mapsto \bar{\tau}(x)^{\pm(k+5k')}$ there, where $\bar{\tau}(x) \in \mathbb{F}_E^\times$ is the residue class of $\tau(x)$, and the sign is fixed by the normalizations. By Proposition 8.2, θ is unramified outside $\{\mathfrak{p},5\}$, and $\theta|_{I_\mathfrak{p}} = \bar{\kappa}_\lambda$. Let $\theta_\mathfrak{p}$ be the character of $\mathcal{O}_\mathfrak{p}^\times$ attached to $\theta|_{I_\mathfrak{p}}$ by class field theory. Its order divides 3. The idele class character of θ is trivial on $\mu_6 \subset K^\times$, so $\theta_\mathfrak{p}(\zeta)\,\bar{\tau}(\zeta)^{\pm(k+5k')} = 1$ for $\zeta \in \mu_6$. For $\zeta = -1$ this gives $(-1)^{k+k'} = 1$, so $(k,k') \in \mathcal{T}$. For $\zeta = \omega$ it gives $\theta_\mathfrak{p}(\omega) = \bar{\tau}(\omega)^{\mp(k-k')}$, because $\omega^5 = \omega^{-1}$. In the unramified case $\theta_\mathfrak{p}$ is trivial, so $k \equiv k'$ modulo 3 and modulo 2, hence $k = k'$; then $\theta\bar{\varepsilon}_5^{k}$ is unramified at 5 (all crystalline characters with the same Hodge–Tate weights agree on inertia), at $\mathfrak{p}$ and everywhere else, so it is trivial, because K has class number one. In the ramified case $\theta_\mathfrak{p}$ is a character of order 3 of $\mathcal{O}_\mathfrak{p}^\times/(1+\mathfrak{p}^2) \cong \mu_6$ (by (F3) and (M3)), so $\theta_\mathfrak{p}(\omega) \neq 1$ and $k \not\equiv k'$ (mod 3): (k,k') is $(0,2)$ or $(2,0)$, and which of the two is determined by $\theta_\mathfrak{p}(\omega) = \bar{\kappa}_\lambda(\mathrm{Art}_\mathfrak{p}(\omega))$.

(iii) By (i) the jumps of the three characters at τ are $0,1,2$ in some order. By (ii) this is impossible in the ramified case, and in the unramified case the characters are $\bar{\varepsilon}_5^{-k}$ with $k = 0,1,2$. They are distinct because $\bar{\varepsilon}_5$ has order 4 on G_K.

(iv) $\Theta|_{G_{\mathbb{Q}_{25}}} = \mathbf{T}(\mathcal{D}_\Theta)$ with $\mathcal{D}_\Theta$ an extension of an object $\mathcal{D}_2$ of rank one with jumps (j,j) by a subobject $\mathcal{D}_1$ of rank one with jumps $(2,2)$. By strictness, $\mathrm{Fil}^i \mathcal{D}_\Theta = \mathcal{D}_\Theta$ for $i \le j$ and $\mathrm{Fil}^i \mathcal{D}_\Theta = \mathcal{D}_1$ for $j < i \le 2$. Let $e_\tau, e_{\tau'}$ generate the two components of $\mathcal{D}_1$ and let $f_\tau, f_{\tau'} \in \mathcal{D}_\Theta$ lift generators of the two components of $\mathcal{D}_2$. Since $e_\tau \in \mathrm{Fil}^{j+1}\mathcal{D}_\Theta$, $\varphi_j(e_\tau) = 5\varphi_{j+1}(e_\tau) = 0$. Write $\varphi_j(f_\tau) = \beta_\tau f_{\tau''} + y_\tau e_{\tau''}$, where τ'' is the other embedding and $\beta_\tau \in \mathbb{F}_E^\times$. Replacing $f_{\tau''}$ by $f_{\tau''} + (y_\tau/\beta_\tau)e_{\tau''}$, for both τ, does not change $\varphi_j(f_\tau)$ and makes $y_\tau = 0$. Then $f_\tau, f_{\tau'}$ span a subobject mapping isomorphically to $\mathcal{D}_2$: the extension of filtered modules splits, and so does $\Theta|_{G_{\mathbb{Q}_{25}}}$. □

With Hodge–Tate weights normalized as in Section 2, (iv) says that an extension, in the image of $\mathbf{T}$, of a character by a character of larger Hodge–Tate weight splits. For weights 0 and 1 this is the splitting of an extension of a multiplicative group scheme by an étale one, whereas extensions in the other direction (the Kummer ones) can be nonsplit.

9.2. **A lattice with a prescribed socle.**

Lemma 9.2. *Let Θ be a constituent of $\overline{R}^{\mathrm{ss}}$ of multiplicity one. Then there is a stable lattice Λ' such that Θ is the unique irreducible subrepresentation of $\overline{R}_{\Lambda'}$.*

Proof. Passing to the dual of R and to dual lattices, it suffices to find a stable lattice whose reduction has Θ as its unique irreducible quotient. Fix a stable lattice Λ_0, and let $\mathfrak{L}$ be the set of stable lattices $\Lambda \subset \Lambda_0$ such that Θ is not a constituent of Λ_0/Λ. It is closed under finite intersections. Let X_0 be the smallest subrepresentation of $\Lambda_0/\mathfrak{m}_E\Lambda_0$ whose quotient does not have Θ as a constituent. It is nonzero, and the image of every $\Lambda \in \mathfrak{L}$ in $\Lambda_0/\mathfrak{m}_E\Lambda_0$ contains it. So the sets $\Lambda \smallsetminus \mathfrak{m}_E\Lambda_0$, $\Lambda \in \mathfrak{L}$, are nonempty and compact, and any finite number of them have a common point. Hence $\Lambda_\infty = \bigcap_{\Lambda\in\mathfrak{L}} \Lambda$ is nonzero. It is a G_K-stable $\mathcal{O}_E$-submodule of Λ_0, so it is a lattice, because R is irreducible (Proposition 7.9). Then $\mathfrak{m}_E^m\Lambda_0 \subset \Lambda_\infty$ for some m, and as $\Lambda_0/\mathfrak{m}_E^m\Lambda_0$ is finite, Λ_∞ is a finite intersection of members of $\mathfrak{L}$; so Λ_∞ is the smallest element of $\mathfrak{L}$. If $\overline{R}_{\Lambda_\infty}$ had an irreducible quotient not isomorphic to Θ, the kernel of the map from Λ_∞ to it would be a smaller element of $\mathfrak{L}$. So every irreducible quotient of $\overline{R}_{\Lambda_\infty}$ is isomorphic to Θ, and there is only one, because Θ has multiplicity one. □

9.3. **The main case analysis.**

Theorem 9.3. *Let $\mathcal{R}$ be a compatible system as in Section 7.6, λ a prime of its coefficient field above 5, and Λ a stable lattice of $R = R_\lambda$. Then one of the following holds.*

(A) *$\overline{R}_\Lambda$ is irreducible; put $\Theta = \overline{R}_\Lambda$.*
(B) *$\overline{R}^{\mathrm{ss}} = \theta \oplus \Theta$ with θ a character and Θ irreducible of dimension 2.*

In both cases let Δ be the projective image of Θ and L the field it cuts out. Then:

(1) *L is a Galois extension of $\mathbb{Q}$ of degree $2|\Delta|$, it contains K, and it is unramified outside $\{3, 5\}$;*
(2) *the inertia groups of L/K at $\mathfrak{p}$ have order 5; in particular $\bar{U}_\Theta \neq 1$, and the matrix N of* (P3) *is not zero.*

Proof. After enlarging E, $\overline{R}^{\mathrm{ss}}$ is irreducible, or the sum of a character and an irreducible representation of dimension 2, or a sum of three characters. The polarization of R gives $(\overline{R}^{\mathrm{ss}})^{\mathsf{c}} \cong (\overline{R}^{\mathrm{ss}})^\vee \otimes \bar\varepsilon_5^{-2}$. In the first two cases this gives $\Theta^{\mathsf{c}} \cong \Theta^\vee \otimes \bar\varepsilon_5^{-2}$, so the kernel of the projective representation of Θ is stable under $\tilde{\mathsf{c}}$ and $L/\mathbb{Q}$ is Galois; L contains K, it is totally complex of degree $2|\Delta|$, and it is unramified outside $\{3, 5\}$ by Proposition 8.2 (c). Let $e_\mathfrak{p} \in \{1, 5\}$ be the order of the inertia groups of L/K at $\mathfrak{p}$ (Proposition 8.2 (b)).

Three characters. By Lemma 9.1 (iii) we are in the unramified case and $\overline{R}^{\mathrm{ss}} = 1 \oplus \bar\varepsilon_5^{-1} \oplus \bar\varepsilon_5^{-2}$. By Lemma 9.2 there is a stable lattice Λ' such that $\bar\varepsilon_5^{-2}$ is the unique irreducible subrepresentation of $\overline{R}_{\Lambda'}$. An irreducible subrepresentation of $\overline{R}_{\Lambda'}/\bar\varepsilon_5^{-2}$ is $\bar\varepsilon_5^{-j}$ with $j \in \{0, 1\}$, and its preimage in $\overline{R}_{\Lambda'}$ is a nonsplit extension of $\bar\varepsilon_5^{-j}$ by $\bar\varepsilon_5^{-2}$. Its class is a nonzero element of $H^1(G_K, \mathbb{F}_E(\eta))$ with $\eta = \bar\varepsilon_5^{j-2} \in \{\bar\varepsilon_5^{-1}, \bar\varepsilon_5^{-2}\}$. This class is unramified outside $\{\mathfrak{p}, 5\}$ (Proposition 8.2 (c)) and trivial on $G_{\mathbb{Q}_{25}}$ (Lemma 9.1 (iv)). It is also trivial on $G_{K_\mathfrak{p}}$: by the local Euler characteristic formula and local duality, $H^1(G_{K_\mathfrak{p}}, \mathbb{F}_E(\eta)) = 0$, because η and $\eta^{-1}\bar\varepsilon_5$ are nontrivial on $G_{K_\mathfrak{p}}$ (they are unramified at $\mathfrak{p}$, and $\bar\varepsilon_5(\mathrm{Frob}_\mathfrak{p}) = 3^{\pm1}$ has order 4). Let K_η be the field cut out by η: it is $K(\zeta_5)$ or $K(\sqrt{5})$, of degree 4 or 2 over K. This degree is prime to 5, so the restriction of the class to G_{K_η} is a nonzero homomorphism $G_{K_\eta} \to \mathbb{F}_E$, and it is unramified at every place. It defines a cyclic unramified extension of K_η of degree 5, which contradicts Lemma 8.6 (a). So $\overline{R}^{\mathrm{ss}}$ is not a sum of three characters.

Cases (A) and (B) with $e_\mathfrak{p} = 1$. Then L/K is unramified outside 5, and Proposition 8.2 (d) gives $\mathrm{rd}(L) < 3^{1/2} \cdot 5^{3/2}$, $\mathrm{rd}(L) < 3^{1/2} \cdot 5^{7/5}$ if $25 \nmid |\Delta|$, and $\mathrm{rd}(L) < 3^{1/2} \cdot 5$ if $5 \nmid |\Delta|$. We compare with Proposition 8.3.

- If $5 \nmid |\Delta|$ in case (A): $|\Delta| \geq 9$ (Lemma 8.5 (b)), so $[L : \mathbb{Q}] \geq 18$ and $\mathrm{rd}(L) > 9.2709 > 8.6603$.
- If $5 \mid |\Delta|$ in case (B): Δ is dihedral of order $2m \geq 4$, or A_4, or S_4 (Lemma 8.5 (c)). Each of these groups has a quotient that Lemma 8.6 forbids for the Galois group of an extension of K unramified outside 5 of degree prime to 5: $(\mathbb{Z}/2)^2$ if Δ is dihedral with m even, and $\mathbb{Z}/3$ if $\Delta \cong A_4$, by Lemma 8.6 (b); and a dihedral group of order $2m'$ with $m' \geq 3$ odd if Δ is dihedral with m odd ($m' = m$) or $\Delta \cong S_4$ ($m' = 3$, through its quotient S_3). For a dihedral quotient of order $2m'$ the quadratic subextension is $K(\sqrt{5})$ by Lemma 8.6 (b), and it has a cyclic extension of degree m' unramified outside 5, which Lemma 8.6 (c) forbids.
- If $5 \mid |\Delta|$ and $25 \nmid |\Delta|$: $|\Delta| \geq 60$ (Lemma 8.4), so $[L : \mathbb{Q}] \geq 120$ and $\mathrm{rd}(L) > 16.9886 > 16.4862$.
- If $25 \mid |\Delta|$: $|\Delta| \geq 3600$ (Lemma 8.4 and Lemma 8.5 (a)), so $[L : \mathbb{Q}] \geq 7200 \geq 2002$ and $\mathrm{rd}(L) > 21.4136 > 19.3650$.

Each case is contradictory, so $e_{\mathfrak{p}} = 5$.

As $e_{\mathfrak{p}} = 5$, the image of $\bar{U}_\Theta$ in the projective linear group of Θ is not trivial (Proposition 8.2 (b)), so $\bar{U}_\Theta \neq 1$. Then $U \neq 1$, so the monodromy operator of R at $\mathfrak{p}$ is not zero, and neither is N (Proposition 7.8). □

Remark 9.4. The case $e_{\mathfrak{p}} = 1$ of this proof concerns a representation of G_K modulo 5 of Fontaine–Laffaille type with weights in $[0, 2]$ whose projective image cuts out an extension of K unramified outside 5 (in the unramified case the representation itself is unramified outside 5): the situation of the theorems of Abrashkin [1] and Fontaine [54] on smooth proper schemes over rings of integers, which combine the ramification bound of Theorem 8.1 with unconditional lower bounds for discriminants (see [69, §2.4]). Abrashkin asserts that K satisfies his condition SH$(5, 2)$ [1, §7, 5.2 a)] (p. 516 of the English translation) and writes that the proof is analogous to his proof for $\mathbb{Q}$; no proof is printed. That condition, with the upper ramification number $2/(5-1) = 1/2$ itself allowed, as in his proof of 5.1 there, implies the case $e_{\mathfrak{p}} = 1$. The proof above does not rely on this assertion.

9.4. **Inertia at $\mathfrak{p}$ for the Frey representation.**

Proposition 9.5. *For every solution, the group $\bar{\rho}(I_{\mathfrak{p}})$ is not contained in the group of scalar matrices.*

Proof. Suppose that it is. We construct a compatible system as in Section 7.6 for which the matrix N of (P3) is zero, which contradicts Theorem 9.3 (2).

By (7.1), $\bar{\rho}|_{I_{\mathfrak{p}}} = \bar{\kappa}$. Let I_1 be the kernel of κ on $I_{\mathfrak{p}}$. It is normal in $G_{\mathbb{Q}_3}$, because $\kappa^{\mathsf{c}} = \kappa^{-1}$, and the prolongation $\bar{\rho}_{\mathcal{G}}$ (Section 7.4) is trivial on it, because $\bar{\varepsilon}_p^{-2}\bar{\delta}_{K/\mathbb{Q}}$ is trivial on $I_{\mathfrak{p}}$. The group $G_{\mathbb{Q}_3}/I_1$ is the semidirect product of the finite group $\bar{I} = I_{\mathbb{Q}_3}/I_1$, of order 2 or 6, and the closure of the group generated by a Frobenius lift σ_3, which is isomorphic to $\hat{\mathbb{Z}}$. Let $\mathcal{O}'$ be the ring of integers of a finite extension of $\mathbb{Q}_p$ with residue field $\mathbb{F}'$ such that $\bar{\rho}_{\mathcal{G}}$ has values in $\mathcal{G}_3(\mathbb{F}')$.

(1) As $|\bar{I}|$ is prime to p and $\mathcal{G}_3$ is smooth, $\bar{\rho}_{\mathcal{G}}|_{\bar{I}}$ lifts to a homomorphism $h\colon \bar{I} \to \mathcal{G}_3(\mathcal{O}')$. The characters $\mathrm{mult} \circ h$ and $\varepsilon_p^{-2}\delta_{K/\mathbb{Q}}|_{\bar{I}}$ have order prime to p and the same reduction, so they are equal.

(2) The scheme of elements g of $\mathcal{G}_3$ with $g\,h(x)\,g^{-1} = h(\sigma_3 x \sigma_3^{-1})$ for all $x \in \bar{I}$ is the scheme of fixed points of an action of $\bar{I}$ on $\mathcal{G}_3$, so it is smooth over $\mathcal{O}'$ [50, Proposition 3.4]; it has the point $\bar{\rho}_{\mathcal{G}}(\sigma_3)$ over $\mathbb{F}'$, which by Hensel's lemma lifts to a point g_0 over $\mathcal{O}'$. The torus

$\{(t \cdot 1_3, t^2)\}$ is central in $\mathcal{G}_3$, and $\mathrm{mult}(t \cdot 1_3, t^2) = t^2$. Multiplying g_0 by the element of this torus with $t^2 = (\varepsilon_p^{-2}\delta_{K/\mathbb{Q}})(\sigma_3)/\,\mathrm{mult}(g_0)$ and $t \equiv 1$, we get a lift g_1 of $\bar\rho_{\mathcal{G}}(\sigma_3)$ with the same property and with $\mathrm{mult}(g_1) = (\varepsilon_p^{-2}\delta_{K/\mathbb{Q}})(\sigma_3)$.

(3) The map $x \mapsto h(x)$, $\sigma_3 \mapsto g_1$ extends to a continuous homomorphism $\rho'_{\mathcal{G}}\colon G_{\mathbb{Q}_3} \to \mathcal{G}_3(\mathcal{O}')$, trivial on I_1, which lifts $\bar\rho_{\mathcal{G}}|_{G_{\mathbb{Q}_3}}$ and has multiplier $\varepsilon_p^{-2}\delta_{K/\mathbb{Q}}$. On $I_{\mathfrak{p}}$ its GL_3-component has order dividing 3 and scalar reduction, so it is the scalar κ, as in the proof of Lemma 7.6. So $\rho'_{\mathcal{G}}$ has finite image on inertia, and its monodromy operator is zero.

(4) Let τ_3 be the inertial type of $\rho'_{\mathcal{G}}$, and let X be the generic fiber of the ring of framed liftings of $\bar\rho_{\mathcal{G}}|_{G_{\mathbb{Q}_3}}$ to $\mathcal{G}_3$ of type τ_3 with multiplier $\varepsilon_p^{-2}\delta_{K/\mathbb{Q}}$. The locus of X where the monodromy operator vanishes is a union of irreducible components of X, and it is regular. This is the case $l \neq p$ of [13, Theorem 3.3.7 and the paragraph before it]; there p is the residue characteristic of the local field and l that of the coefficients, so here the local field is $\mathbb{Q}_3$ and l is our p. It applies to $\mathcal{G}_3$: [13, §§1.3.2, 3] allow any finite extension of their $\mathbb{Q}_p$ (here $\mathbb{Q}_3$) and any smooth affine group scheme whose geometric fibers are reductive, not necessarily connected, and whose center is smooth (the center of $\mathcal{G}_3$ is $\{(t \cdot 1_3, t^2)\} \cong \mathrm{GL}_1$), and the condition on the multiplier is the condition $\mathrm{ab} \circ \rho = \psi$ of [13, §3] for $\mathcal{G}_3$ [13, §5.1], where $\mathcal{G}_3$-valued representations at places of F^+ that are inert or ramified in F are treated explicitly.

That every point of X with vanishing monodromy lies on a component on which it vanishes identically is the statement of the paragraph before [13, Theorem 3.3.7]. We recall the argument. Let x be a closed point of this locus (it suffices to treat these), with residue field E_x, and let $L_3/\mathbb{Q}_3$ be a finite Galois extension with $\tau_3|_{I_{L_3}}$ trivial. The completed local ring at x of the locus $N = 0$ pro-represents the framed liftings of ρ_x with multiplier $\varepsilon_p^{-2}\delta_{K/\mathbb{Q}}$ to artinian local E_x-algebras B with residue field E_x that factor through $G_{\mathbb{Q}_3}/I_{L_3}$: for a lifting ρ_B of type τ_3 with Weil–Deligne representation (ϕ_B, N_B) we have $\rho_B(\sigma) = \phi_B(\sigma)\exp(t_p(\sigma)N_B)$ for $\sigma \in I_{\mathbb{Q}_3}$ (Section 2), and ϕ_B is trivial on I_{L_3}, since $\phi_B(I_{L_3})$ is a finite subgroup of the kernel of $\mathcal{G}_3(B) \to \mathcal{G}_3(E_x)$, which is torsion-free; so $N_B = 0$ if and only if ρ_B is trivial on I_{L_3}, and a lifting trivial on I_{L_3} has type τ_3, as representations of the finite group $I_{\mathbb{Q}_3}/I_{L_3}$ in characteristic 0 do not deform. As $I_{\mathbb{Q}_3}/I_{L_3}$ is finite and the quotient of $G_{\mathbb{Q}_3}/I_{L_3}$ by it is $\hat{\mathbb{Z}}$, these liftings are unobstructed, and their tangent space has dimension $\dim \mathcal{G}_3^{\mathrm{der}} = 9$, where $\mathcal{G}_3^{\mathrm{der}} = \mathrm{GL}_3 \times 1$. So the locus $N = 0$ is regular of dimension 9 at x; as x is a closed point of the generic fiber of a complete local noetherian ring, the irreducible component of the locus through x has dimension 9, so it is an irreducible component of X, which is equidimensional of dimension 9 [13, Theorem 3.3.2].

Let $\mathcal{C}'_3$ be the irreducible component of this locus through $\rho'_{\mathcal{G}}$ (it is unique, as the locus is regular): it is a polarized component at 3 (these are defined through [13, §3], [27, §1.5.19]), and the monodromy operator vanishes at all its points.

(5) Theorem 7.3 with the components $\mathcal{C}'_3$ and $\mathcal{C}_p$ gives a compatible system as in Section 7.6 whose p-adic member has $N = 0$ in (P3). □

If the unipotent part of $\bar\rho|_{I_{\mathfrak{p}}}$ is not trivial, then every lift of $\bar\rho|_{G_{K_{\mathfrak{p}}}}$ has $N \neq 0$ (Lemma 7.6), and no choice of component can force $N = 0$. At this point the argument leaves the prime 5.

Part III: the member at 3, and the proof of Theorem A

10. The member at 3

Part III works with the members of $\mathcal{R}$ at the primes above 3, which were of no use in Part II: their Hodge–Tate weights $\{0,1,2\}$ do not lie in the Fontaine–Laffaille range $[0,\ell-2]$ for $\ell=3$. For them, ordinarity at $\mathfrak{p}$ takes the place of Fontaine–Laffaille theory in bounding the ramification of the reductions, and weak admissibility forces it once the monodromy at $\mathfrak{p}$ is a single Jordan block. We prove Theorem 11.18 by steps (2)–(5) of Section 1.5: steps (2) and (3) in this section, steps (4) and (5) in Section 11.

Throughout this part, $p\geq 17$ is a prime with $p\equiv 1 \pmod 3$, ρ and $\bar\rho$ are the Frey representation of a solution of $x^3+y^3=z^p$ in coprime nonzero integers and its reduction (Definition 5.4), with the properties (F1)–(F6) of Section 7.1, and $\mathcal{R}=\{R_\lambda\}$ is a compatible system as in Section 7.6, with coefficient field M; the polarized component at 3 used to construct $\mathcal{R}$ may be any, not necessarily $\mathcal{C}_3$. As in Part II, representations over finite fields and over ℓ-adic fields are considered over an algebraic closure where convenient, and *irreducible* means absolutely irreducible. The completion $K_\mathfrak{p}=\mathbb{Q}_3(\sqrt{-3})$ has uniformizer $1-\omega$, residue field $\mathbb{F}_3$ and maximal unramified subfield $\mathbb{Q}_3$, and it contains the cube roots of unity. Let $G_{K_\mathfrak{p}}\subset G_K$ be a decomposition group at $\mathfrak{p}$ and $I_\mathfrak{p}$ its inertia subgroup. Upper ramification groups G^y ($y\geq -1$ real) are numbered as in Section 8 [101, Chapitre IV]. For a finite Galois extension of $K_\mathfrak{p}$, G^0 is its inertia group, and G^y for $y>0$ is contained in its wild inertia group.

10.1. **Regular monodromy at $\mathfrak{p}$.** For a square matrix A we write ${}^tA$ for its transpose and ${}^tA^{-1}$ for the inverse of the transpose. A unipotent matrix $U\in \mathrm{GL}_3$ is *regular* if $(U-1)^2\neq 0$, that is, if it has a single Jordan block. A nilpotent 3×3 matrix N is regular if $N^2\neq 0$.

Lemma 10.1. *Let k be a field, $A\in\mathrm{GL}_3(k)$, and $B=A\,{}^tA^{-1}$. If $B=\beta U$ with $\beta\in\bar k^\times$ and U unipotent, then $B=1$ or B is a regular unipotent matrix.*

Proof. As $\det B=1$, $\beta^3=1$. We have ${}^tB^{-1}={}^tA^{-1}A=A^{-1}BA$, so B is conjugate to ${}^tB^{-1}$, whose eigenvalues are the inverses of those of B. All eigenvalues of B equal β, so $\beta=\beta^{-1}$, and with $\beta^3=1$ this gives $\beta=1$: B is unipotent. From $B\,{}^tA=A$ we get $A-{}^tA=(B-1)\,{}^tA$, so $B-1$ and $A-{}^tA$ have the same rank. The matrix $A-{}^tA$ is alternating (antisymmetric with zero diagonal), so its rank is even, in every characteristic. A unipotent $B\neq 1$ with $(B-1)^2=0$ has $\mathrm{rank}(B-1)=1$; so this case does not occur. □

Proposition 10.2. *Let $\ell\notin\{2,3\}$ be a prime and $r\colon G_K\to\mathrm{GL}_3(\overline{\mathbb{F}}_\ell)$ a continuous irreducible representation. Suppose that $r^\mathsf{c}\cong r^\vee\otimes\nu|_{G_K}$ for a character ν of $G_\mathbb{Q}$, and that $r(\sigma)=\theta(\sigma)u(\sigma)$ for $\sigma\in I_\mathfrak{p}$, with θ a character of $I_\mathfrak{p}$ and $u(\sigma)$ unipotent. Then $u(I_\mathfrak{p})$ is trivial or generated by a regular unipotent matrix.*

Proof. The map $u=\theta^{-1}r|_{I_\mathfrak{p}}$ is a homomorphism with finite image, consisting of unipotent matrices in characteristic ℓ; so its image is an ℓ-group.

The isomorphism $r^\mathsf{c}\cong r^\vee\otimes\nu|_{G_K}$ gives $P\in\mathrm{GL}_3(\overline{\mathbb{F}}_\ell)$ with $r(\tilde{\mathsf{c}}h\tilde{\mathsf{c}}^{-1})=\nu(h)\,P\,{}^tr(h)^{-1}P^{-1}$ for $h\in G_K$. Let $\sigma\in G_\mathbb{Q}\smallsetminus G_K$, and write $\sigma=\tilde{\mathsf{c}}g$ with $g\in G_K$. Since ν takes values in an abelian group, $\nu(ghg^{-1})=\nu(h)$, and $r(\sigma h\sigma^{-1})=\nu(h)\,P_\sigma\,{}^tr(h)^{-1}P_\sigma^{-1}$ with $P_\sigma=P\,{}^tr(g)^{-1}$. Applying this to $\sigma h\sigma^{-1}\in G_K$ in place of h, and using $\nu(\sigma h\sigma^{-1})=\nu(h)$ again, we find

$$r(\sigma^2h\sigma^{-2})=(P_\sigma\,{}^tP_\sigma^{-1})\,r(h)\,(P_\sigma\,{}^tP_\sigma^{-1})^{-1}\qquad(h\in G_K).$$

Since also $r(\sigma^2h\sigma^{-2})=r(\sigma^2)r(h)r(\sigma^2)^{-1}$ and r is irreducible, Schur's lemma gives $r(\sigma^2)=\kappa_0\,P_\sigma\,{}^tP_\sigma^{-1}$ with $\kappa_0\in\overline{\mathbb{F}}_\ell^\times$.

Now choose σ as follows. Let $I_3 \subset G_{\mathbb{Q}_3}$ be the inertia group containing $I_{\mathfrak{p}}$, so that $I_{\mathfrak{p}} = I_3 \cap G_K$, and $P_3 \subset I_3$ its wild inertia group, the unique pro-3 Sylow subgroup of I_3; it lies in $I_{\mathfrak{p}}$, which has index 2 in I_3. The quotient I_3/P_3 is procyclic, and the surjection $I_3 \to \mathrm{Gal}(K_{\mathfrak{p}}/\mathbb{Q}_3)$ factors through it, because $K_{\mathfrak{p}}/\mathbb{Q}_3$ is tamely ramified. So every lift $\sigma \in I_3$ of a topological generator of I_3/P_3 lies outside G_K, and $\sigma^2 \in I_{\mathfrak{p}}$ maps to a topological generator of the tame quotient $I_{\mathfrak{p}}/P_3$. As $\ell \neq 3$, u is trivial on P_3, and $u(I_{\mathfrak{p}})$ is generated by $u(\sigma^2)$. Now

$$P_\sigma\, {}^t P_\sigma^{-1} = \kappa_0^{-1} r(\sigma^2) = \kappa_0^{-1}\theta(\sigma^2)\, u(\sigma^2)$$

is a scalar times a unipotent matrix. By Lemma 10.1 (with $A = P_\sigma$) it is 1 or a regular unipotent matrix. A scalar times a unipotent matrix determines the scalar, its only eigenvalue; so $\kappa_0^{-1}\theta(\sigma^2) = 1$, and $u(\sigma^2)$ is 1 or regular. □

Corollary 10.3. *By (7.1), $\bar\rho(\sigma) = \bar\kappa(\sigma)\bar u(\sigma)$ for $\sigma \in I_{\mathfrak{p}}$, with $\bar u(\sigma)$ unipotent. The group $\bar u(I_{\mathfrak{p}})$ is generated by a regular unipotent matrix. For every compatible system as in Section 7.6, the matrix N of* (P3) *is regular.*

Proof. Apply Proposition 10.2 with $\ell = p \geq 17$, $r = \bar\rho$ (irreducible by (F6)), $\nu = \bar\varepsilon_p^{-2}$ (by (F4), $\bar\rho^{\mathsf{c}} \cong \bar\rho^\vee \otimes \bar\varepsilon_p^{-2}$; see Lemma 7.1) and $\theta = \bar\kappa|_{I_{\mathfrak{p}}}$. By Proposition 9.5, $\bar\rho(I_{\mathfrak{p}})$ is not contained in the scalar matrices, so $\bar u(I_{\mathfrak{p}}) \neq 1$, and it is generated by a regular unipotent matrix.

Let $\mathcal{R}$ be as in Section 7.6. By (P1) and (F6), the reduction of every G_K-stable lattice in R_p is $\bar\rho$, and the lattice is unique up to homothety. In a basis of such a lattice whose reduction is $\bar\rho$, the matrix $U(\sigma) = \kappa(\sigma)^{-1}R_p(\sigma)$ is integral for $\sigma \in I_{\mathfrak{p}}$ (as $\kappa(\sigma) \in \mu_3$ is a unit), it equals $\exp(t_p(\sigma)N')$ by (P3), with N' conjugate to N, and its reduction is $\bar\kappa(\sigma)^{-1}\bar\rho(\sigma) = \bar u(\sigma)$. If $N^2 = 0$, then $U(\sigma) - 1 = t_p(\sigma)N'$ and $(U(\sigma) - 1)^2 = 0$, hence $(\bar u(\sigma) - 1)^2 = 0$ for all $\sigma \in I_{\mathfrak{p}}$, which the first part excludes. So $N^2 \neq 0$. □

10.2. **The member at a prime above 3.** From now on in this part, λ is a prime of M above 3 and $R = R_\lambda \colon G_K \to \mathrm{GL}_3(\overline{M}_\lambda)$. We use the notation of Section 8.1 with 3 in place of 5: $E \subset \overline{M}_\lambda$ is a finite extension of $\mathbb{Q}_3$ over which R is defined, with ring of integers $\mathcal{O}_E$, maximal ideal $\mathfrak{m}_E$ and residue field $\mathbb{F}_E$; a *stable lattice* is a G_K-stable $\mathcal{O}_E$-lattice Λ in the space of R; its reduction is $\overline{R}_\Lambda = \Lambda/\mathfrak{m}_E\Lambda$; and the semisimplification $\overline{R}^{\mathrm{ss}}$ of $\overline{R}_\Lambda$ does not depend on Λ. We enlarge E when needed, and in particular assume that E contains the images of the two embeddings of $K_{\mathfrak{p}}$ in $\overline{M}_\lambda$.

Proposition 10.4. *The representation R is unramified at every prime of K other than $\mathfrak{p}$.*

Proof. Let $\mathfrak{q} \neq \mathfrak{p}$ be a prime of K. Then $\mathfrak{q} \nmid 3$. By (P1) and (P2), R_p is unramified at $\mathfrak{q}$ if $\mathfrak{q} \nmid p$ and crystalline at $\mathfrak{q}$ if $\mathfrak{q} \mid p$. By Lemma 7.7 (a), R is unramified at $\mathfrak{q}$. □

Proposition 10.5. *The restriction $R|_{G_{K_{\mathfrak{p}}}}$ is de Rham, with Hodge–Tate weights $\{0,1,2\}$ for both embeddings of $K_{\mathfrak{p}}$ in $\overline{M}_\lambda$, and $\mathrm{WD}(R|_{G_{K_{\mathfrak{p}}}})^{F\text{-ss}}$ corresponds to $\mathrm{WD}(R_p|_{G_{K_{\mathfrak{p}}}})^{F\text{-ss}}$ under an isomorphism of their coefficient fields that is the identity on M. So $I_{\mathfrak{p}}$ acts on $\mathrm{WD}(R|_{G_{K_{\mathfrak{p}}}})$ through a character with values in $\mu_3(\overline{M}_\lambda)$, which is $\kappa|_{I_{\mathfrak{p}}}$ after an identification of the groups μ_3 of the two coefficient fields (as in* (M3)*), and the monodromy operator of $\mathrm{WD}(R|_{G_{K_{\mathfrak{p}}}})$ is regular.*

Proof. The first assertion is part of the definition of a compatible system (Section 7.4), with (P2). By Lemma 7.7 with $\mathfrak{q} = \mathfrak{p}$, $\mathrm{WD}(R|_{G_{K_{\mathfrak{p}}}})^{F\text{-ss}}$ corresponds to $\mathrm{WD}(R_p|_{G_{K_{\mathfrak{p}}}})^{F\text{-ss}}$ (compose with the inverse of an isomorphism $j' \colon \overline{\mathbb{Q}}_p \to \mathbb{C}$ restricting to $\imath_{\mathfrak{p}}$ on M). Here λ lies above 3, the residue characteristic of $\mathfrak{p}$, and in this case Lemma 7.7 gives the monodromy operator

of $\mathrm{WD}(R|_{G_{K_\mathfrak{p}}})$ as well as its semisimplification (the Shin-regular case of [9, Theorem 1.1]; see the proof of Lemma 7.7), and the regularity of the monodromy operator, shown next, depends on this. By (P3), $I_\mathfrak{p}$ acts on $\mathrm{WD}(R_p|_{G_{K_\mathfrak{p}}})$ through the scalar character κ, and its monodromy operator is conjugate to N, which is regular by Corollary 10.3; by Lemma 7.7 (b), the same holds for $\mathrm{WD}(R|_{G_{K_\mathfrak{p}}})$, after identifying the two groups μ_3 as in the statement. □

Let $\kappa_\lambda\colon G_K \to \mu_3(\overline{M}_\lambda)$ be the character obtained from κ through an identification as in Proposition 10.5, so that $I_\mathfrak{p}$ acts on $\mathrm{WD}(R|_{G_{K_\mathfrak{p}}})$ through $\kappa_\lambda|_{I_\mathfrak{p}}$, the analogue for $\lambda \mid 3$ of the character κ_λ of (M3); in the unramified case $\kappa|_{I_\mathfrak{p}} = 1$ and either identification may be used. Twisting by κ_λ does not change the subspaces stable under a subgroup of G_K, and $\kappa_\lambda \equiv 1 \pmod{\mathfrak{m}_E}$, because $\mu_3 \subset 1 + \mathfrak{m}_E$.

Proposition 10.6. *Let $V = (R \otimes \kappa_\lambda^{-1})|_{G_{K_\mathfrak{p}}}$. Then V is semistable, and it has $G_{K_\mathfrak{p}}$-stable subspaces $0 \subset V_1 \subset V_2 \subset V$ of dimensions 1 and 2 whose graded pieces V_1, V_2/V_1, V/V_2 are the characters ψ, $\psi\varepsilon_3^{-1}$, $\psi\varepsilon_3^{-2}$, for one unramified character $\psi\colon G_{K_\mathfrak{p}} \to E^\times$. In particular $R|_{G_{K_\mathfrak{p}}}$ stabilizes the line V_1. For every stable lattice Λ there is a basis of Λ in which*

$$\overline{R}_\Lambda(g) = \bar{\psi}(g)\begin{pmatrix} 1 & a(g) & c(g) \\ 0 & 1 & b(g) \\ 0 & 0 & 1 \end{pmatrix} \qquad (g \in G_{K_\mathfrak{p}}),$$

where $\bar{\psi}$ is the reduction of ψ, $a, b \in \mathrm{Hom}(G_{K_\mathfrak{p}}, \mathbb{F}_E)$, and $c\colon G_{K_\mathfrak{p}} \to \mathbb{F}_E$ is continuous with $c(gh) = c(g) + c(h) + a(g)b(h)$.

Proof. By Proposition 10.5, $R|_{G_{K_\mathfrak{p}}}$ is de Rham, hence potentially semistable [17], and so is V; and $I_\mathfrak{p}$ acts trivially on $\mathrm{WD}(V) = \mathrm{WD}(R|_{G_{K_\mathfrak{p}}}) \otimes \mathrm{WD}(\kappa_\lambda^{-1}|_{G_{K_\mathfrak{p}}})$ (WD is compatible with tensor products), by the choice of κ_λ. So V is semistable [56, 55]. Let $D = D_{\mathrm{st}}(V)$ be its filtered (φ, N)-module (covariant), with coefficients in E. The maximal unramified subfield of $K_\mathfrak{p}$ is $\mathbb{Q}_3$, so D is a free E-module of rank 3 with E-linear φ and N, and $N\varphi = 3\varphi N$; by Proposition 10.5, N is regular. The N-stable subspaces of D are $0 \subset \ker N \subset \ker N^2 \subset D$, and they are φ-stable. If φ acts on $D/\ker N^2$ by $\alpha \in E^\times$, then, as N induces isomorphisms $D/\ker N^2 \to \ker N^2/\ker N \to \ker N$ and $\varphi N = 3^{-1}N\varphi$, it acts on $\ker N^2/\ker N$ and on $\ker N$ by $\alpha/3$ and $\alpha/9$. The Hodge filtration lives on $D \otimes_{\mathbb{Q}_3} K_\mathfrak{p} = \bigoplus_\tau D_\tau$, the sum over the two embeddings τ of $K_\mathfrak{p}$ in E, and its jumps on each D_τ are $0, 1, 2$. For a (φ, N)-stable subspace D' put $t_N(D') = v_3(\det(\varphi|D'))$ and $t_H(D') = \frac{1}{2}\sum_\tau \sum_i i \dim \mathrm{gr}^i(D'_\tau)$, for the induced filtrations; these are the usual invariants of D' divided by $[E : \mathbb{Q}_3]$ (for ε_3 both are -1). Weak admissibility says $t_H(D') \le t_N(D')$, with equality for $D' = D$. For D: $t_H(D) = \frac{1}{2}(3+3) = 3 = t_N(D) = 3v_3(\alpha) - 3$, so $v_3(\alpha) = 2$, and $\ker N$, $\ker N^2/\ker N$, $D/\ker N^2$ have slopes $0, 1, 2$. For $\ker N$: $t_N = 0$ and $t_H \ge 0$, so $t_H = 0$ by weak admissibility, that is, the jump of the line $(\ker N)_\tau$ is 0 for both τ. For $\ker N^2$: $t_N = 0 + 1 = 1$, while the two jumps of each plane $(\ker N^2)_\tau$ are distinct elements of $\{0, 1, 2\}$, so $t_H \ge \frac{1}{2}(1+1) = 1$; so $t_H = 1$, and the jumps are $\{0, 1\}$ for both τ. Hence $\ker N$ and $\ker N^2$, with the induced structures, have $t_H = t_N$; they are weakly admissible, hence admissible [33], and they are D_{st} of $G_{K_\mathfrak{p}}$-stable subspaces $V_1 \subset V_2$ of V of dimensions 1 and 2. The graded pieces $\ker N$, $\ker N^2/\ker N$, $D/\ker N^2$ have $N = 0$, jumps $h = 0, 1, 2$ at both embeddings, and φ-eigenvalues $\alpha/9$, $\alpha/3$, α; so they are D_{st} of crystalline characters of Hodge–Tate weights (h, h), that is, of characters $\psi_h\varepsilon_3^{-h}$ with ψ_h unramified (a crystalline character with all Hodge–Tate weights 0 is unramified). The eigenvalue of φ on $D_{\mathrm{cris}}(\psi_h\varepsilon_3^{-h})$ is 3^h times that

on $D_{\mathrm{cris}}(\psi_h)$, so the three unramified characters ψ_h have the same eigenvalue $\alpha/9$, and they are equal; call them ψ.

Let Λ be a stable lattice. The subspaces $V_1 \subset V_2$ are $G_{K_\mathfrak{p}}$-stable subspaces of the space of R, so $\Lambda \cap V_1 \subset \Lambda \cap V_2 \subset \Lambda$ are $G_{K_\mathfrak{p}}$-stable direct summands, and the graded pieces are lattices in the characters $\psi\varepsilon_3^{-h}\kappa_\lambda$, $h = 0, 1, 2$. The reductions of these characters are all $\bar\psi$: $\bar\varepsilon_3$ is trivial on $G_{K_\mathfrak{p}}$ because $K_\mathfrak{p}$ contains the cube roots of unity, and $\bar\kappa_\lambda = 1$. So in a basis of Λ adapted to this flag, $\bar\psi^{-1}\overline{R}_\Lambda|_{G_{K_\mathfrak{p}}}$ is upper unitriangular. Its entries a, b next to the diagonal are then homomorphisms, and its corner entry c satisfies $c(gh) = c(g) + c(h) + a(g)b(h)$. □

Proposition 10.7. *The representation R is irreducible.*

Proof. R is semisimple, as is every member of a compatible system (Section 7.4). If $R = R_1 \oplus R_2$ with $R_1, R_2 \neq 0$, then $\mathrm{WD}(R|_{G_{K_\mathfrak{p}}}) = \mathrm{WD}(R_1|_{G_{K_\mathfrak{p}}}) \oplus \mathrm{WD}(R_2|_{G_{K_\mathfrak{p}}})$, and the monodromy operator is the sum of nilpotent operators on spaces of dimension at most 2, so its square is zero. This contradicts Proposition 10.5. □

11. The reductions of the member at 3, and the proof of Theorem A

It remains to show that every reduction of the member R at a prime above 3 has trivial semisimplification (Corollary 11.15). Then, by Corollary 11.17, R has the same image as its inertia group at $\mathfrak{p}$, which stabilizes the line V_1 of Proposition 10.6; so R is reducible, against Proposition 10.7. This proves Theorem 11.18, which completes the proof of Theorem A. The notation is that of Section 10.2. For a stable lattice Λ let L_Λ be the field cut out by $\overline{R}_\Lambda$. By Proposition 10.4, L_Λ/K is a finite Galois extension unramified at every place other than $\mathfrak{p}$, including the infinite places, as K has no real place. On $G_{K_\mathfrak{p}}$, $\overline{R}_\Lambda$ has the shape of Proposition 10.6.

11.1. Characters.

Proposition 11.1. *Every continuous character $\theta\colon G_K \to \overline{\mathbb{F}}_3^\times$ unramified outside $\mathfrak{p}$ is trivial. In particular every one-dimensional constituent of $\overline{R}^{\mathrm{ss}}$ is trivial.*

Proof. The character θ has finite order prime to 3, since $\overline{\mathbb{F}}_3^\times$ has no element of order 3. If $\mathfrak{p}^n$ is its conductor, it factors through the ray class group $\mathrm{Cl}_{\mathfrak{p}^n}(K)$, which is $(\mathcal{O}/\mathfrak{p}^n)^\times/\mu_6$ because K has class number one and no real place. The group $(\mathcal{O}/\mathfrak{p}^n)^\times$ has order $2 \cdot 3^{n-1}$, and μ_6 injects into it for $n \geq 2$ (Section 2); so $\mathrm{Cl}_{\mathfrak{p}^n}(K)$ is a 3-group (of order 1 for $n \leq 2$ and 3^{n-2} for $n \geq 2$), and $\theta = 1$. The constituents of $\overline{R}^{\mathrm{ss}}$ are unramified outside $\mathfrak{p}$ by Proposition 10.4. □

11.2. Cubic characters of $K_\mathfrak{p}$.

As $\omega \in K_\mathfrak{p}$, Kummer theory identifies $\mathrm{Hom}(G_{K_\mathfrak{p}}, \mu_3)$ with $K_\mathfrak{p}^\times/K_\mathfrak{p}^{\times 3}$. We identify μ_3 with $\mathbb{F}_3$ by $\omega \mapsto 1$, and put

$$\mathcal{H} = \mathrm{Hom}(G_{K_\mathfrak{p}}, \mathbb{F}_3) \cong K_\mathfrak{p}^\times/K_\mathfrak{p}^{\times 3}.$$

Let $U^{(j)} = 1 + \mathfrak{p}^j$ be the groups of principal units of $K_\mathfrak{p}$, $\mathcal{U} \subset \mathcal{H}$ the image of $U^{(2)}$, and $e_\pi, e_2, e_1, e_0 \in \mathcal{H}$ the classes of

$$1 - \omega, \qquad \omega, \qquad 4, \qquad 1 + (1 - \omega)^3.$$

We fix an isomorphism $H^2(G_{K_\mathfrak{p}}, \mathbb{F}_3) \cong \mathbb{F}_3$ (local class field theory). The cup product $\mathcal{H} \times \mathcal{H} \to H^2(G_{K_\mathfrak{p}}, \mathbb{F}_3) = \mathbb{F}_3$ is alternating. We call a plane $W \subset \mathcal{H}$ *isotropic* if the cup product vanishes on $W \times W$. Under these identifications the cup product of the classes of $x, y \in K_\mathfrak{p}^\times$ is, up to a sign, the cubic Hilbert symbol $(x, y)_\mathfrak{p}$ [101, Chapitre XIV, §§1–2].

Lemma 11.2.

(a) *$\mathcal{H}$ has dimension 4 over $\mathbb{F}_3$, and (e_π, e_2, e_1, e_0) is a basis; $\mathcal{U} = \mathbb{F}_3 e_1 \oplus \mathbb{F}_3 e_0$.*

(b) *Let $\alpha \in \mathcal{H}$, $\alpha \neq 0$. The cubic extension of $K_\mathfrak{p}$ cut out by α has upper ramification break 3 if $\alpha \notin \langle e_2, e_1, e_0\rangle$, 2 if $\alpha \in \langle e_2, e_1, e_0\rangle \smallsetminus \mathcal{U}$, and 1 if $\alpha \in \mathcal{U} \smallsetminus \mathbb{F}_3 e_0$, and it is unramified if $\alpha \in \mathbb{F}_3 e_0$. In particular every $\alpha \in \mathcal{H}$ vanishes on $G^y_{K_\mathfrak{p}}$ for $y > 3$.*

(c) *In the basis (e_π, e_2, e_1, e_0) the cup product has, up to a sign, the matrix*

$$\begin{pmatrix} 0 & 0 & 2 & 1 \\ 0 & 0 & 1 & 0 \\ 1 & 2 & 0 & 0 \\ 2 & 0 & 0 & 0 \end{pmatrix}.$$

Exactly 40 of the 130 planes of $\mathcal{H}$ are isotropic, and 13 of these meet $\mathcal{U}$ nontrivially.

Proof. (a) As $\mu_3 \subset K_\mathfrak{p}$ and $[K_\mathfrak{p} : \mathbb{Q}_3] = 2$, $K_\mathfrak{p}^\times / K_\mathfrak{p}^{\times 3}$ has order 3^{2+2}. Write $\pi = 1 - \omega$, so that $3 = -\omega^2\pi^2$. For $j \geq 2$ and $v_\mathfrak{p}(x) = j$ we have $(1+x)^3 \equiv 1 + 3x \pmod{\mathfrak{p}^{j+3}}$, so cubing induces isomorphisms $U^{(j)}/U^{(j+1)} \to U^{(j+2)}/U^{(j+3)}$, and $U^{(4)} = (U^{(2)})^3$ by completeness. For a unit z, $(1+\pi z)^3 = 1 + \pi^3(z^3 - \omega^2 z) + 3\pi^2 z^2 \in U^{(4)}$, as $z^3 \equiv z$ and $\omega \equiv 1$ modulo $\mathfrak{p}$. So the cubes of units are $\pm U^{(4)}$, and $K_\mathfrak{p}^\times / K_\mathfrak{p}^{\times 3}$ is the product of the group generated by the class of π, of order 3, and of $\mathcal{O}_\mathfrak{p}^\times / \{\pm 1\} U^{(4)} = (\mathcal{O}/9)^\times / \{\pm 1\}$, of order 27. The latter group is generated by the classes of ω, 4 and $1 + \pi^3 = -2(1+3\omega)$, which lie in $U^{(1)}$, $U^{(2)}$, $U^{(3)}$ with $v_\mathfrak{p}(\omega - 1) = 1$, $v_\mathfrak{p}(4-1) = 2$, $v_\mathfrak{p}(\pi^3) = 3$; and $\mathcal{U}$ is the image of $U^{(2)}/U^{(4)}$, of order 9, generated by 4 and $1 + \pi^3$.

(b) Let x represent α; replacing α by $-\alpha$ does not change the extension. We use the valuation $v_\mathfrak{p}$ of $K_\mathfrak{p}$, extended to an algebraic closure. For a cyclic extension of degree 3 of $K_\mathfrak{p}$, totally ramified with break t (the same in both numberings), the different has $v_\mathfrak{p}$-valuation $2(t+1)/3$; and if the ring of integers is generated by a root Π of a polynomial f, the different is generated by $f'(\Pi)$ [101, Chapitre III, §6, and Chapitre IV, §1]. If $\alpha \notin \langle e_2, e_1, e_0\rangle$ we may take $x = \pi z$ with z a unit; $X^3 - x$ is an Eisenstein polynomial, and $v_\mathfrak{p}(3X^2) = 2 + \frac{2}{3}$ at a root, so $t = 3$. If $\alpha \in \langle e_2, e_1, e_0\rangle \smallsetminus \mathcal{U}$ we may take $x = 1 + y$ with $v_\mathfrak{p}(y) = 1$; then $T = x^{1/3} - 1$ is a root of the Eisenstein polynomial $T^3 + 3T^2 + 3T - y$, whose derivative $3(T+1)^2$ has valuation 2, so $t = 2$. If $\alpha \in \mathcal{U} \smallsetminus \mathbb{F}_3 e_0$ we may take $x = 1 + y$ with $v_\mathfrak{p}(y) = 2$; then $\Pi = \pi/T$ is a root of the Eisenstein polynomial $\Pi^3 - (3\pi/y)\Pi^2 - (3\pi^2/y)\Pi - \pi^3/y$, whose derivative at Π has valuation $\min(2 + \frac{2}{3},\, 1 + \frac{1}{3},\, 2) = \frac{4}{3}$, attained once, so $t = 1$. If $\alpha \in \mathbb{F}_3 e_0$ we may take $x = 1 + \pi^3 z$ with z a unit; then $S = T/\pi$ satisfies $S^3 + (3/\pi)S^2 + (3/\pi^2)S - z = 0$, whose reduction $S^3 - S - \bar{z}$ is separable ($3/\pi^2 = -\omega^2 \equiv -1$), so the extension is unramified. Finally, an element of $\mathcal{H}$ vanishes on $G^y_{K_\mathfrak{p}}$ for every y larger than the break of the extension it cuts out, because the upper numbering passes to quotients.

(c) Besides $\mathfrak{p}$, the only primes that divide the representatives $1 - \omega$, ω, 4 and $1 + \pi^3 = -2(1+3\omega)$ are (2) and $\mathfrak{l} = (2 - \omega) = (1 + 3\omega)$, with residue fields $\mathbb{F}_4$ and $\mathbb{F}_7$, and K has no real place. So, by the product formula, $(x, y)_\mathfrak{p}$ is the inverse of the product of the tame symbols $\left((-1)^{v_\mathfrak{q}(x)v_\mathfrak{q}(y)} x^{v_\mathfrak{q}(y)} y^{-v_\mathfrak{q}(x)} \bmod \mathfrak{q}\right)^{(\mathrm{N}\,\mathfrak{q}-1)/3}$ at $\mathfrak{q} = (2)$ and $\mathfrak{q} = \mathfrak{l}$. This gives $(\pi, \omega)_\mathfrak{p} = (\omega, 1+\pi^3)_\mathfrak{p} = (4, 1+\pi^3)_\mathfrak{p} = 1$, $(\pi, 4)_\mathfrak{p} = \omega^2$ and $(\pi, 1+\pi^3)_\mathfrak{p} = (\omega, 4)_\mathfrak{p} = \omega$; with $(x, x)_\mathfrak{p} = 1$ and antisymmetry this is the matrix stated. Its Pfaffian is 1, so the form is nondegenerate, and $\mathcal{H}$ has $(3+1)(3^2+1) = 40$ isotropic planes among its $(3^4-1)(3^3-1)/((3^2-1)(3-1)) = 130$ planes (a symplectic space of dimension 4 over $\mathbb{F}_q$ has $(q+1)(q^2+1)$ Lagrangian planes). The plane $\mathcal{U}$ is isotropic, and the isotropic planes

meeting it only in 0 are the graphs of the $3^3 = 27$ self-adjoint maps from a fixed isotropic complement of $\mathcal{U}$ to $\mathcal{U}$; so 13 meet $\mathcal{U}$ nontrivially. □

11.3. **Heisenberg extensions of $K_\mathfrak{p}$.** The reductions in Proposition 10.6, divided by their unramified character, cut out, on the decomposition group at $\mathfrak{p}$, extensions of $K_\mathfrak{p}$ whose group is a subgroup of the group of upper unitriangular matrices over the residue field. The aim of this subsection is to prove Proposition 11.10, which bounds the upper ramification groups of these extensions; Proposition 11.11 turns the bound into one for root discriminants. Over $\mathbb{F}_3$ the unitriangular group is the Heisenberg group of order 27. A *Heisenberg extension* of $K_\mathfrak{p}$ is a finite Galois extension $L/K_\mathfrak{p}$ whose group is isomorphic to it, and its *plane* is the plane of $\mathcal{H}$ formed by the homomorphisms $G_{K_\mathfrak{p}} \to \mathbb{F}_3$ that factor through $\mathrm{Gal}(L/K_\mathfrak{p})$.

Throughout, F is a finite extension of $K_\mathfrak{p}$ in a fixed algebraic closure, v_F its normalized valuation ($v_F(F^\times) = \mathbb{Z}$), $\mathcal{O}_F$ its ring of integers, ϖ_F a uniformizer, $e_F = v_F(3)$, and $U_F^{(j)} = 1 + \varpi_F^j \mathcal{O}_F$ for $j \geq 1$. As $\omega \in F$ and $(1-\omega)^2 = -3\omega$, e_F is even and $v_F(\omega - 1) = e_F/2$. For a continuous homomorphism χ from G_F to an abelian group and a real number T, we say that χ *has break at most* T if $\chi(G_F^y) = 0$ for every $y \geq -1$ with $y > T$; these χ form a group. For $u \in F^\times$ we say that u has break at most T if the character $g \mapsto g(u^{1/3})/u^{1/3}$ of G_F does; this depends only on the class of u in $F^\times/F^{\times 3}$. Unramified characters have break at most T for every $T \geq -1$. If F'/F is cyclic of degree 3 and totally ramified, then $\mathrm{Gal}(F'/F)^y = \mathrm{Gal}(F'/F)$ for $y \leq t$ and $\mathrm{Gal}(F'/F)^y = 1$ for $y > t$, for one integer $t \geq 1$, the *break* of F'/F (the same in both numberings). When $F(u^{1/3})/F$ is cyclic of degree 3 and totally ramified, its break is also called the *break* of u. For a generator s of $\mathrm{Gal}(F'/F)$ and every uniformizer Π of F' we have $v_{F'}(s(a) - a) \geq t + 1$ for all $a \in \mathcal{O}_{F'}$, with equality for $a = \Pi$ [101, Chapitre IV, §1, Lemme 1] (as $\mathcal{O}_{F'} = \mathcal{O}_F[\Pi]$, [101, Chapitre I, §6, Propositions 17 and 18]). Herbrand's functions are

$$\varphi_{F'/F}(u) = \begin{cases} u, & u \leq t, \\ t + \frac{u-t}{3}, & u \geq t, \end{cases} \qquad \psi_{F'/F}(y) = \begin{cases} y, & y \leq t, \\ t + 3(y-t), & y \geq t. \end{cases}$$

If F'/F is unramified, $\varphi_{F'/F} = \psi_{F'/F}$ is the identity. We use three facts from [101, Chapitre IV].

(R1) The upper numbering passes to quotients (§3, Proposition 14).

(R2) If N/F is finite Galois with group G, $F \subset F' \subset N$ with F'/F Galois, and $H = \mathrm{Gal}(N/F')$, then $G^y \cap H = H^{\psi_{F'/F}(y)}$ for $y \geq -1$. (By §1, Proposition 2, $H_u = G_u \cap H$; and $\psi_{N/F} = \psi_{N/F'} \circ \psi_{F'/F}$ by §3.)

(R3) If a character χ of G_F has break at most T, then $\chi|_{G_{F'}}$ has break at most $\psi_{F'/F}(T)$, for F'/F finite Galois. (Apply (R2) to the compositum N of F' and the field cut out by χ, and (R1) twice.)

Lemma 11.3. *Let $u \in F^\times$ and $e = e_F$.*

(a) *If $3 \nmid v_F(u)$, then $F(u^{1/3})/F$ is cyclic of degree 3, totally ramified, with break $3e/2$.*

(b) *If $u \in U_F^{(r)}$ with $r \geq 1$, then u has break at most $3e/2 - r$, and at most $3e/2 - r - 1$ if moreover $3 \mid r$ and $r < 3e/2$.*

(c) *If $u \in U_F^{(r)} \smallsetminus U_F^{(r+1)}$ with $3 \nmid r$ and $1 \leq r < 3e/2$, then $F(u^{1/3})/F$ is cyclic of degree 3, totally ramified, with break exactly $3e/2 - r$.*

For $F = K_{\mathfrak{p}}$ ($e = 2$) this is the computation in the proof of Lemma 11.2 (b). We use it for F cubic and totally ramified over $K_{\mathfrak{p}}$ ($e = 6$, breaks $9 - r$) and for F the unramified cubic extension of $K_{\mathfrak{p}}$ ($e = 2$).

Proof. (a) Let ϑ be a cube root of u and $F' = F(\vartheta)$. As $v_F(\vartheta) = v_F(u)/3 \notin \mathbb{Z}$, F'/F is totally ramified of degree 3. Choose integers a, b with $a\, v_F(u) + 3b = 1$; then $\Pi = \vartheta^a \varpi_F^b$ is a uniformizer of F'. A generator s of $\mathrm{Gal}(F'/F)$ maps ϑ to $\omega^{\pm 1}\vartheta$, so $s(\Pi)/\Pi = \omega^{\pm a}$ with $3 \nmid a$, and $v_{F'}(s(\Pi) - \Pi) = 1 + 3v_F(\omega^{\pm a} - 1) = 1 + 3e/2$. The break is $3e/2$.

(c) Put $z = u - 1$, so $v_F(z) = r$, and let T be a root of $(1 + T)^3 = u$, that is, $T^3 + 3T^2 + 3T = z$. If $v_F(T) \geq e/2$, all three terms on the left have valuation at least $3e/2 > r$; so $\tau = v_F(T) < e/2$, the term T^3 has the smallest valuation, and $3\tau = r$. As $3 \nmid r$, $F' = F(T) = F(u^{1/3})$ is totally ramified of degree 3. Choose integers a, b with $ar + 3b = 1$; then $\Pi = T^a \varpi_F^b$ is a uniformizer of F'. For the generator s with $s(1 + T) = \omega(1 + T)$ we have $s(T) - T = (\omega - 1)(1 + T)$, so $s(T)/T = 1 + \eta$ with $\eta = (\omega - 1)(1 + T)/T$ and $v_F(\eta) = e/2 - r/3 > 0$. Then $s(\Pi)/\Pi = (1 + \eta)^a$, and as $3 \nmid a$, $v_F\big((1 + \eta)^a - 1\big) = v_F(\eta)$. So $v_{F'}(s(\Pi) - \Pi) = 1 + 3(e/2 - r/3) = 1 + 3e/2 - r$, and the break is $3e/2 - r$.

(b) We argue by descending induction on r. Let $\pi_0 = \omega - 1$, so $v_F(\pi_0) = e/2$ and $3/\pi_0^2 = -\omega^2$. If $r \geq 3e/2$, put $T = \pi_0 S$: the equation $(1 + T)^3 = u$ becomes $S^3 + (3/\pi_0)S^2 + (3/\pi_0^2)S = (u - 1)/\pi_0^3$, with $v_F(3/\pi_0) = e/2 > 0$ and $(u - 1)/\pi_0^3$ integral, so its reduction is $S^3 - S - \bar{c}$ for some $\bar{c}$ in the residue field, which is separable. If $r > 3e/2$ then $\bar{c} = 0$, the root $S = 0$ of the reduction is simple, and by Hensel's lemma u is a cube; if $r = 3e/2$, $F(u^{1/3})/F$ is unramified. In both cases the claim holds. Let $r < 3e/2$. If $3 \mid r$, write $u = 1 + \varpi_F^r \varepsilon$ with $\varepsilon \in \mathcal{O}_F$ and choose $a \in \mathcal{O}_F$ with $a^3 \equiv \varepsilon \pmod{\varpi_F}$ (the residue field is perfect); as $v_F(3a\varpi_F^{r/3}) \geq e + r/3 > r$, $u(1 + a\varpi_F^{r/3})^{-3} \in U_F^{(r+1)}$, and u has the class of an element of $U_F^{(r+1)}$, of break at most $3e/2 - r - 1$ by induction (this is the second assertion). If $3 \nmid r$, either $u \in U_F^{(r+1)}$ and we conclude by induction, or (c) applies. □

Lemma 11.4. *Let $K_1/K_{\mathfrak{p}}$ be cyclic of degree 3 and totally ramified, with break t, let σ generate $\mathrm{Gal}(K_1/K_{\mathfrak{p}})$, and let θ_1 be a uniformizer of K_1. Write $U^{(j)} = U_{K_1}^{(j)}$.*

(a) *$\sigma(u)/u \in U^{(t+1)}$ for every unit u of K_1, and $\sigma(\theta_1)/\theta_1 \in U^{(t)} \smallsetminus U^{(t+1)}$. Hence $\sigma(w)/w \in U^{(t)}$ for every $w \in K_1^\times$.*

(b) *$\sigma(u)/u \in U^{(m+t)}$ for every $u \in U^{(m)}$, $m \geq 1$.*

Proof. We have $v_{K_1}(\sigma(a) - a) \geq t + 1$ for all $a \in \mathcal{O}_{K_1}$, with equality for $a = \theta_1$. (a) follows from $\sigma(u)/u - 1 = (\sigma(u) - u)/u$ and $\sigma(\theta_1)/\theta_1 - 1 = (\sigma(\theta_1) - \theta_1)/\theta_1$. (b) Write $u = 1 + \theta_1^m a$ with $a \in \mathcal{O}_{K_1}$. Then $\sigma(u) - u = \theta_1^m((\sigma(\theta_1)/\theta_1)^m \sigma(a) - a)$, and by (a) $(\sigma(\theta_1)/\theta_1)^m \sigma(a) \equiv \sigma(a) \equiv a \pmod{\theta_1^t}$; so $v_{K_1}(\sigma(u) - u) \geq m + t$, and $\sigma(u)/u - 1 = (\sigma(u) - u)/u$. □

The next lemma, on the Kummer generators of a Heisenberg extension over a cubic subfield, is in substance due to Massy [83] and Sharifi [104, Theorem 2.5]: every Heisenberg extension with a given plane is obtained by adjoining a cube root of an explicit element of the form below, unique up to multiplication by an element of the base field and a cube in the compositum of the two cubic extensions. Our short proof is by a different argument. That this construction does give Heisenberg extensions is also in [86, §2.2, Lemma 2.1 and Proposition 2.2].

Lemma 11.5. *Let $L/K_{\mathfrak{p}}$ be a finite Galois extension whose group G is isomorphic to the Heisenberg group of order 27, let $K_1 \subset L$ be an extension of degree 3 of $K_{\mathfrak{p}}$, cut out*

by $\alpha \in \mathrm{Hom}(G, \mathbb{F}_3)$, $\alpha \neq 0$, and let σ generate $\mathrm{Gal}(K_1/K_\mathfrak{p})$. Then $H = \mathrm{Gal}(L/K_1)$ is elementary abelian of order 9, and there are $w \in K_1^\times$ and $f \in K_\mathfrak{p}^\times$ such that the Kummer group $D \subset K_1^\times/K_1^{\times 3}$ of L/K_1 is generated by the classes of

$$z = \mathrm{N}_{K_1/K_\mathfrak{p}}(w) \in K_\mathfrak{p}^\times \qquad \text{and} \qquad f\,\sigma(w)^2\sigma^2(w) = f\,z\,\frac{\sigma(w)}{w}.$$

Moreover the class of z in $\mathcal{H}$ lies in $\mathrm{Hom}(G, \mathbb{F}_3) \smallsetminus \mathbb{F}_3\alpha$. In particular every element of D is the class of $a \cdot (\sigma(w)/w)^k$ with $a \in K_\mathfrak{p}^\times$ and $k \in \mathbb{Z}$.

Proof. The center Z of G has order 3 and equals $[G, G]$ and the Frattini subgroup; $H = \ker\alpha$ is a maximal subgroup, so it contains Z, and it is abelian of exponent 3 (every maximal subgroup of the Heisenberg group is), of order 9. As $\mu_3 \subset K_1$, Kummer theory gives D, of order 9, with $L = K_1(D^{1/3})$, and the pairing $H \times D \to \mu_3$, $\langle h, \delta\rangle = h(\delta^{1/3})/\delta^{1/3}$, is perfect. Let $M_0 = L^Z$, the maximal abelian subextension; $M_0/K_\mathfrak{p}$ has group $(\mathbb{Z}/3)^2$, so $M_0 = K_1(z_0^{1/3})$ for some $z_0 \in K_\mathfrak{p}^\times$ whose class in $\mathcal{H}$ lies in $\mathrm{Hom}(G, \mathbb{F}_3)$ and not in $\mathbb{F}_3\alpha$ (the kernel of $\mathcal{H} \to K_1^\times/K_1^{\times 3}$ is $\mathbb{F}_3\alpha$), and the class $[z_0]$ of z_0 in $K_1^\times/K_1^{\times 3}$ is a nonzero element of D.

σ preserves D and acts on it nontrivially. Let $g \in G$ map to σ. For $\delta \in K_1^\times$ with $[\delta] \in D$, $g(\delta^{1/3}) \in L$ is a cube root of $\sigma(\delta)$, so σ preserves D, and for $h \in H$, $ghg^{-1}(g(\delta^{1/3})) = g(\langle h, \delta\rangle\delta^{1/3}) = \langle h, \delta\rangle\, g(\delta^{1/3})$, that is, $\langle ghg^{-1}, \sigma(\delta)\rangle = \langle h, \delta\rangle$. If σ acted trivially on D, perfectness would give $ghg^{-1} = h$ for all $h \in H$, and $G = \langle g, H\rangle$ would be abelian. So $\sigma - 1 \neq 0$ on the plane D; as $(\sigma-1)^3 = \sigma^3 - 1 = 0$ in characteristic 3, $(\sigma-1)D = \ker(\sigma-1)$ is a line, and it contains $[z_0] \neq 0$. Choose $\gamma \in K_1^\times$ with $D = \langle [z_0], [\gamma]\rangle$. Then $\sigma(\gamma)/\gamma \in z_0^j K_1^{\times 3}$ with $j \in \{1, 2\}$; put $z_1 = z_0^j$ and write $\sigma(\gamma) = \gamma z_1 c^3$ with $c \in K_1^\times$.

Exponent 3. Fix cube roots $\gamma^{1/3}, z_1^{1/3} \in L$. The lifts of σ to $M_0 = K_1(z_1^{1/3})$ form a coset of $\mathrm{Gal}(M_0/K_1)$, which permutes the three cube roots of z_1 simply transitively; so exactly one lift fixes $z_1^{1/3}$. Let $s \in G$ lift it. Then $s(\gamma^{1/3})$ is a cube root of $\sigma(\gamma) = \gamma z_1 c^3$, so $s(\gamma^{1/3}) = \zeta\gamma^{1/3} z_1^{1/3} c$ with $\zeta \in \mu_3$; replacing s by sh with $h \in Z = \mathrm{Gal}(L/M_0)$, which acts on $\gamma^{1/3}$ through a nontrivial character (as $L = M_0(\gamma^{1/3})$), we may take $\zeta = 1$. Using $s(z_1^{1/3}) = z_1^{1/3}$ and $s|_{K_1} = \sigma$,

$$s^3(\gamma^{1/3}) = \gamma^{1/3} \cdot z_1^{1/3} c \cdot z_1^{1/3}\sigma(c) \cdot z_1^{1/3}\sigma^2(c) = \gamma^{1/3}\, z_1\, \mathrm{N}_{K_1/K_\mathfrak{p}}(c).$$

Every element of G has order dividing 3, so $s^3 = 1$ and $z_1\,\mathrm{N}_{K_1/K_\mathfrak{p}}(c) = 1$.

Conclusion. Put $w = \sigma^2(c)^{-1}$. Then $\mathrm{N}(w) = \mathrm{N}(c)^{-1} = z_1$ and $\sigma(w) = c^{-1}$. The element $\gamma_0 = z_1\sigma(w)/w = \sigma(w)^2\sigma^2(w)$ satisfies $\sigma(\gamma_0)/\gamma_0 = \sigma^2(w)\, w/\sigma(w)^2 = \mathrm{N}(w)/\sigma(w)^3 = z_1 c^3 = \sigma(\gamma)/\gamma$, so $f = \gamma/\gamma_0$ is fixed by σ, that is, $f \in K_\mathfrak{p}^\times$. Hence $D = \langle [z_1], [f\gamma_0]\rangle$ with $z = z_1 = \mathrm{N}(w)$, and the class of z in $\mathcal{H}$ is j times that of z_0. □

The exponent 3 is used once, in $s^3 = 1$, and the lemma fails without it: the field $K_\mathfrak{p}(\zeta_9, (1-\omega)^{1/9})$, whose group over $K_\mathfrak{p}$ is non-abelian of order 27 and exponent 9, contains $K_1 = K_\mathfrak{p}((1-\omega)^{1/3})$, and its Kummer group over K_1 contains the class of $(1-\omega)^{1/3}$, which has valuation 1 and break 9 over K_1, whereas every element $a\,(\sigma(w)/w)^k$ with $a \in K_\mathfrak{p}^\times$ has v_{K_1}-valuation divisible by 3, as $K_1/K_\mathfrak{p}$ is totally ramified.

Proposition 11.6. *Let $L/K_\mathfrak{p}$ be a finite Galois extension whose group is isomorphic to the Heisenberg group of order 27, let G^y $(y \geq -1)$ be the upper ramification groups of $\mathrm{Gal}(L/K_\mathfrak{p})$,*

and let $W \subset \mathcal{H}$ be the plane of homomorphisms $G_{K_\mathfrak{p}} \to \mathbb{F}_3$ that factor through $\mathrm{Gal}(L/K_\mathfrak{p})$. Then W is isotropic, and:

(i) *if $W \cap \mathcal{U} = 0$, then $G^y \neq 1$ for $y \leq 11/3$ and $G^y = 1$ for $y > 11/3$;*
(ii) *if $W \cap \mathcal{U}$ is a line other than $\mathbb{F}_3 e_0$, then $G^y \neq 1$ for $y \leq 10/3$ and $G^y = 1$ for $y > 10/3$;*
(iii) *if $e_0 \in W$, then $G^y = 1$ for $y > 3$.*

Every isotropic plane falls under exactly one of (i), (ii), (iii). *In particular every Heisenberg extension of $K_\mathfrak{p}$ has largest upper ramification break at most* $11/3$.

Proof. Choose an isomorphism of $\mathrm{Gal}(L/K_\mathfrak{p})$ with the unitriangular group, and let a, b, c be its entries in positions $(1,2)$, $(2,3)$, $(1,3)$. Then a, b is a basis of W and $c(gh) = c(g) + c(h) + a(g)b(h)$, so the cup product $a \cup b$ is the class of the coboundary of c, and W is isotropic.

Exhaustion. Let $\mathcal{H}_0 = \langle e_2, e_1, e_0 \rangle$, the classes of units, which contains $\mathcal{U}$. By Lemma 11.2 (c) the cup product on $\mathcal{H}_0$ has radical $\mathbb{F}_3 e_0$, and it is nondegenerate on the plane $\mathcal{H}_0/\mathbb{F}_3 e_0$, whose isotropic subspaces have dimension at most 1. So an isotropic plane contained in $\mathcal{H}_0$ contains e_0. If $W \cap \mathcal{U} \neq 0$ and $W \cap \mathcal{U}$ is not a line other than $\mathbb{F}_3 e_0$, then $W \cap \mathcal{U}$ is $\mathbb{F}_3 e_0$ or $\mathcal{U}$, and $e_0 \in W$. If $W \cap \mathcal{U}$ is a line other than $\mathbb{F}_3 e_0$, then $e_0 \notin W$. So (i), (ii), (iii) are exhaustive and mutually exclusive. Moreover, in case (i), $W \not\subset \mathcal{H}_0$ (otherwise $\dim W \cap \mathcal{U} \geq 2 + 2 - 3$), and in case (ii) also $W \not\subset \mathcal{H}_0$ (as $e_0 \notin W$): in cases (i) and (ii), W contains a class of nonzero valuation modulo 3.

Reduction to a cubic subfield. Let $\alpha \in W$, $\alpha \neq 0$, and let $K_1 \subset L$ be the cubic extension of $K_\mathfrak{p}$ cut out by α, $H = \mathrm{Gal}(L/K_1)$, D the Kummer group of L/K_1, σ a generator of $\mathrm{Gal}(K_1/K_\mathfrak{p})$, and $\psi = \psi_{K_1/K_\mathfrak{p}}$, $\varphi = \varphi_{K_1/K_\mathfrak{p}}$. By Lemma 11.2 (b), $K_1/K_\mathfrak{p}$ is totally ramified with break $t \in \{1, 2, 3\}$, or unramified (put $t = 0$). For $y > t$, α vanishes on G^y (by (R1); if $t = 0$, because $G^y \subset G^0$), so $G^y \subset H$ and, by (R2),

$$G^y = G^y \cap H = H^{\psi(y)} \qquad (y > t). \tag{11.1}$$

The characters of H are the characters $h \mapsto \langle h, \delta \rangle$, $[\delta] \in D$, and by (R1) the character attached to δ vanishes on H^u if and only if the character of G_{K_1} cut out by δ vanishes on $G^u_{K_1}$. Hence, for $T \geq t$:

- if every element of D has break at most T, then $H^u = 1$ for $u > T$, and by (11.1) $G^y = 1$ for $y > \varphi(T)$;
- if some δ with $[\delta] \in D$ cuts out a totally ramified extension of K_1 with break $T > t$, then $H^T \neq 1$, and by (11.1) $G^y \supset H^{\psi(y)} \supset H^T \neq 1$ for $t < y \leq \varphi(T)$; so $G^y \neq 1$ for all $y \leq \varphi(T)$.

By Lemma 11.5, every element of D is the class of $a(\sigma(w)/w)^k$ with $a \in K_\mathfrak{p}^\times$, where $w \in K_1^\times$ has $z = \mathrm{N}(w)$, and D contains the class of $\delta_0 = f\, z\, \sigma(w)/w$ for some $f \in K_\mathfrak{p}^\times$. By Lemma 11.2 (b) every element of $K_\mathfrak{p}^\times$ has break at most 3 over $K_\mathfrak{p}$, so by (R3) its image in $K_1^\times$ has break at most $\psi(3)$, which is $9 - 2t$ if $t \geq 1$.

Case (iii). Take $\alpha = e_0$: K_1 is the unramified cubic extension of $K_\mathfrak{p}$, with $e_{K_1} = 2$, uniformizer $1 - \omega$ and residue field $\mathbb{F}_{27}$. Every $\delta \in K_1^\times$ is $(1-\omega)^n \varepsilon u_1$ with ε a root of unity of order dividing 26 (a cube) and $u_1 \in U^{(1)}_{K_1}$; by Lemma 11.3 (a), (b) it has break at most 3. So $G^y = 1$ for $y > \varphi(3) = 3$.

Case (ii). Take $\alpha \in W \cap \mathcal{U}$, $\alpha \notin \mathbb{F}_3 e_0$, of break 1, represented by $x \in U^{(2)}$ (Lemma 11.2). So $t = 1$, $K_1 = K_\mathfrak{p}(x^{1/3})$, $e_{K_1} = 6$, and Lemma 11.3 applies over K_1 with $3e_{K_1}/2 = 9$. By

Lemma 11.4 (a), $\sigma(w)/w \in U_{K_1}^{(1)}$ has break at most 8; elements of $K_\mathfrak{p}^\times$ have break at most $\psi(3) = 7$. So every element of D has break at most 8, and $G^y = 1$ for $y > \varphi(8) = 1 + \frac{7}{3} = \frac{10}{3}$. For the lower bound: the class of z lies in $W \smallsetminus \mathbb{F}_3\alpha$ (Lemma 11.5), so $W = \mathbb{F}_3\alpha + \mathbb{F}_3[z]$; the valuation modulo 3 is a linear form on $\mathcal{H}$ that vanishes at α and not on W, so $3 \nmid v_\mathfrak{p}(z)$. As $K_1/K_\mathfrak{p}$ is totally ramified, $v_{K_1}(w) = v_\mathfrak{p}(\mathrm{N}(w)) = v_\mathfrak{p}(z)$, so $3 \nmid v_{K_1}(w)$. Write $w = \theta_1^j u$ with θ_1 a uniformizer of K_1, $j = v_{K_1}(w)$ and u a unit. By Lemma 11.4 (a), $\sigma(\theta_1)/\theta_1 \in U_{K_1}^{(1)} \smallsetminus U_{K_1}^{(2)}$, hence $(\sigma(\theta_1)/\theta_1)^j \in U_{K_1}^{(1)} \smallsetminus U_{K_1}^{(2)}$ as $3 \nmid j$, and $\sigma(u)/u \in U_{K_1}^{(2)}$; so $\sigma(w)/w \in U_{K_1}^{(1)} \smallsetminus U_{K_1}^{(2)}$, which by Lemma 11.3 (c) cuts out a totally ramified extension with break exactly 8. As δ_0 differs from $\sigma(w)/w$ by an element of $K_\mathfrak{p}^\times$, of break at most 7, δ_0 also has break exactly 8. So $G^y \neq 1$ for $y \leq \varphi(8) = 10/3$.

Case (i). W contains a class of nonzero valuation; replacing it by its negative, it has valuation $\equiv 1 \pmod 3$, and it is represented by some x with $v_\mathfrak{p}(x) = 1$. Take $\alpha = [x]$: $t = 3$, $K_1 = K_\mathfrak{p}(\theta)$ with $\theta^3 = x$, a uniformizer of K_1, $\mathcal{O}_{K_1} = \mathcal{O}_\mathfrak{p}[\theta]$, and $\sigma(\theta) = \omega\theta$ for a suitable generator σ. Write $w = \theta^j u$ with u a unit. Then $\sigma(w)/w = \omega^j \sigma(u)/u$ with $\sigma(u)/u \in U_{K_1}^{(4)}$ (Lemma 11.4 (a)), of break at most $9 - 4 = 5$ (Lemma 11.3 (b)), and $\omega^j \in K_\mathfrak{p}^\times$ has break at most $\psi(3) = 3$. So every element of D has break at most 5, and $G^y = 1$ for $y > \varphi(5) = 3 + \frac{2}{3} = \frac{11}{3}$. For the lower bound, write $u = \pm u_1$ with $u_1 \in U_{K_1}^{(1)}$. Then $z = \mathrm{N}(w) = x^j \cdot (\pm 1) \cdot \mathrm{N}(u_1)$, as $\mathrm{N}(\theta) = \theta^3 = x$. Suppose that $u_1 \in U_{K_1}^{(2)}$. Then $\mathrm{N}(u_1) \in U^{(2)}$: write $u_1 = 1 + \zeta$ with $\zeta \in \theta^2\mathcal{O}_{K_1}$, that is, $\zeta = a_0 + a_1\theta + a_2\theta^2$ with $a_i \in \mathcal{O}_\mathfrak{p}$ and $v_\mathfrak{p}(a_0), v_\mathfrak{p}(a_1) \geq 1$; then $\mathrm{N}(1 + \zeta) = 1 + s_1 + s_2 + s_3$ with $s_1 = \mathrm{Tr}(\zeta) = 3a_0$, $s_2 = \frac{1}{2}(\mathrm{Tr}(\zeta)^2 - \mathrm{Tr}(\zeta^2))$, $s_3 = \mathrm{N}(\zeta)$, and as $\mathrm{Tr}(\theta) = \mathrm{Tr}(\theta^2) = 0$ and the constant coefficient of ζ^2 is $a_0^2 + 2a_1a_2x$, we get $v_\mathfrak{p}(s_1) \geq 3$, $v_\mathfrak{p}(s_2) \geq 4$, $v_\mathfrak{p}(s_3) = v_{K_1}(\zeta) \geq 2$. So the class of $\pm z\, x^{-j}$, which is $[z] - j\alpha$, lies in $W \cap \mathcal{U} = 0$, and $[z] \in \mathbb{F}_3\alpha$, against Lemma 11.5. Hence $u_1 \in U_{K_1}^{(1)} \smallsetminus U_{K_1}^{(2)}$, and $u_1 = (1 + \epsilon\theta)u_2$ with $\epsilon \in \{1, -1\}$ and $u_2 \in U_{K_1}^{(2)}$. Now

$$\frac{\sigma(w)}{w} = \omega^j \cdot \frac{1 + \epsilon\omega\theta}{1 + \epsilon\theta} \cdot \frac{\sigma(u_2)}{u_2}, \qquad \frac{1 + \epsilon\omega\theta}{1 + \epsilon\theta} = 1 + \frac{\epsilon(\omega - 1)\theta}{1 + \epsilon\theta} \in U_{K_1}^{(4)} \smallsetminus U_{K_1}^{(5)},$$

as $v_{K_1}(\omega - 1) = 3$; the middle factor cuts out a totally ramified extension of break exactly $9 - 4 = 5$ (Lemma 11.3 (c)), $\sigma(u_2)/u_2 \in U_{K_1}^{(5)}$ (Lemma 11.4 (b)) has break at most 4, and ω^j has break at most 3. So $\sigma(w)/w$, and δ_0, which differs from it by an element of $K_\mathfrak{p}^\times$, have break exactly 5, and $G^y \neq 1$ for $y \leq \varphi(5) = 11/3$. □

Corollary 11.7. *Let $W = \langle \alpha, \beta \rangle$ be an isotropic plane, $c\colon G_{K_\mathfrak{p}} \to \mathbb{F}_3$ continuous with $c(gh) = c(g) + c(h) + \alpha(g)\beta(h)$, and L_W the field cut out by*

$$g \mapsto \begin{pmatrix} 1 & \alpha(g) & c(g) \\ 0 & 1 & \beta(g) \\ 0 & 0 & 1 \end{pmatrix}.$$

Then the largest upper ramification break of $L_W/K_\mathfrak{p}$ is 11/3 if $W \cap \mathcal{U} = 0$, it is 10/3 if $W \cap \mathcal{U}$ is a line other than $\mathbb{F}_3 e_0$, and it is at most 3 if $e_0 \in W$. In particular it is at most 10/3 if $W \cap \mathcal{U} \neq 0$.

Proof. Such a c exists because W is isotropic. The image of the representation maps onto the unitriangular group modulo its center, because α, β are linearly independent, and the center is the Frattini subgroup; so the image is the whole unitriangular group, $\mathrm{Gal}(L_W/K_\mathfrak{p})$ is isomorphic to it, and W is the plane of Proposition 11.6. □

Remark 11.8. By Corollary 11.7, each of the two irreducible representations ρ_W of dimension 3 of $\mathrm{Gal}(L_W/K_\mathfrak{p})$ has Artin conductor $f(\rho_W) = 3(1+y_{\max})$, where $y_{\max}$ is the largest upper break. Indeed $f(\rho) = \int_{-1}^{\infty} \operatorname{codim} \rho^{G^y}\, dy$, by the definition in [101, Chapitre VI, §2] and a change of variable by Herbrand's function [101, Chapitre IV, §3], and ρ_W has no nonzero vector fixed by G^y for $y \le y_{\max}$, because every nontrivial normal subgroup contains the center, on which ρ_W is a nontrivial scalar. So $f(\rho_W) = 14$ in case (i) and 13 in case (ii). The bound 11/3 also follows from a theorem of Abrashkin: for a finite extension F_0 of $\mathbb{Q}_\ell$, $\ell > 2$, containing a primitive ℓ-th root of unity, with ramification index e_{F_0}, and for $1 \le s < \ell$, the maximal ℓ-extension $F_0[s]$ of F_0 whose Galois group has exponent ℓ and nilpotency class at most s satisfies $\mathrm{Gal}(F_0[s]/F_0)^y = 1$ if and only if $y > e_{F_0}(1 + \frac{s}{\ell-1}) - \frac{1-\delta_{1s}}{\ell}$, where δ_{1s} is 1 for $s = 1$ and 0 otherwise [3, Theorem 0.5 and the remark after it], [4, Theorem 4.5]. Abrashkin's upper numbering is that of [101], with the valuation of the base field normalized to have value group $\mathbb{Z}$ [3, §4.1]; as a check, for $s = 1$ his value $e_{F_0}\ell/(\ell-1)$ is 3 for $F_0 = K_\mathfrak{p}$, the largest break in Lemma 11.2 (b). For $F_0 = K_\mathfrak{p}$ ($e_{F_0} = 2$, $\ell = 3$) and $s = 2$ the value is $2 \cdot 2 - \frac{1}{3} = \frac{11}{3}$, which [3, §6.7] obtains as $\varphi_{K_1/K_\mathfrak{p}}(5)$ with $K_1 = K_\mathfrak{p}((1-\omega)^{1/3})$, as in case (i) of the proof of Proposition 11.6. Every Heisenberg extension of $K_\mathfrak{p}$, and every field cut out by a representation as in Proposition 11.10, lies in $K_\mathfrak{p}[2]$, so its largest upper break is at most 11/3 by (R1). Proposition 11.6 shows in addition which planes attain the bound, and gives the values 10/3 and at most 3 for the others. Single planes were treated before: Sharifi's computation of conductors for the plane $\langle [\ell], [1-\ell] \rangle$ over $\mathbb{Q}_\ell(\zeta_\ell)$ [104, Proposition 4.18] gives, for $\ell = 3$, the plane $\langle [3], [-2] \rangle = \langle [3], [2] \rangle$ (W_3 of Remark 11.9), of type (ii), with largest upper break 10/3; and for the plane $\langle [\omega], [1-\omega] \rangle = \langle e_2, e_\pi \rangle$, of type (i), compare the conductor of the top step computed by Davis and Pries [38, Lemma 4.15]. We have not found in the literature the values of Proposition 11.6 for every isotropic plane, the conductors 14 and 13, or the bound $|G^y| \le 27$ for $3 < y \le 10/3$ of Proposition 11.10.

Remark 11.9 (worked examples). We make Proposition 11.6 explicit for four of the planes used in the proof of Proposition 11.10. Let $x \in K_\mathfrak{p}^\times$ with $\alpha = [x] \ne 0$, let θ be a cube root of x, $K_1 = K_\mathfrak{p}(\theta)$ and $\sigma(\theta) = \omega\theta$, and let $w \in K_1^\times$ be such that $z = \mathrm{N}_{K_1/K_\mathfrak{p}}(w)$ satisfies $[z] \notin \mathbb{F}_3\alpha$. Put $\gamma = \sigma(w)^2\sigma^2(w) = z\,\sigma(w)/w$ and

$$L = K_1(z^{1/3}, \gamma^{1/3}) = K_\mathfrak{p}(x^{1/3},\, z^{1/3},\, (\sigma(w)/w)^{1/3}).$$

This is the converse of Lemma 11.5: $L/K_\mathfrak{p}$ is a Heisenberg extension with plane $\langle \alpha, [z] \rangle$. Indeed, z is not a cube in K_1, as the kernel of $\mathcal{H} \to K_1^\times/K_1^{\times 3}$ is $\mathbb{F}_3\alpha$, and $\sigma(\gamma)/\gamma = z/\sigma(w)^3$; so the Kummer group $\langle [z], [\gamma] \rangle$ of L/K_1 has order 9, is stable under σ and is not fixed by it, and $L/K_\mathfrak{p}$ is Galois of degree 27 and, as in the proof of Lemma 11.5, not abelian. As there, some lift s of σ fixes $z^{1/3}$ and maps $\gamma^{1/3}$ to $\gamma^{1/3}z^{1/3}\sigma(w)^{-1}$; then $s^3(\gamma^{1/3}) = \gamma^{1/3} z\, \mathrm{N}_{K_1/K_\mathfrak{p}}(\sigma(w))^{-1} = \gamma^{1/3}$, so $s^3 = 1$; and for $h \in \mathrm{Gal}(L/K_1)$ and $i \in \{1, 2\}$, $(s^i h)^3 = (s^i h s^{-i})(s^{2i} h s^{-2i})h = 1$, because $1 + \sigma + \sigma^2 = (\sigma - 1)^2$ vanishes on the $\mathbb{F}_3$-plane $\mathrm{Gal}(L/K_1)$, on which σ acts by conjugation by s. So $\mathrm{Gal}(L/K_\mathfrak{p})$ has exponent 3; being non-abelian of order 27, it is the Heisenberg group, and its plane is $\langle \alpha, [z] \rangle$, as $K_\mathfrak{p}(x^{1/3}, z^{1/3}) \subset L$ is abelian of degree 9. (See also [86, §2.2, Lemma 2.1 and Proposition 2.2].) Below, G^y are the upper ramification groups of $L/K_\mathfrak{p}$, computed from the breaks over K_1 by (R1), (R2) and Herbrand's functions as in the proof of Proposition 11.6, and $d = \int_{-1}^{\infty}(1 - |G^y|^{-1})\, dy$ is the valuation of the different of $L/K_\mathfrak{p}$, normalized by $v_\mathfrak{p}$ (proof of Proposition 11.11); the discriminant of $L/K_\mathfrak{p}$ is $\mathfrak{p}^{27d}$.

Case (i)*:* $W_1=\langle e_\pi,e_2\rangle$. Take $x=1-\omega$ and $w=1-\theta$, so that $z=1-x=\omega$ and

$$L=K_\mathfrak{p}(\zeta_9,\theta,\eta),\qquad \zeta_9^3=\omega,\quad \theta^3=1-\omega,\quad \eta^3=\frac{1-\omega\theta}{1-\theta}=1+\frac{\theta^4}{1-\theta}.$$

Here $t=3$ and θ is a uniformizer of K_1. Over K_1, $\eta^3\in U_{K_1}^{(4)}\smallsetminus U_{K_1}^{(5)}$ has break $9-4=5$ and $\omega=(1-\theta)^3(1+3\theta(1-\theta)^{-2})$ has break $9-7=2$ (Lemma 11.3 (c)), so the four lines of the Kummer group of L/K_1 have breaks $2,5,5,5$. Hence $|G^y|$ is 27 for $-1<y\le 2$, 9 for $2<y\le 3$, 3 for $3<y\le\frac{11}{3}$, and 1 for $y>\frac{11}{3}$. So $L/K_\mathfrak{p}$ is totally ramified, its lower breaks are $2,5,11$, and the top step $L/K_\mathfrak{p}(\zeta_9,\theta)$, whose group is the center (contained in every nontrivial G_u), has break 11 and conductor 12, the value of [38, Lemma 4.15] at the prime 3; and $d=3\cdot\frac{26}{27}+\frac{8}{9}+\frac{2}{3}\cdot\frac{2}{3}=\frac{38}{9}$, so $v_L(\mathfrak{D}_{L/K_\mathfrak{p}})=27d=114$ and the discriminant of $L/K_\mathfrak{p}$ is $\mathfrak{p}^{114}$. This agrees with the conductor–discriminant formula: the six characters of order 3 of $\mathrm{Gal}(L/K_\mathfrak{p})$ outside $\mathbb{F}_3e_2$ have conductor 4, the two in $\mathbb{F}_3e_2$ conductor 3, and the two irreducible characters of degree 3 conductor 14 (Remark 11.8), and $6\cdot4+2\cdot3+2\cdot3\cdot14=114$.

Case (ii)*:* $W_3=\langle e_\pi+e_2,e_1\rangle=\langle[3],[2]\rangle$, the plane of [104, Proposition 4.18] at the prime 3. Take $x=2$, of class $-e_1$, so that $t=1$ and $\theta=2^{1/3}$ is a unit of K_1, and $w=1+\theta$; then $z=3$, of class $-(e_\pi+e_2)$, and

$$L=K_\mathfrak{p}(2^{1/3},3^{1/3},\eta),\qquad \eta^3=\frac{1+\omega\,2^{1/3}}{1+2^{1/3}}=1+\frac{(\omega-1)\,2^{1/3}}{1+2^{1/3}}\in U_{K_1}^{(1)}\smallsetminus U_{K_1}^{(2)},$$

as $v_{K_1}(1+\theta)=v_\mathfrak{p}(3)=2$ and $v_{K_1}(\omega-1)=3$. Over K_1, η^3 has break 8, that is, conductor $9=\ell^2-\ell+3$ for $\ell=3$, as in [104, Proposition 4.18], and z has break $\psi_{K_1/K_\mathfrak{p}}(3)=7$ (by (R2) for $K_\mathfrak{p}(2^{1/3},3^{1/3})$). Hence $|G^y|$ is 27 for $-1<y\le 1$, 9 for $1<y\le 3$, 3 for $3<y\le\frac{10}{3}$ and 1 beyond; the largest upper break is $\varphi_{K_1/K_\mathfrak{p}}(8)=\frac{10}{3}$, $d=\frac{106}{27}$, and the discriminant of $L/K_\mathfrak{p}$ is $\mathfrak{p}^{106}$, in agreement with $6\cdot4+2\cdot2+2\cdot3\cdot13=106$.

Case (iii). Here the largest upper break of $L/K_\mathfrak{p}$ is the largest break of the Kummer group of L over the unramified cubic extension of $K_\mathfrak{p}$ (proof of Proposition 11.6), so by Lemma 11.3 (with $e=2$) it is an integer; by (R1) it is at least the largest break of the characters in W, which is 2 if $W\ne\mathcal{U}$ and 1 if $W=\mathcal{U}$: by Lemma 11.2 (c) an isotropic plane containing e_0 lies in $\langle e_2,e_1,e_0\rangle$, and Lemma 11.2 (b) gives the breaks. It depends on c: for W_4 below both values 2 and 3 occur, and for $W_5=\mathcal{U}$ all three values 1, 2, 3.

For $W_4=\langle e_2,e_0\rangle$ take $x=\omega$, so that $\theta=\zeta_9$, $K_1=K_\mathfrak{p}(\zeta_9)$ and $t=2$, and $w=1+(1-\omega)\zeta_9$; then $z=7+3\omega$, of class e_0, is unramified over K_1, and $\sigma(w)/w\in U_{K_1}^{(6)}$ has break at most 2 (Lemma 11.3 (b)). So the largest upper break is 2, the inertia group has order 9, and the discriminant is $\mathfrak{p}^{72}$ $(=\mathfrak{p}^{6\cdot3+2\cdot3\cdot9})$. Replacing $\sigma(w)/w$ by $(1-\omega)\sigma(w)/w$, which changes c in Corollary 11.7 by an element of $\mathcal{H}$, gives break 5 over K_1, since $1-\omega=(1-\zeta_9)^3(1+3\zeta_9(1-\zeta_9)^{-2})$; the largest upper break becomes $\varphi_{K_1/K_\mathfrak{p}}(5)=3$ and the discriminant $\mathfrak{p}^{90}$.

For $W_5=\mathcal{U}$ take $x=2$ $(t=1)$ and $w=1-(1-\omega)\theta$, so that $z=7+12\omega$, of class e_0, and $\sigma(w)/w\in U_{K_1}^{(6)}$ has break at most 2. Over K_1, ω and $1-\omega$ have breaks $\psi_{K_1/K_\mathfrak{p}}(2)=4$ and $\psi_{K_1/K_\mathfrak{p}}(3)=7$ (by (R2) for $K_\mathfrak{p}(2^{1/3},\omega^{1/3})$ and $K_\mathfrak{p}(2^{1/3},(1-\omega)^{1/3})$). So replacing $\sigma(w)/w$ by $f\sigma(w)/w$ with $f=1$, ω, $1-\omega$ gives the largest upper breaks 1 (an integer at most $\varphi_{K_1/K_\mathfrak{p}}(2)=\frac{4}{3}$), $\varphi_{K_1/K_\mathfrak{p}}(4)=2$ and $\varphi_{K_1/K_\mathfrak{p}}(7)=3$, and the discriminants $\mathfrak{p}^{48}$, $\mathfrak{p}^{66}$ and $\mathfrak{p}^{84}$.

All the discriminants above were also computed from the number fields of degree 54 given by the same x, w and f over K, such as $\mathbb{Q}(\zeta_9,\theta,\eta)$ in case (i) and $\mathbb{Q}(\omega,2^{1/3},3^{1/3},\eta)$ in case (ii). Each has a single prime above 3, with completion L, and the 3-adic valuations of

their discriminants, 27 more than the exponents above, are 141, 133, 99, 117, 75, 93 and 111 (Supplement, item S8).

Proposition 11.10. *Let k be a finite field of characteristic 3, let $a, b \in \mathrm{Hom}(G_{K_\mathfrak{p}}, k)$, and let $c\colon G_{K_\mathfrak{p}} \to k$ be continuous with $c(gh) = c(g) + c(h) + a(g)b(h)$, so that*

$$\Upsilon\colon G_{K_\mathfrak{p}} \to \mathrm{GL}_3(k), \qquad g \mapsto \begin{pmatrix} 1 & a(g) & c(g) \\ 0 & 1 & b(g) \\ 0 & 0 & 1 \end{pmatrix}$$

is a homomorphism. Let G^y be the upper ramification groups of the field cut out by Υ, identified with $\Upsilon(G^y_{K_\mathfrak{p}})$. Then $G^y = 1$ for $y > 11/3$, $|G^y| \le 3$ for $10/3 < y \le 11/3$, and $|G^y| \le 27$ for $3 < y \le 10/3$.

For $y > 3$ the restriction of c to $G^y_{K_\mathfrak{p}}$ depends linearly on the Plücker vector of $a \wedge b$, which lies in a space of dimension 5. So it is enough to control it for five suitably chosen isotropic planes whose Plücker vectors form a basis. Corollary 11.7 says, for each isotropic plane, in which range of y it vanishes, according to how the plane meets $\mathcal{U}$. The bounds stated come from a basis with one plane meeting $\mathcal{U}$ only in 0, two meeting it in a line other than $\mathbb{F}_3 e_0$, and two containing e_0, as in the proof.

Proof. Write $\mathcal{H}_k = \mathrm{Hom}(G_{K_\mathfrak{p}}, k) = \mathcal{H} \otimes_{\mathbb{F}_3} k$, and $a = \sum_i a_i e_i$, $b = \sum_i b_i e_i$ with $a_i, b_i \in k$, where i runs over $\{\pi, 2, 1, 0\}$ in this order. For $y > 3$, every element of $\mathcal{H}_k$ vanishes on $G^y_{K_\mathfrak{p}}$ (Lemma 11.2 (b)); so a and b vanish there, and $\Upsilon(g)$, for $g \in G^y_{K_\mathfrak{p}}$, is determined by $c(g)$. We show that c vanishes on $G^y_{K_\mathfrak{p}}$ for $y > 11/3$, and that its values on $G^y_{K_\mathfrak{p}}$ lie in an $\mathbb{F}_3$-line of k for $10/3 < y \le 11/3$, and in an $\mathbb{F}_3$-subspace of dimension at most 3 for $3 < y \le 10/3$.

For maps f, f' from $G_{K_\mathfrak{p}}$ to k put $(\partial f)(g,h) = f(gh) - f(g) - f(h)$ and $(f \cdot f')(g,h) = f(g)f'(h)$. For $f, f' \in \mathcal{H}_k$, the pointwise product ff' satisfies $\partial(ff') = f \cdot f' + f' \cdot f$, and $\partial(f^2) = 2f \cdot f$. Expanding $a \cdot b = \sum_{i,j} a_i b_j\, e_i \cdot e_j$ we get

$$a \cdot b = \sum_{i<j} \eta_{ij}\, e_i \cdot e_j + \partial Q, \qquad \eta_{ij} = a_i b_j - a_j b_i, \qquad Q = \sum_{i<j} a_j b_i\, e_i e_j + \tfrac{1}{2} \sum_i a_i b_i\, e_i^2.$$

The hypothesis on c is $\partial c = a \cdot b$, so $c' = c - Q$ satisfies $\partial c' = \sum_{i<j} \eta_{ij} e_i \cdot e_j$. The vector (η_{ij}) is the Plücker vector $a \wedge b \in \bigwedge^2 \mathcal{H}_k$ in the basis $(e_i \wedge e_j)_{i<j}$. Let $\mathcal{P} \subset \bigwedge^2 \mathcal{H}$ be the kernel of the linear form $\bigwedge^2 \mathcal{H} \to \mathbb{F}_3$, $f \wedge f' \mapsto f \cup f'$, induced by the cup product; it has dimension 5 by Lemma 11.2 (c). For $\xi = \sum \xi_{ij} e_i \wedge e_j \in \mathcal{P}$ the 2-cocycle $\sum \xi_{ij} e_i \cdot e_j$ is a coboundary: there is a continuous $c_\xi\colon G_{K_\mathfrak{p}} \to \mathbb{F}_3$ with $\partial c_\xi = \sum \xi_{ij} e_i \cdot e_j$. Choose such c_ξ for ξ in a basis of $\mathcal{P}$, and extend $\xi \mapsto c_\xi$ linearly to $\mathcal{P} \otimes k$. The class of the 2-cocycle $\sum_{i<j} \eta_{ij}\, e_i \cdot e_j$ in $H^2(G_{K_\mathfrak{p}}, k) = H^2(G_{K_\mathfrak{p}}, \mathbb{F}_3) \otimes_{\mathbb{F}_3} k = k$ is $\sum_{i<j} \eta_{ij}\, (e_i \cup e_j)$, the value at $a \wedge b$ of the k-linear extension of the form induced by the cup product; as this cocycle is the coboundary $\partial c'$, the value is 0, that is, $a \wedge b$ lies in $\mathcal{P} \otimes k$. So $c' - c_{a \wedge b}$ is a homomorphism $G_{K_\mathfrak{p}} \to k$. For $y > 3$, both $c' - c_{a\wedge b}$ and Q vanish on $G^y_{K_\mathfrak{p}}$, so

$$c|_{G^y_{K_\mathfrak{p}}} = c_{a \wedge b}|_{G^y_{K_\mathfrak{p}}} \qquad (y > 3).$$

For $y > 3$ the map $\Phi_y\colon \mathcal{P} \to \mathrm{Hom}(G^y_{K_\mathfrak{p}}, \mathbb{F}_3)$, $\xi \mapsto c_\xi|_{G^y_{K_\mathfrak{p}}}$, is $\mathbb{F}_3$-linear, and it does not depend on the choice of the c_ξ, since two choices differ by an element of $\mathcal{H}$. Let $W = \langle \alpha, \beta \rangle$ be an isotropic plane, and c_W as in Corollary 11.7. Applying the identity just proved to (α, β, c_W) in place of (a, b, c), we get $c_W = c_{\alpha \wedge \beta}$ on $G^y_{K_\mathfrak{p}}$ for $y > 3$. By Corollary 11.7, c_W vanishes on

$G^y_{K_\mathfrak{p}}$ for $y > 11/3$, for $y > 10/3$ if $W \cap \mathcal{U}$ is a line other than $\mathbb{F}_3 e_0$, and for $y > 3$ if $e_0 \in W$. So $\Phi_y(\alpha \wedge \beta) = 0$ in these ranges.

Let $\mathcal{P}_0 \subset \mathcal{P}$ be the kernel of the map $\mathcal{P} \to \bigwedge^2(\mathcal{H}/\mathcal{U}) \cong \mathbb{F}_3$; in coordinates, $\xi \mapsto \xi_{\pi 2}$. Consider the planes

$$W_1 = \langle e_\pi, e_2\rangle, \quad W_2 = \langle e_\pi, e_1 + e_0\rangle, \quad W_3 = \langle e_\pi + e_2, e_1\rangle,$$
$$W_4 = \langle e_2, e_0\rangle, \quad W_5 = \mathcal{U} = \langle e_1, e_0\rangle,$$

which are isotropic by Lemma 11.2 (c). (Remark 11.9 gives explicit Heisenberg extensions for W_1, W_3, W_4 and W_5, and the Supplement, item S8, one for each of the five planes.) In the basis $(e_\pi \wedge e_2, e_\pi \wedge e_1, e_\pi \wedge e_0, e_2 \wedge e_1, e_2 \wedge e_0, e_1 \wedge e_0)$ of $\bigwedge^2 \mathcal{H}$ their Plücker vectors are

$$\xi_1 = (1,0,0,0,0,0), \quad \xi_2 = (0,1,1,0,0,0), \quad \xi_3 = (0,1,0,1,0,0),$$
$$\xi_4 = (0,0,0,0,1,0), \quad \xi_5 = (0,0,0,0,0,1).$$

They are linearly independent, so they form a basis of $\mathcal{P}$, which has dimension 5; and $\xi_2, \dots, \xi_5$ form a basis of $\mathcal{P}_0$, which has dimension 4 since $\xi_1 \notin \mathcal{P}_0$. Now $W_1 \cap \mathcal{U} = 0$; $W_2 \cap \mathcal{U} = \mathbb{F}_3(e_1 + e_0)$ and $W_3 \cap \mathcal{U} = \mathbb{F}_3 e_1$ are lines other than $\mathbb{F}_3 e_0$; and $e_0 \in W_4 \cap W_5$. So $\Phi_y(\xi_1) = 0$ for $y > 11/3$, $\Phi_y(\xi_2) = \Phi_y(\xi_3) = 0$ for $y > 10/3$, and $\Phi_y(\xi_4) = \Phi_y(\xi_5) = 0$ for $y > 3$. Hence $\Phi_y = 0$ for $y > 11/3$, and $\Phi_y(\mathcal{P}_0) = 0$ for $y > 10/3$. For $y > 11/3$ this gives $c = 0$ on $G^y_{K_\mathfrak{p}}$, so $G^y = 1$. For $10/3 < y \le 11/3$, $a \wedge b - \eta_{\pi 2}\xi_1 \in \mathcal{P}_0 \otimes k$, so $c = \eta_{\pi 2}\, c_{\xi_1}$ on $G^y_{K_\mathfrak{p}}$, with values in the line $\eta_{\pi 2}\mathbb{F}_3$, and $|G^y| \le 3$. For $3 < y \le 10/3$, write $a \wedge b = \sum_{i=1}^5 \nu_i \xi_i$ with $\nu_i \in k$. As $\Phi_y(\xi_4) = \Phi_y(\xi_5) = 0$, we get $c = \nu_1 c_{\xi_1} + \nu_2 c_{\xi_2} + \nu_3 c_{\xi_3}$ on $G^y_{K_\mathfrak{p}}$, with values in the $\mathbb{F}_3$-span of ν_1, ν_2, ν_3, a group of order at most 27; so $|G^y| \le 27$. □

11.4. **Root discriminants.**

Proposition 11.11. *Let Λ be a stable lattice and $L \subset L_\Lambda$ a finite Galois extension of K. Then $\mathrm{rd}(L) < 3^{449/162}$. If moreover the inertia groups of L/K at the primes above $\mathfrak{p}$ have order at most 3^s, $s \ge 0$, then*

$$\mathrm{rd}(L) \le T_s := 3^{\frac{1}{2} + (1-3^{-s})\cdot\frac{13}{6} + \min(1-3^{-s}, \frac{2}{3})\cdot\frac{1}{6}}.$$

Here $T_1 = 3^{37/18} < 9.5665$, $T_2 = 3^{137/54} < 16.2359$ and $T_3 = 3^{437/162} < 19.3665$.

Proof. The extension L/K is unramified outside $\mathfrak{p}$, and its primes above $\mathfrak{p}$ are conjugate. Let w be one of them, G^y the upper ramification groups of $L_w/K_\mathfrak{p}$, and $d = v_\mathfrak{p}(\mathfrak{D}_{L_w/K_\mathfrak{p}})$ the valuation of the different, normalized by $v_\mathfrak{p}(1-\omega) = 1$. As $d_L = \mathrm{N}_{K/\mathbb{Q}}(d_{L/K})\, d_K^{[L:K]}$, $|d_K| = 3$ and $\mathrm{N}\,\mathfrak{p} = 3$, we have $\mathrm{rd}(L) = 3^{(1+d)/2}$. By [101, Chapitre IV, §1, Proposition 4], $v_{L_w}(\mathfrak{D}) = \int_{-1}^{\infty}(|G_x| - 1)\, dx$ in the lower numbering; the change of variables $y = \varphi(x)$, $dx = (|G_0|/|G_x|)\, dy$, and $e(L_w/K_\mathfrak{p}) = |G_0|$ give

$$d = \int_{-1}^{\infty} \Big(1 - \frac{1}{|G^y|}\Big)\, dy.$$

The field L_w is contained in the field cut out by $\overline{R}_\Lambda|_{G_{K_\mathfrak{p}}} = \bar\psi \cdot \Upsilon$, with Υ and (a,b,c) as in Propositions 10.6 and 11.10, hence in the compositum of the unramified extension cut out by $\bar\psi$ and of the field cut out by Υ. So for $y \ge 0$ the group G^y is a quotient of the corresponding ramification group of the field cut out by Υ (the upper numbering passes to quotients, and an unramified extension does not change the ramification groups). As $\Upsilon(I_\mathfrak{p})$ consists of unipotent matrices, it is a 3-group, and $L_w/K_\mathfrak{p}$ has no tame part: $G^y = G^0$ for $-1 < y \le 0$ and for small $y > 0$. By Proposition 11.10, applied with $k = \mathbb{F}_E$, $G^y = 1$ for

$y > 11/3$, $|G^y| \le 3$ for $10/3 < y \le 11/3$, and $|G^y| \le 27$ for $3 < y \le 10/3$. The integrand $1 - 1/|G^y|$ lies in $[0,1)$, as $1 \le |G^y| < \infty$, so

$$d < 4 + \frac{1}{3}\Big(1 - \frac{1}{27}\Big) + \frac{1}{3}\Big(1 - \frac{1}{3}\Big) = \frac{368}{81}, \qquad \mathrm{rd}(L) < 3^{(1+368/81)/2} = 3^{449/162}.$$

If $|G^0| \le 3^s$, the integrand is at most $1 - 3^{-s}$ on $(-1, 10/3]$, at most $\min(1 - 3^{-s}, \frac{2}{3})$ on $(10/3, 11/3]$, where $|G^y| \le 3$, and 0 beyond, so $d \le (1 - 3^{-s}) \cdot \frac{13}{3} + \min(1 - 3^{-s}, \frac{2}{3}) \cdot \frac{1}{3}$ and $\mathrm{rd}(L) \le T_s$. The decimal values are those of Appendix A, item C5. □

The bounds on $|G^y|$ for $3 < y \le 11/3$ are what make this work. With only $G^y = 1$ for $y > 11/3$, the proof gives $d < 14/3$ and $\mathrm{rd}(L) < 3^{17/6}$, and $3^{17/6} > 22.48$ lies above the supremum $4\pi e^\gamma < 22.39$ of the bounds of Section 8.3; with them, $3^{449/162} < 21.01$ lies below it.

11.5. **Lower bounds.**

Proposition 11.12. *Let L be a totally complex number field of degree n. Then*

$n \ge$	1378	674	118	80	24	20
$\mathrm{rd}(L) >$	21.1515	20.4476	16.9179	15.6281	10.5939	9.7691

and $\mathrm{rd}(L) > 3.2422$ if $n \ge 4$. On the other hand $3^{449/162} < 21.0084$, $T_3 < 19.3665$, $T_2 < 16.2359$, $3^{5/2} < 15.5885$, $3^{11/6} < 7.4942$, $T_1 < 9.5665$ and $\sqrt{3} < 1.7321$.

Proof. The right side of (8.2), with $r_1 = 0$ and the test function $\Phi(x) = \Phi_0(x/b)/\cosh(x/2)$ of Section 8.3, was evaluated with certified error bounds at $b = \frac{63}{2}, 25, 12, 10, 6, 6, 2$ for the seven degrees $n = 1378, 674, 118, 80, 24, 20, 4$ (Appendix A, item C5). For fixed b the bound increases with n. The smallest margin is $2.54 \cdot 10^{-3}$ in $\log \mathrm{rd}$, at $n = 80$, against $3^{5/2}$ (item C5). The comparison at $n = 674$ with T_3 is used in the case $s = 3$ of the proof of Proposition 11.13, where Δ is the projective image of an irreducible reduction $\overline{R}_\Lambda$ and 3^s the 3-part of $|\Delta|$: with $3^{449/162}$ in place of T_3, step (c) there would give only $|\Delta| \le 688$, while for non-solvable Δ the count of step (d) gives only $|\Delta| \ge 540$. □

11.6. **The reductions.**

Proposition 11.13. *For every stable lattice Λ, $\overline{R}_\Lambda$ is reducible.*

Proof. Suppose that $\overline{R}_\Lambda$ is irreducible. Let $\Delta \subset \mathrm{PGL}_3(\mathbb{F}_E)$ be its projective image, $L \subset L_\Lambda$ the field cut out by the projective representation, which is Galois over K with group Δ and totally complex of degree $2|\Delta|$, and $P \subset \Delta$ an inertia group at a prime above $\mathfrak{p}$.

(a) *Δ is generated by the conjugates of P, which is a 3-group.* The subgroup generated by the inertia groups at the primes above $\mathfrak{p}$ is normal, and its fixed field is unramified over K at every place. A nontrivial extension of K unramified at every place would be totally complex of degree at least 4 with root discriminant $\mathrm{rd}(K) = \sqrt{3}$, which Proposition 11.12 excludes; so that subgroup is Δ. And P is a 3-group, by the proof of Proposition 11.11.

(b) *Δ has no nontrivial normal 3-subgroup.* Let $Q \subset \Delta$ be one, and $\tilde{Q}$ its preimage in $\overline{R}_\Lambda(G_K)$. The kernel of $\overline{R}_\Lambda(G_K) \to \Delta$ consists of scalar matrices, whose orders are prime to 3; so $\tilde{Q}$ is the direct product of this kernel and of its unique Sylow 3-subgroup Q_3, which is therefore normal in $\overline{R}_\Lambda(G_K)$. A 3-subgroup of $\mathrm{GL}_3(\mathbb{F}_E)$ is unipotent, so the vectors fixed by Q_3 form a nonzero subspace, stable under $\overline{R}_\Lambda(G_K)$. As $\overline{R}_\Lambda$ is irreducible, Q_3 acts trivially, so $Q_3 = 1$ and $Q = 1$.

(c) *Orders.* $\Delta \ne 1$, since otherwise $\overline{R}_\Lambda(G_K)$ would consist of scalars; by (a), 3 divides $|\Delta|$. Let 3^s be the 3-part of $|\Delta|$, so $s \ge 1$ and $|P| \le 3^s$. By Proposition 11.11, $\mathrm{rd}(L) < 3^{449/162}$

and $\mathrm{rd}(L) \le T_s$; by Proposition 11.12, $2|\Delta| < 20$, 118, 674, 1378 if $s = 1$, 2, 3, $s \ge 4$ respectively. So $|\Delta| \le 9$, 58, 336, 688 respectively.

(d) *Groups.* If $s = 1$, then $|\Delta| \in \{3, 6\}$, and the Sylow 3-subgroup is normal, against (b). Let $s \ge 2$; then $s \le 5$, since $3^6 > 688$. Suppose first that Δ is solvable, and let Δ_{F} be its Fitting subgroup. By (b), Δ_{F} has order prime to 3, and it contains its own centralizer in Δ; so a Sylow 3-subgroup of Δ, of order 3^s, acts faithfully on Δ_{F} by conjugation, and 3^s divides $|\mathrm{Aut}(\Delta_{\mathrm{F}})|$. The order of Δ_{F} divides the part m of $|\Delta|$ prime to 3, and by (c) $m \le 6$, 12, 8, 2 for $s = 2, 3, 4, 5$. But for every group Y of order at most 12 and prime to 3, the 3-part of $|\mathrm{Aut}(Y)|$ is at most 3: these groups are 1, C_2, C_4, C_2^2, C_5, C_7, C_8, $C_4 \times C_2$, D_4, Q_8, C_2^3, C_{10}, D_5 and C_{11}, whose automorphism groups have orders 1, 1, 2, 6, 4, 6, 4, 8, 8, 24, 168, 4, 20 and 10. This contradicts $3^s \ge 9$. If Δ is not solvable, it has a non-abelian simple composition factor S with $|S| \le 688$, so S is one of A_5, $\mathrm{PSL}_2(\mathbb{F}_7)$, A_6, $\mathrm{PSL}_2(\mathbb{F}_8)$, $\mathrm{PSL}_2(\mathbb{F}_{11})$, of orders 60, 168, 360, 504, 660 and with 3-parts 3, 3, 9, 9, 3 [34]. The other composition factors contribute the rest of the 3-part of $|\Delta|$. So $|\Delta| \ge 60 > 58$ if $s = 2$; $|\Delta| \ge \min(9 \cdot 60,\ 3 \cdot 360) = 540 > 336$ if $s = 3$; and $|\Delta| \ge \min(27 \cdot 60,\ 9 \cdot 360) = 1620 > 688$ if $s \ge 4$. In each case this is a contradiction. □

Proposition 11.14. *$\overline{R}^{\mathrm{ss}}$ is not of the form $\theta \oplus \Theta$ with θ a character and Θ irreducible of dimension 2.*

Proof. Suppose it is. For a suitable stable lattice Λ, Θ is a subquotient of $\overline{R}_\Lambda$, so by Proposition 10.6 its restriction to $G_{K_\mathfrak{p}}$ has, in a suitable basis, the form $g \mapsto \bar{\psi}(g)\left(\begin{smallmatrix} 1 & \eta(g) \\ 0 & 1 \end{smallmatrix}\right)$ with $\eta \in \mathrm{Hom}(G_{K_\mathfrak{p}}, \mathbb{F}_E)$. Let Δ be the projective image of Θ and L the field it cuts out, Galois over K with group Δ, totally complex of degree $2|\Delta|$, unramified outside $\mathfrak{p}$. The completions of L at the primes above $\mathfrak{p}$ are cut out by η: they are abelian of exponent 3, without tame part, and with upper breaks at most 3 by Lemma 11.2 (b). As in the proof of Proposition 11.11, $d < 1 + 3$ and $\mathrm{rd}(L) < 3^{5/2}$, so $2|\Delta| < 80$ by Proposition 11.12, and $|\Delta| \le 39$. As in (a) and (b) of the proof of Proposition 11.13, Δ is generated by its elements of order a power of 3 and has no nontrivial normal 3-subgroup. Also $\Delta \ne 1$, since Θ is irreducible, so 3 divides $|\Delta|$. By Dickson's classification of the finite subgroups of $\mathrm{PGL}_2(\overline{\mathbb{F}}_3)$ [47] (see [51, Theorem B and Remark 2.3]), a finite subgroup of $\mathrm{PGL}_2(\overline{\mathbb{F}}_3)$ of order divisible by 3 without nontrivial normal 3-subgroup is isomorphic to $A_4 \cong \mathrm{PSL}_2(\mathbb{F}_3)$, $S_4 \cong \mathrm{PGL}_2(\mathbb{F}_3)$, A_5, $\mathrm{PSL}_2(\mathbb{F}_{3^m})$ or $\mathrm{PGL}_2(\mathbb{F}_{3^m})$ with $m \ge 2$. Of these only A_4 and S_4 have order at most 39, and S_4 is not generated by its elements of order 3. So $\Delta \cong A_4$, whose 3-subgroups have order at most 3: the inertia groups have order at most 3, so $d \le \frac{2}{3} \cdot 4$ and $\mathrm{rd}(L) \le 3^{11/6} < 7.4942$, while $[L : \mathbb{Q}] = 24$ gives $\mathrm{rd}(L) > 10.5939$ (Proposition 11.12). This is a contradiction. □

Corollary 11.15. *For every stable lattice Λ, $\overline{R}^{\mathrm{ss}}$ is the sum of three copies of the trivial character.*

Proof. After enlarging E, every constituent of $\overline{R}^{\mathrm{ss}}$ is absolutely irreducible, and $\overline{R}^{\mathrm{ss}}$ is irreducible, or the sum of a character and an irreducible representation of dimension 2, or a sum of three characters. The first two cases are excluded by Propositions 11.13 and 11.14, and in the third every character is trivial by Proposition 11.1. □

11.7. **Local generation.** The following lemma is elementary and well known. It goes back to Shafarevich and Koch [103, 79], and Greenberg states it in the form "$\mathfrak{p}$ is totally ramified in M/K" [67, Remark 6.1.4]. Freitas, Kraus and Siksek prove that an ℓ-extension of a number field unramified away from one prime $\mathfrak{q}$ and the infinite places is totally ramified at $\mathfrak{q}$ when ℓ does not divide the narrow class number [60, Theorem 9(b)]. We include the proof.

Lemma 11.16. *Let ℓ be an odd prime and K' a number field with only one prime $\mathfrak{q}$ above ℓ and with class number prime to ℓ. Let Ω be the maximal pro-ℓ extension of K' unramified outside $\mathfrak{q}$, and $G = \mathrm{Gal}(\Omega/K')$. Then the inertia group in G of a prime of Ω above $\mathfrak{q}$ is G.*

Proof. Let $T \subset G$ be such an inertia group; it is compact, hence closed. As G is a pro-ℓ group, a closed subgroup that maps onto $G/\Phi(G)$, where $\Phi(G)$ is the Frattini subgroup (the closure of $G^\ell[G,G]$), is G itself. So it suffices to show that every continuous homomorphism $\chi\colon G \to \mathbb{F}_\ell$ with $\chi(T) = 0$ is zero. Such a χ vanishes on all the inertia groups above $\mathfrak{q}$, which are conjugate to T; so it cuts out an extension of K' of degree 1 or ℓ that is unramified at every finite place, and also at the infinite places, as ℓ is odd. As ℓ does not divide the class number, the extension is trivial and $\chi = 0$. □

Corollary 11.17. *Let $R'\colon G_K \to \mathrm{GL}_3(\overline{\mathbb{Q}}_3)$ be a continuous representation, unramified outside $\mathfrak{p}$, whose reduction has trivial semisimplification. Then $R'(G_K) = R'(I_\mathfrak{p})$.*

Proof. The image of R' is compact, so R' is defined over the ring of integers $\mathcal{O}'$ of a finite extension of $\mathbb{Q}_3$, with uniformizer ϖ and residue field k', and stabilizes a lattice. The reduction of the lattice has trivial semisimplification, so in a suitable basis of the lattice it is upper unitriangular, and $R'(G_K)$ lies in the preimage in $\mathrm{GL}_3(\mathcal{O}')$ of the group of upper unitriangular matrices of $\mathrm{GL}_3(k')$, a pro-3 group (an extension of a finite 3-group by $1 + \varpi M_3(\mathcal{O}')$). So R' factors through $\mathrm{Gal}(\Omega/K)$, where Ω is the maximal pro-3 extension of K unramified outside $\mathfrak{p}$. The field K has one prime above 3 and class number one, so by Lemma 11.16 the image of $I_\mathfrak{p}$ in $\mathrm{Gal}(\Omega/K)$ is the whole group. Hence $R'(G_K) = R'(I_\mathfrak{p})$. □

11.8. **The theorem.**

Theorem 11.18. *Let $p \geq 17$ be a prime with $p \equiv 1 \pmod 3$. Then $x^3 + y^3 = z^p$ has no solution in coprime nonzero integers.*

Proof. Suppose that (a,b,c) is a solution. By Proposition 5.1, $3 \mid c$, $p \nmid c$ and $7 \nmid abc$, so the Frey representation ρ of the solution is defined and has the properties (F1)–(F6) of Section 7.1. By Proposition 7.2, Lemma 7.5, and Theorem 7.3 there is a compatible system $\mathcal{R}$ as in Section 7.6. Let λ be a prime of its coefficient field above 3 and $R = R_\lambda$. By Proposition 10.4, R is unramified outside $\mathfrak{p}$; by Proposition 10.6, $R|_{G_{K_\mathfrak{p}}}$ stabilizes a line V_1; by Corollary 11.15, the reduction of R has trivial semisimplification. By Corollary 11.17, $R(G_K) = R(I_\mathfrak{p}) \subset R(G_{K_\mathfrak{p}})$, so V_1 is stable under G_K, and R is reducible. This contradicts Proposition 10.7. □

Corollary 11.19. *For every integer $n \geq 3$ the equation $x^3 + y^3 = z^n$ has no solution in coprime nonzero integers.*

Proof. An integer $n \geq 3$ has an odd prime factor q, or is divisible by 4; a solution (a,b,c) for the exponent n gives the solution $(a,b,c^{n/q})$ for the exponent q, or $(a,b,c^{n/4})$ for the exponent 4. For the exponents m with $3 \leq m \leq 10^9$, in particular $m = 4$ and the primes $q \leq 13$, there is no solution by [30, Theorem 2]; for the primes $q \geq 17$ with $q \equiv 2 \pmod 3$ by [58, Theorem 3]; and for the primes $q \geq 17$ with $q \equiv 1 \pmod 3$ by Theorem 11.18. □

Remark 11.20. The two-dimensional analogue of Propositions 11.13 and 11.14 is a theorem of Şengün: there is no irreducible continuous representation of G_K in $\mathrm{GL}_2(\overline{\mathbb{F}}_3)$ unramified outside $\mathfrak{p}$ [99, Theorem C]. The method, a ramification bound played against lower bounds for discriminants, is Tate's [109]; it was refined by Moon and Taguchi [89] and extended to representations of higher dimension by Moon [88], and Ghitza and Yamauchi prove, under

the generalized Riemann hypothesis, that $G_{\mathbb{Q}}$ has no irreducible totally real representation modulo 3 of dimension 2, 3 or 4 unramified outside 3 [64, Theorem A (b)]. Dieulefait and Golfieri Madriaga [48, §2] also argue at a prime above 3, for Fermat's equation over totally real fields when $3 \mid xyz$, but differently: the Frey curve has multiplicative reduction there, and level lowering with the Hasse–Weil bound excludes large exponents.

Proposition 11.21. *There is no continuous representation $R\colon G_K \to \mathrm{GL}_3(\overline{\mathbb{Q}}_3)$ that is semisimple, unramified at every prime $\mathfrak{q} \neq \mathfrak{p}$, and de Rham at $\mathfrak{p}$ with Hodge–Tate weights $\{0,1,2\}$ for both embeddings of $K_{\mathfrak{p}}$, and such that the monodromy operator of $\mathrm{WD}(R|_{G_{K_{\mathfrak{p}}}})$ is regular.*

Proof. The proofs of Propositions 10.6 and 10.7 and of Proposition 11.1 to Corollary 11.17, and the last three sentences of the proof of Theorem 11.18, use only these four properties of R, together with a character of $G_{K_{\mathfrak{p}}}$ of 3-power order through which $I_{\mathfrak{p}}$ acts on $\mathrm{WD}(R|_{G_{K_{\mathfrak{p}}}})$, which replaces $\kappa_\lambda|_{G_{K_{\mathfrak{p}}}}$. Such a character exists. The action of $I_{\mathfrak{p}}$ on $\mathrm{WD}(R|_{G_{K_{\mathfrak{p}}}})$ has finite image and commutes with the regular monodromy operator, so it is through a scalar character χ. The cube of χ is the restriction to $I_{\mathfrak{p}}$ of $\varepsilon_3^3 \det R$, a character of G_K that is unramified outside $\mathfrak{p}$ and de Rham at $\mathfrak{p}$ with Hodge–Tate weights 0, hence of finite order on $I_{\mathfrak{p}}$, and so of finite order, as K has class number one; it is a character of some ray class group $\mathrm{Cl}_{\mathfrak{p}^n}(K)$, which is a 3-group by the proof of Proposition 11.1. So χ has 3-power order. It is invariant under conjugation by the Weil group of $K_{\mathfrak{p}}$, so it factors through the image of $I_{\mathfrak{p}}$ in $G_{K_{\mathfrak{p}}}^{\mathrm{ab}}$, which is $\mathcal{O}_{\mathfrak{p}}^\times$ by local class field theory, and it extends to a character of $G_{K_{\mathfrak{p}}}$ of the same order. □

Remark 11.22. Each of the last three properties of Proposition 11.21 fails for an irreducible representation with the other three.

(a) *Ramified outside* $\mathfrak{p}$: the restriction to G_K of the symmetric square of H^1 of the elliptic curve 15a1, of conductor 15, is ramified at the inert prime $5\mathcal{O}$, where the curve has multiplicative reduction. It is de Rham at $\mathfrak{p}$ with Hodge–Tate weights $\{0,1,2\}$, and its monodromy operator at $\mathfrak{p}$ is regular, as the curve has multiplicative reduction at 3.

(b) *Other Hodge–Tate weights*: for the newform $f = \eta(z)^6\eta(3z)^6$ of weight 6 on $\Gamma_0(3)$, the restriction to G_K of the symmetric square of the 3-adic representation ρ_f of f has Hodge–Tate weights $\{0,5,10\}$. It is unramified outside $\mathfrak{p}$, and its monodromy operator at $\mathfrak{p}$ is regular: f is new of level 3, with $a_3(f) = 9 = 3^{(6-2)/2}$, so ρ_f is semistable at 3 with nonzero monodromy operator [96].

(c) *Monodromy operator* 0: the curve $y^2 - 3xy + \omega y = x^3$ over K has discriminant $27\omega^2$ and j-invariant $27(-216 - 703\omega)$, so it has good reduction outside $\mathfrak{p}$ and potentially good reduction at $\mathfrak{p}$, and the symmetric square of its H^1 has monodromy operator 0 at $\mathfrak{p}$. It is unramified outside $\mathfrak{p}$, and de Rham at $\mathfrak{p}$ with Hodge–Tate weights $\{0,1,2\}$.

These representations are irreducible. In (a) and (c) the curve has no complex multiplication (15a1 has non-integral j-invariant, and the j-invariant in (c) has no real conjugate, unlike every j-invariant with complex multiplication), so the image of G_K acting on H^1 is open in $\mathrm{GL}_2(\mathbb{Z}_3)$ [100, Chapter IV, §2.2], hence Zariski dense in GL_2, and the symmetric square is irreducible. In (b), ρ_f is irreducible: otherwise its semisimplification would be a sum of two characters unramified outside 3 with Hodge–Tate weights 0 and 5, whose values at Frob_2 have absolute values 1 and 2^5, while $a_2(f) = -6$. So the symmetric square of $\rho_f|_{G_K}$ is semisimple, with regular monodromy operator at $\mathfrak{p}$, hence irreducible, as in the proof of

Proposition 10.7. The following kinds of objects over K fail one of the properties: induced and CM ones have $N = 0$; endoscopic and CAP ones (for $\mathrm{U}(2,1)$) have reducible Galois representations [12, §3.2.3], hence $N^2 = 0$; and symmetric squares of elliptic curves over K with $N^2 \neq 0$, that is, of curves with potentially multiplicative reduction at $\mathfrak{p}$, ramify outside $\mathfrak{p}$ (by [99, Theorem C] and [60, Theorem 1], after a quadratic twist). Moreover, there is no nonzero scalar-valued Picard modular cusp form of weight 3 (the weight of holomorphic 2-forms) for the principal congruence subgroup of level $\sqrt{-3}$ of $\mathrm{SU}(2,1)(\mathbb{Z}[\omega])$, nor, equivalently, for that of $\mathrm{U}(2,1)(\mathbb{Z}[\omega])$ with a power of det as character [18, §2.1 and Proposition 2.2].

Part IV: the equation $x^3 + y^3 = 3z^n$

12. The equation $x^3 + y^3 = 3z^n$

The methods of Parts I, II and III, together with Frey curves and descents on curves of genus one and two, also apply to the equations

$$x^3 + y^3 = 3^k z^n \qquad (k \geq 1),$$

and in particular to $x^3 + y^3 = 3z^n$. A *solution* of $x^3 + y^3 = 3^k z^n$ is a triple (a, b, c) of integers with $\gcd(a, b) = 1$, $c \neq 0$ and $a^3 + b^3 = 3^k c^n$. For $k = 1$ this is the same as a solution in coprime nonzero integers: $a = 0$ would give $\pm 1 = 3c^n$, and a prime dividing a and b divides c. For $k \geq 3$ the condition $\gcd(a, b) = 1$ is stronger than $\gcd(a, b, c) = 1$ (for instance $6^3 + 3^3 = 3^5$), and it is the one we use. From Section 12.2 to Section 12.5, and from Section 12.7 on, the exponent is a prime p.

12.1. **Results.**

Theorem 12.1. *For every integer $n \geq 3$, the equation $x^3 + y^3 = 3z^n$ has no solution in coprime nonzero integers. For $n = 2$ there are solutions, for example $11^3 + (-2)^3 = 3 \cdot 21^2$.*

Theorem 12.1 follows from the cases $k = 1$ of the next three theorems and the classical case $n = 3$. The theorems also treat $x^3 + y^3 = 3^k z^n$ with $k \geq 2$; these cases are used in Corollary 12.17 and in Remarks 12.5 and 12.26.

Theorem 12.2. *Let $p \geq 7$ be a prime and $k \geq 1$ an integer.*

(a) *If $2k - 3$ is not a nonzero square modulo p, then $x^3 + y^3 = 3^k z^p$ has no solution. In particular, for every prime $p \equiv 3 \pmod 4$ with $p \geq 7$, $x^3 + y^3 = 3z^p$ has no solution in coprime nonzero integers.*

(b) *For every prime p with $7 \leq p < 10^8$, $x^3 + y^3 = 3z^p$ has no solution in coprime nonzero integers.*

(c) *For $3 \leq k \leq 7$ and every prime p with $7 \leq p \leq 10^6$, $x^3 + y^3 = 3^k z^p$ has no solution.*

Part (a) is Freitas's symplectic argument [58, §2], applied to the twist by -3 of Kraus's Frey curve; parts (b) and (c) come from a criterion of Kraus's type [80, Théorème 3.1] with an auxiliary prime $q \equiv 1 \pmod p$, checked by computer (Proposition 12.11 and the Supplement, items S14–S16). In part (c), the pairs $(k, p) = (3, 7), (5, 7), (7, 11), (7, 23)$ come from part (a): for them $2k - 3$ is not a nonzero square modulo p, and for $(5, 7)$ and $(7, 11)$ it is divisible by p.

Theorem 12.3.

(a) *If x, y, z are integers with $\gcd(x, y) = 1$ and $x^3 + y^3 = 3z^4$, then $(x, y, z) = \pm(1, -1, 0)$. For every odd $k \geq 1$, $x^3 + y^3 = 3^k z^4$ has no solution.*

(b) *If x, y, z are integers with $\gcd(x, y) = 1$ and $x^3+y^3 = 3z^5$, then $(x, y, z) = \pm(1, -1, 0)$. For every $k \geq 1$ with $k \equiv 1$ or $3 \pmod 5$, $x^3 + y^3 = 3^k z^5$ has no solution.*

(c) *The solutions of $x^3 + y^3 = 9z^5$ are $(2, 1, 1)$, $(1, 2, 1)$, $(-2, -1, -1)$ and $(-1, -2, -1)$. For every $k \geq 7$ with $k \equiv 2 \pmod 5$, $x^3 + y^3 = 3^k z^5$ has no solution.*

The proofs of Theorem 12.3 (Section 12.6) are descents in the manner of Bruin's treatment of $x^3 + y^3 = z^4$ and $x^3 + y^3 = z^5$ [26]: to the elliptic curve $v^2 = u^3 + 27u$ for the exponent 4, and to the curves $y^2 = x^5 - 2^8 \cdot 3^j$ of genus two, $j = 9, 3, 1$, for the exponent 5, where for $j = 1$ we use Chabauty's method at 7.

Theorem 12.4. *Let $p \geq 17$ be a prime and $k \geq 1$ an integer. Then $x^3 + y^3 = 3^k z^p$ has no solution with $3 \mid z$, and no solution at all if $k = 1$ or $k \geq 8$. In particular, for every prime $p \geq 17$, $x^3 + y^3 = 3z^p$ has no solution in coprime nonzero integers.*

For $p \equiv 1 \pmod 3$ the proof of Theorem 12.4 is that of Theorem 11.18; for $p \equiv 2 \pmod 3$ it uses the extension of that proof to an inert prime (Propositions 12.22 and 12.24 and Section 12.10).

Proof of Theorem 12.1. If (a, b, c) is a solution of $x^3 + y^3 = 3z^n$ in coprime nonzero integers and $m \mid n$, then $(a, b, c^{n/m})$ is one of exponent m. Every $n \geq 3$ has a divisor $m \in \{3, 4\}$ or a prime divisor $p \geq 5$. For $m = 3$ there is no solution: the cubic curve $X^3 + Y^3 = 3Z^3$ has only the rational point $(1 : -1 : 0)$. This is classical: the curve is isomorphic to the elliptic curve $y^2 = x^3 - 3888$ (Cremona label 243b2), which has rank 0 and trivial torsion (the Supplement, item S17). The exponents 4 and 5 are Theorem 12.3 (a), (b). The primes $7 \leq p < 10^8$ are Theorem 12.2 (b), the primes $p \equiv 3 \pmod 4$ are Theorem 12.2 (a), and the remaining primes, which are larger than 10^8 and congruent to 1 modulo 4, are Theorem 12.4. Of these, Theorem 12.4 uses Lemma 12.21 only for $p \equiv 2 \pmod 3$, that is, for $p \equiv 5 \pmod{12}$. So Lemma 12.21 is needed only when n is divisible neither by 3 nor by 4 and all its prime factors $p \geq 5$ satisfy $p \equiv 5 \pmod{12}$ and $p > 10^8$. □

Remark 12.5 (what is not settled). For the exponent 4, $x^3 + y^3 = 3^k z^4$ has no solution for k odd (Theorem 12.3 (a)), nor for $k \equiv 0 \pmod 4$, where it reads $x^3 + y^3 = (3^{k/4}z)^4$ and Bruin's theorem [26, Theorem 1] applies. For $k \equiv 2 \pmod 4$ it reads $x^3 + y^3 = 9(3^{(k-2)/4}z)^4$, and the equation $x^3 + y^3 = 9z^4$ remains open. Besides $2^3 + 1^3 = 9 \cdot 1^4$ it has the solution $71^3 + (-23)^3 = 9 \cdot 14^4$. Lemma 12.12 leads to the curve $Y^2 = 4X^4 - 3$, and the map $(X, Y) \mapsto (X/3, Y)$ takes it isomorphically to the curve $C_{4,-1}\colon Y^2 = 324X^4 - 3$ of [26, §3], of rank one.

For the exponent 5 every k is settled (Theorem 12.3 (b), (c), and Corollary 12.17 for $k \equiv 0, 4 \pmod 5$). For prime exponents $p \geq 7$, Remark 12.26 describes what remains; in particular, for $k = 2$ and every prime $p \geq 7$ it is open whether $(2, 1, 1)$, $(1, 2, 1)$ and their negatives are the only solutions.

For $k = 1$ the equation is, to our knowledge, not treated in the literature on twisted sums of two cubes, where the twisting prime is at least 5 [16, 14]. The equations $x^r + y^r = 3z^n$ with $r \in \{5, 7, 13\}$ have been solved for all $n \geq 2$ by Billerey, Chen, Dieulefait and Freitas, with Dembélé for $r = 13$ [22, 21], [24, Theorem 1.2]; Theorem 12.1 is the corresponding result for $r = 3$. The obstruction is the one recalled in Section 1, the identity that [23, Remark 1.7] writes as $2^3 + 1^3 = 3 \cdot 3^1 = 3^2$. For the exponents 4 and 5 the nearest results we know of are Bruin's for the coefficient 1 [26] and, for the coefficient 2, those of Bai and Zhang on $x^3 + y^3 = 2z^{2n}$ with $n \geq 2$ [6] and of Wilcox on $2x^3 + 2y^3 = z^4$ [114, Proposition A.4].

12.2. **Notation, and elementary facts.** Let (a,b,c) be a solution of $x^3+y^3=3^kz^p$ with $p\geq 5$. We write

$$\nu \coloneqq v_3(a^3+b^3)=k+p\,v_3(c), \qquad S\coloneqq a+b, \qquad T\coloneqq \frac{a^2-ab+b^2}{3}.$$

Besides Kraus's Frey curve $E_{a,b}$ and the curve $W=E_{2,1}$ of Section 1 we use the curves

$$E'_{a,b}\colon\ Y^2=X^3-(a-b)X^2+TX, \qquad W'=E'_{2,1}\colon\ Y^2=X^3-X^2+X.$$

The curve $E'_{a,b}$ is the quadratic twist of $E_{a,b}$ by -3, and W', of conductor 24 (Cremona label 24a4), is the twist of W by -3; Freitas denotes these curves E and W [58, §2]. A solution is *normalized* if either a is even, b is odd and $b\equiv 1 \pmod 4$, or a and b are odd and $a\equiv 1 \pmod 4$. Every solution becomes normalized after exchanging a and b, replacing (a,b,c) by $(-a,-b,-c)$, or both (p is odd); each of the first two operations replaces $E_{a,b}$ and $E'_{a,b}$ by their quadratic twists by -1, and the two together leave these curves unchanged.

Lemma 12.6. *Let (a,b,c) be a solution of $x^3+y^3=3^kz^p$ with $p\geq 5$.*

(i) *$ab\neq 0$, $a+b\neq 0$, $3\mid a+b$, $3\nmid ab$ and $\gcd(c,ab)=1$.*
(ii) *$v_3(a^2-ab+b^2)=1$; T is an integer prime to 3 and to $a+b$; $v_3(a+b)=\nu-1$ and $\nu\geq 2$. In particular $3\mid c$ if $k=1$.*
(iii) *$a+b=3^{k-1}c_1^p$ and $T=c_2^p$ with integers c_1,c_2 such that $c=c_1c_2$.*
(iv) *In $\mathcal{O}$, $a+b\omega=(1-\omega)\gamma^p$ for some $\gamma\in\mathcal{O}$, and $\mathrm{N}(\gamma)^p=T$.*

Proof. (i) If $a=0$ then $b=\pm 1$ and $\pm 1=3^kc^p$, which is impossible; $a+b\neq 0$ because $c\neq 0$. Since $a^3+b^3\equiv a+b \pmod 3$, $3\mid a+b$, and then $3\mid a$ would give $3\mid b$. A prime dividing c and a divides b^3. (ii) $a^2-ab+b^2=(a+b)^2-3ab$ with $9\mid(a+b)^2$ and $3\nmid ab$. A prime $\ell\neq 3$ dividing $a+b$ and $3T$ divides $3ab$, hence a and b. So $\nu=v_3(a+b)+1\geq 2$, and for $k=1$ this gives $p\,v_3(c)\geq 1$. (iii) $((a+b)/3^{k-1})\cdot T=c^p$, the two factors are coprime integers, $v_3((a+b)/3^{k-1})=p\,v_3(c)$, $T>0$, and p is odd. (iv) Put $\pi=1-\omega$, so $\pi^2=-3\omega$. In the factorization $a^3+b^3=(a+b)(a+b\omega)(a+b\omega^2)$, the differences $(a+b)-(a+b\omega)=b\pi$ and $\omega(a+b)-(a+b\omega)=-a\pi$, their complex conjugates, and $(a+b\omega)-(a+b\omega^2)=b(\omega-\omega^2)=b\omega\pi$ and $\omega(a+b\omega)-(a+b\omega^2)=a(\omega-1)=-a\pi$ show that a common divisor of two factors divides $\pi\gcd(a,b)=\pi$. Moreover $v_\pi(a+b)=2(\nu-1)\geq 2$ and $a+b\omega=(a+b)-b\pi$, so $v_\pi(a+b\omega)=v_\pi(a+b\omega^2)=1$. Hence $(a+b)/\pi^{2(\nu-1)}$, $(a+b\omega)/\pi$ and $(a+b\omega^2)/\pi$ are pairwise coprime, and their product is a unit times $\big(c/3^{v_3(c)}\big)^p$. As $\mathcal{O}$ is a principal ideal domain whose unit group μ_6 consists of p-th powers ($\gcd(p,6)=1$), $(a+b\omega)/\pi=\gamma^p$ with $\gamma\in\mathcal{O}$. Taking norms, $3T=a^2-ab+b^2=3\,\mathrm{N}(\gamma)^p$. □

Lemma 12.7. *Let (a,b,c) be a solution of $x^3+y^3=3^kz^p$ with $p\geq 5$, and $E'=E'_{a,b}$.*

(a) *E' is an elliptic curve with the rational point $(0,0)$ of order 2; $c_4(E')=-2^4ab$, $\Delta(E')=-2^4\cdot 3^{2k-3}c^{2p}$, and $j(E')=2^83^3a^3b^3/(a^3+b^3)^2$.*
(b) *At a prime $\ell\geq 5$: E' has good reduction if $\ell\nmid c$; if $\ell\mid c$, the model is minimal, the reduction is multiplicative and $v_\ell(\Delta_{\min})=2p\,v_\ell(c)$.*
(c) *At 3: the model is minimal, the reduction is multiplicative, and $v_3(\Delta_{\min})=2\nu-3=2k-3+2p\,v_3(c)\geq 1$.*
(d) *At 2, if a is even and b odd (so that c is odd): the model is minimal, $v_2(\Delta_{\min})=4$, $v_2(j(E'))=8+3v_2(a)>0$, and the Kodaira type and the exponent of the conductor are* II *and 4 if $b\equiv 3 \pmod 4$;* III *and 3 if $b\equiv 1 \pmod 4$ and $v_2(a)=1$;* IV *and 2 if $b\equiv 1 \pmod 4$ and $4\mid a$.*

(e) *At 2, if a and b are odd and $a \equiv 1 \pmod 4$ (so that c is even and $M := v_2(a+b) = p\,v_2(c) \geq 5$): the reduction is multiplicative and $v_2(\Delta_{\min}) = 2M - 8$.*

In particular, for a normalized solution the conductor of E' is $2^e \cdot 3 \cdot \prod_{\ell \mid c,\, \ell \geq 5} \ell$, with $e = 3$ if $v_2(a) = 1$, $e = 2$ if $4 \mid a$, and $e = 1$ if ab is odd.

Proof. (a) These are identities in $\mathbb{Q}(a,b)$; the model of E' is that of the twist of $E_{a,b}$ by -3 (c_4 and c_6 multiplied by $1/9$ and $-1/27$), and $(a^3+b^3)^2/27 = 3^{2k-3}c^{2p}$. (b), (c) If $\ell \geq 5$ divides $\Delta(E')$ then $\ell \mid c$, and then $\ell \nmid c_4(E')$ by Lemma 12.6 (i); likewise $3 \nmid c_4(E')$ and $v_3(\Delta(E')) = 2\nu - 3 \geq 1$. An integral model whose c_4 is a unit at ℓ is minimal at ℓ and has multiplicative reduction there if ℓ divides its discriminant.

(d) Here $a_1 = a_3 = a_6 = 0$, $a_2 = b - a$ and $a_4 = T$ are odd, and $v_2(\Delta) = 4$. The reduction $Y^2 = X^3 + X^2 + X$ is singular at $(1,1)$, and the translation $X = x+1$, $Y = y+1$ gives $y^2 + 2y = x^3 + a_2'x^2 + a_4'x + a_6'$ with $a_2' = a_2 + 3$, $a_4' = a_4 + 2a_2 + 3$ and $a_6' = a_2 + a_4$, all even; as $b_2 = 4a_2'$ is even, the reduction is additive. Tate's algorithm [105, IV.9] stops with type II (exponent $v_2(\Delta) = 4$) if $4 \nmid a_6'$; otherwise with type III (exponent 3) if $a_4' \equiv 2 \pmod 4$, as then $b_8 = 4a_2'a_6' + 4a_2' - a_4'^2 \equiv -a_4'^2 \not\equiv 0 \pmod 8$; and otherwise with type IV (exponent 2), as $b_6 = 4(1 + a_6')$ is not divisible by 8. In particular the model is minimal. As $b^2 \equiv 1 \pmod 8$, $3T \equiv a^2 - ab + 1 \pmod 4$, so $T \equiv 1 \pmod 4$ if $v_2(a) = 1$ and $T \equiv 3 \pmod 4$ if $4 \mid a$. Hence $a_6' \equiv b - 1 \pmod 4$ in both cases, and $a_4' \equiv T + 1 \pmod 4$ is $\equiv 2$ if $v_2(a) = 1$ and $\equiv 0$ if $4 \mid a$.

(e) Here $b \equiv -a \pmod{32}$, $r := (a-b)/2 \equiv a \equiv 1 \pmod 4$, $D := (a+b)^2/12$ is an integer divisible by 2^8, and $X^2 - (a-b)X + T = (X - r)^2 + D$. The substitution $X = 4x + r$, $Y = 8y + 4x$ turns E' into $y^2 + xy = x^3 + \frac{r-1}{4}x^2 + \frac{D}{16}x + \frac{rD}{64}$, an integral model with $c_4 = -ab$ odd and discriminant $\Delta(E')/2^{12}$, of valuation $2M - 8 > 0$. □

12.3. **The elliptic step.**

Lemma 12.8. *Let (a,b,c) be a solution of $x^3 + y^3 = 3^k z^p$ with $p \geq 7$. Then $\bar\rho_{E'_{a,b},p}$ is absolutely irreducible.*

Proof. The representation is odd, so if it is not absolutely irreducible it is reducible over $\mathbb{F}_p$, and $E' = E'_{a,b}$ has a rational subgroup of order p; with the point $(0,0)$ it has a rational cyclic subgroup of order $2p$. By the theorems of Mazur [84] and Kenku [75], for a prime $p \geq 7$ an elliptic curve over $\mathbb{Q}$ with rational isogenies of degrees 2 and p exists only for $p = 7$, and then $j \in \{-15^3, 255^3\}$ (the two noncuspidal rational points of $X_0(14)$). But $v_3(j(E')) = 3 - 2\nu < 0$ by Lemma 12.7 (a) and Lemma 12.6 (ii), so $j(E')$ is not an integer. □

Theorem 12.9. *Let $p \geq 7$ be a prime, $k \geq 1$, and (a,b,c) a normalized solution of $x^3 + y^3 = 3^k z^p$. Then:*

(i) *$p \nmid 2k - 3$;*
(ii) *c is odd, a is even with $v_2(a) = 1$, and $b \equiv 1 \pmod 4$;*
(iii) *$\bar\rho_{E'_{a,b},p} \cong \bar\rho_{W',p}$, equivalently $\bar\rho_{E_{a,b},p} \cong \bar\rho_{W,p}$;*
(iv) *$p \nmid c$;*
(v) *if $p \neq 7$, then $7 \nmid abc$ and $a^3 \equiv b^3 \pmod 7$.*

Statements (i), (iv) *and* (v) *hold for every solution, since they do not change under the operations that normalize it.*

Proof. The curve $E' = E'_{a,b}$ is modular [25] and $\bar\rho_{E',p}$ is irreducible (Lemma 12.8). Let N be the conductor of E'. By Ribet's level-lowering theorem [94], $\bar\rho_{E',p}$ is isomorphic to the

mod p representation of a newform of weight 2 and level dividing $N' = N/\prod \ell$, the product over the primes ℓ exactly dividing N with $p \mid v_\ell(\Delta_{\min})$. We use the theorem in this complete form, valid for $p \geq 3$ (see [95]), as do [80, 58]. By Lemma 12.7, every prime $\ell \geq 5$ dividing N is removed, 3 is removed exactly when $p \mid 2k-3$, and 2 is never removed (in case (e) of that lemma, $v_2(\Delta_{\min}) = 2p\, v_2(c) - 8$ is prime to p). So $N' = 2^e 3^\delta$ with $e \in \{1,2,3\}$ as in Lemma 12.7, and $\delta = 0$ if $p \mid 2k-3$, $\delta = 1$ otherwise. There is no cusp form of weight 2 on $\Gamma_0(M)$ for any proper divisor M of 24, and $S_2(\Gamma_0(24))$ is spanned by the newform of W': these spaces have dimension equal to the genus of $X_0(M)$, which is 0 for the proper divisors M of 24 and 1 for $M = 24$ [46, §3.1 and Theorem 3.5.1]. Hence $\delta = 1$ and $e = 3$, which gives (i) and (ii), and $\bar\rho_{E',p} \cong \bar\rho_{W',p}$, both being semisimple with the same traces of Frobenius. Twisting by -3 gives the statement for $E_{a,b}$ and W.

(iv) Suppose $p \mid c$. Then E' has multiplicative reduction at p, and the semisimplification of $\bar\rho_{E',p}|_{G_{\mathbb{Q}_p}}$ is $\phi\bar\varepsilon_p \oplus \phi$ with ϕ unramified and $\phi^2 = 1$ (Tate curve). The curve W' has good reduction at p. If it were supersingular, $\bar\rho_{W',p}|_{I_p}$ would be the sum of the two fundamental characters of level 2 [102, Proposition 12], not $\bar\varepsilon_p \oplus 1$. So it is ordinary, $\bar\rho_{W',p}|_{G_{\mathbb{Q}_p}}$ has semisimplification $\lambda^{-1}\bar\varepsilon_p \oplus \lambda$ with λ unramified and $\lambda(\mathrm{Frob}_p) \equiv a_p(W') \pmod p$, and comparing the unramified constituents gives $a_p(W') \equiv \pm 1 \pmod p$. But $a_p(W')$ is even (W' has a rational point of order 2), so $a_p(W') \mp 1$ is odd, nonzero, and of absolute value at most $2\sqrt{p} + 1 < p$. Hence $p \nmid a_p(W') \mp 1$, a contradiction.

(v) If $7 \mid c$, then E' has multiplicative reduction at 7, $\bar\rho_{E',p}$ is unramified at 7 (p divides $v_7(\Delta_{\min})$) with trace of Frob_7 equal to ± 8, while $a_7(W') = 0$; so $p \mid 8$, which is false. So $7 \nmid c$, E' has good reduction at 7 and $a_7(E') \equiv a_7(W') = 0 \pmod p$; as $|a_7(E')| \leq 5 < p$, $a_7(E') = 0$, and E' is supersingular at 7, that is $j(E') \equiv 1728 \equiv 6 \pmod 7$. As $2^8 3^3 \equiv 3 \pmod 7$, this reads $3a^3b^3 \equiv 6(a^3+b^3)^2 \pmod 7$ with $a^3, b^3 \in \{0, \pm 1\}$, not both 0 and with $a^3 + b^3 \not\equiv 0$ ($7 \nmid c$); the only possibility is $a^3 \equiv b^3 \equiv \pm 1$. □

Remark 12.10. (1) For $k = 1$ this is the analogue for the coefficient 3 of Kraus's [80, Théorème 6.1, Proposition 6.3], with two simplifications: $3 \mid c$ is elementary (Lemma 12.6 (ii)), and the newform of level 36 with complex multiplication does not occur, because the twisted curve E' is multiplicative at 3, so that the possible levels are the divisors $2^e 3^\delta$ of 24. (2) For a solution that is not normalized, $\bar\rho_{E'_{a,b},p}$ is isomorphic to $\bar\rho_{W',p}$ or to the representation of the twist of W' by -1, and both occur: for $k = 2$, $(-1,-2,-1)$ gives $E' = W'$, and $(1,2,1)$ gives the twist of W' by -1, of conductor 48, whose trace of Frob_{11} is -4, while $a_{11}(W') = 4$.

12.4. **The symplectic argument.** Let E_1, E_2 be elliptic curves over a field of characteristic prime to p. An isomorphism $\phi\colon E_1[p] \to E_2[p]$ of Galois modules is *symplectic* if it multiplies the Weil pairing by a square of $\mathbb{F}_p^\times$, and *anti-symplectic* if it multiplies it by a non-square [58, §3]. We use two criteria, in the form in which Freitas and Kraus state them [59].

At 2 [58, Theorem 4 and Lemma 1] (= [59, Theorem 7]): let E_1, E_2 be elliptic curves over $\mathbb{Q}_2$ with potentially good reduction, with the same inertial field L, and with $\mathrm{Gal}(L/\mathbb{Q}_2^{\mathrm{nr}}) \cong \mathrm{SL}_2(\mathbb{F}_3)$; let $p \geq 3$. Then $E_1[p] \cong E_2[p]$ as modules over the inertia group I_2; if $\left(\frac{2}{p}\right) = 1$ they are symplectically isomorphic I_2-modules; if $\left(\frac{2}{p}\right) = -1$ they are symplectically isomorphic if and only if $v_2(\Delta_{\min}(E_1)) \equiv v_2(\Delta_{\min}(E_2)) \pmod 3$; and they are not both symplectically and anti-symplectically isomorphic.

At a prime $\ell \neq p$ of multiplicative reduction [81, Proposition 2] (= [59, Theorem 13]): let $p \geq 3$, and let E_1, E_2 be elliptic curves over $\mathbb{Q}_\ell$ with multiplicative reduction and $E_1[p] \cong E_2[p]$ as $G_{\mathbb{Q}_\ell}$-modules, with $p \nmid v_\ell(\Delta_{\min}(E_1))$. Then $p \nmid v_\ell(\Delta_{\min}(E_2))$, and $E_1[p]$,

$E_2[p]$ are symplectically isomorphic if and only if $v_\ell(\Delta_{\min}(E_1))/v_\ell(\Delta_{\min}(E_2))$ is a square modulo p; they are not both symplectically and anti-symplectically isomorphic.

Proof of Theorem 12.2 (a). Let (a,b,c) be a normalized solution. By Theorem 12.9, $p\nmid 2k-3$, $v_2(a)=1$, c is odd, and there is an isomorphism $\phi\colon E'[p]\to W'[p]$ of $G_{\mathbb{Q}}$-modules, where $E'=E'_{a,b}$.

At 2. E' and W' have potentially good reduction at 2 ($v_2(j(E'))=11$ and $j(W')=2048/3$), and, because of ϕ, the same inertial field $L=\mathbb{Q}_2^{\mathrm{nr}}(E'[p])=\mathbb{Q}_2^{\mathrm{nr}}(W'[p])$; and $\mathrm{Gal}(L/\mathbb{Q}_2^{\mathrm{nr}})\cong \mathrm{SL}_2(\mathbb{F}_3)$ because $v_2(\Delta_{\min}(W'))=4$ and $v_2(c_4(W'))=5$ [58, §2]. As $v_2(\Delta_{\min}(E'))=4=v_2(\Delta_{\min}(W'))$ (Lemma 12.7 (d)), the criterion at 2 shows that $E'[p]$ and $W'[p]$ are symplectically, and not anti-symplectically, isomorphic I_2-modules. So ϕ, an isomorphism of I_2-modules, is symplectic.

At 3. E' and W' have multiplicative reduction at 3, with $v_3(\Delta_{\min}(W'))=1$ and $v_3(\Delta_{\min}(E'))=2k-3+2p\,v_3(c)$ (Lemma 12.7 (c)). By the criterion at $\ell=3$, ϕ is symplectic if and only if $2k-3$ is a square modulo p.

So $2k-3$ is a nonzero square modulo p. For $k=1$, $2k-3=-1$, which is a square modulo p if and only if $p\equiv 1 \pmod 4$. □

This is Freitas's proof of [58, Theorem 3], with $v_3(\Delta_{\min})=2k-3+2p\,v_3(c)$ in place of $-3+2p\,v_3(c)$; the value $k=0$ gives his conclusion that a solution forces $\left(\frac{-3}{p}\right)=1$.

12.5. **A criterion with an auxiliary prime.** For a prime q and an elliptic curve E over $\mathbb{F}_q$ write $a_q(E)=q+1-\#E(\mathbb{F}_q)$, and for $n\mid q-1$ let $\mu_n(\mathbb{F}_q)$ be the group of n-th roots of unity in $\mathbb{F}_q^\times$.

Proposition 12.11. *Let $p\geq 7$ be a prime, $k\geq 1$, and $q=np+1$ a prime. Suppose*

(A) $a_q(W)^2\not\equiv 4 \pmod p$, *and*

(B_k) *for every ζ in the coset $9^{1-k}\mu_n(\mathbb{F}_q)$ such that $d_2:=(12\zeta-1)/3$ is a square in $\mathbb{F}_q$ (0 allowed), and one square root d of d_2, the curve*

$$E_\zeta\colon\ Y^2=X^3+(1-3\zeta)X+\tfrac{d(2+3\zeta)}{3}$$

over $\mathbb{F}_q$ satisfies $a_q(E_\zeta)^2\not\equiv a_q(W)^2 \pmod p$.

Then $x^3+y^3=3^kz^p$ has no solution. If moreover $q\equiv 1 \pmod 3$ and $r\in\mathbb{F}_q$ is a primitive cube root of unity, it suffices to require (B_k) for those ζ for which, in addition,

$$X_1:=\frac{(1-d)+(1+d)r}{2(1-r)}\in 3^{1-k}\mu_n(\mathbb{F}_q);$$

whether this holds is independent of the choices of d and r. We call these two sufficient conditions the first form *and the* refined form *of the criterion.*

Proof. If $p\mid 2k-3$ there is no solution (Theorem 12.9 (i)). Otherwise let (a,b,c) be a normalized solution, so that $\bar\rho_{E,p}\cong\bar\rho_{W,p}$ with $E=E_{a,b}$ (Theorem 12.9 (iii)). Here n is even and $q\nmid 6p$. If $q\mid c$, then E has multiplicative reduction at q with $v_q(\Delta_{\min})=2p\,v_q(c)$, so $\bar\rho_{E,p}$ is unramified at q and the trace of Frob_q is $\pm(q+1)\equiv\pm 2 \pmod p$; it equals $a_q(W)$ modulo p, against (A). So $q\nmid c$, E has good reduction at q, and $a_q(E)\equiv a_q(W) \pmod p$. As $\mathbb{F}_q^\times$ is cyclic of order np, $(\mathbb{F}_q^\times)^p=\mu_n(\mathbb{F}_q)$; by Lemma 12.6 (iii) the reductions $\bar S$ of $S=a+b$ and $\bar T$ of T lie in $3^{k-1}\mu_n(\mathbb{F}_q)$ and in $\mu_n(\mathbb{F}_q)$. Put $\zeta=\bar T/\bar S^2\in 9^{1-k}\mu_n(\mathbb{F}_q)$ and $a'=a/\bar S$, $b'=b/\bar S$ in $\mathbb{F}_q$. Then $a'+b'=1$, $3a'b'=1-3\zeta$, $(b'-a')^2=(12\zeta-1)/3$ and $b'^3-a'^3=(b'-a')(2+3\zeta)/3$, so the curve $E_{a',b'}$ is E_ζ with $d=b'-a'$; it is nonsingular, of

discriminant $-2^4 3^3 (3\zeta)^2$, and the other square root $-d$ gives $E_{b',a'}$, its twist by -1. The reduction of E modulo q is the twist of $E_{a',b'}$ by $\bar{S}$, and a quadratic twist changes a_q at most by a sign. So $a_q(E_\zeta)^2 \equiv a_q(W)^2 \pmod p$, against (B_k).

Now let $q \equiv 1 \pmod 3$, and let $\mathfrak{q}$ be the prime of $\mathcal{O}$ above q at which $\omega \equiv r$. By Lemma 12.6 (iv), $a + br = (1-r)g^p$ in $\mathbb{F}_q$, where g is the reduction of γ modulo $\mathfrak{q}$; and $g \neq 0$ because $\mathrm{N}(\gamma)^p = T$ is prime to q. So $(a+br)/(1-r) \in \mu_n(\mathbb{F}_q)$ and $X_1 = (a'+b'r)/(1-r) = (a+br)/((1-r)\bar{S}) \in 3^{1-k}\mu_n(\mathbb{F}_q)$, where $a' = (1-d)/2$ and $b' = (1+d)/2$. Put $X_2 = (a' + b'r^2)/(1-r^2)$. Then $X_1 X_2 = \zeta$ (as $(1-r)(1-r^2) = 3$); replacing d by $-d$ exchanges a' and b' and replaces X_1 by $-X_2$ (because $b' + a'r = r(a' + b'r^2)$ and $r/(1-r) = -1/(1-r^2)$); and replacing r by r^2 exchanges X_1 and X_2. As $-1 \in \mu_n(\mathbb{F}_q)$ and $\zeta \in 9^{1-k}\mu_n(\mathbb{F}_q)$, the condition $X_1 \in 3^{1-k}\mu_n(\mathbb{F}_q)$ is independent of the choices. □

Proof of Theorem 12.2 (b) and (c). (b) By the computation of the Supplement, item S14 (summarized in Appendix A), for every prime p with $7 \leq p < 10^8$ and $p \neq 13$ there is an even $n \leq 284$ such that $q = np + 1$ is prime and (A) and (B_1) hold. For $p = 13$ no $n \leq 600$ has this property, but the refined form holds with $n = 6$, $q = 79$: $a_{79}(W) = -8$, so $a_{79}(W)^2 - 4 = 60 \not\equiv 0 \pmod{13}$; $\mu_6(\mathbb{F}_{79}) = \{1, 23, 24, 55, 56, 78\}$; $d_2 = (12\zeta - 1)/3$ is a non-square for $\zeta = 1, 23, 24$ and the square of 3, 31, 38 for $\zeta = 55, 56, 78$; with $r = 23$ and $d = 3, 31, 38$ one finds $X_1 = 59, 45, 2$, whose sixth powers are $46, 22, 64 \neq 1$. So no ζ has to be tested, and there is no solution for $p = 13$ (the Supplement, item S15).

(c) By the computation of the Supplement, item S16, for $3 \leq k \leq 7$ and every prime $7 \leq p \leq 10^6$ the first form of Proposition 12.11 holds with some even $n \leq 2000$, except for $(k,p) = (3,7), (5,7), (7,11), (7,23), (6,7), (6,13)$. For each k the search covers the primes $7 \leq p \leq 10^6$ (78 495 of them), except, for $k = 5$ and $k = 7$, the prime dividing $2k - 3$. In the first four cases $2k - 3$ is 3, 7, 11, 11, which is not a nonzero square modulo p (3 is not a square modulo 7, $7 \mid 7$, $11 \mid 11$, and 11 is not a square modulo 23), and Theorem 12.2 (a) applies. In the last two the refined form holds with $n = 6$ and $q = 43$, respectively $q = 79$ (item S16). □

12.6. **The exponents 4 and 5.**

Lemma 12.12. *Let $n \geq 2$ and $k \geq 1$ be integers, and let x, y, z be integers with $\gcd(x,y) = 1$, $z \neq 0$ and $x^3 + y^3 = 3^k z^n$. Then there are integers $c \neq 0$ and $b \geq 1$ with $3 \nmid b$ and $\gcd(b,c) = 1$ such that*

$$x + y = 3^{k-1}c^n, \qquad x^2 - xy + y^2 = 3b^n,$$

and $(X,Y) = (b/c^2, (x-y)/c^n)$ is a rational point of $Y^2 = 4X^n - 3^{2k-3}$. If $k = 1$, then $3 \mid c$ and $3 \mid z$.

Proof. As in the proof of Lemma 12.6 (i), (ii), whose arguments do not use that the exponent is prime: $3 \mid x + y$, $3 \nmid xy$, $v_3(x^2 - xy + y^2) = 1$, $T = (x^2 - xy + y^2)/3$ is a positive integer prime to 3 and to $x + y$, and $v_3(x+y) = k - 1 + n\, v_3(z)$. So $A = (x+y)/3^{k-1}$ and T are coprime integers with $AT = z^n$. Hence $T = b^n$ with $b \geq 1$, and $A = c^n$ with $c \in \mathbb{Z}$: for n even $A = z^n/T > 0$, and for n odd the sign goes into c; and $c \neq 0$ because $z \neq 0$. If $k = 1$ then $v_3(c^n) = v_3(x+y) \geq 1$, so $3 \mid c$, and $3 \mid z$ because $n\, v_3(z) = v_3(x+y) \geq 1$. Finally $4(x^2 - xy + y^2) = (x+y)^2 + 3(x-y)^2$ gives $12b^n = 3^{2k-2}c^{2n} + 3(x-y)^2$, and we divide by $3c^{2n}$. (For $n = p \geq 5$ prime, c and b are the integers c_1 and c_2 of Lemma 12.6 (iii); in the rest of this subsection, except in the case $k = 0$ of the proof of Corollary 12.17, b and c have the meaning given here.) □

We shall move between the curves $Y^2 = 4X^n - 3^j$ by the following maps, which send rational points to rational points and affine points to affine points: for $m \in \mathbb{Z}$, $(X, Y) \mapsto (X/3^{2m}, Y/3^{nm})$ goes from $Y^2 = 4X^n - 3^j$ to $Y^2 = 4X^n - 3^{j-2nm}$; for $n = 4$, $(X, Y) \mapsto (X/3^m, Y/3^{2m})$ goes to $Y^2 = 4X^4 - 3^{j-4m}$; and $(X, Y) \mapsto (4X, 16Y)$ goes from $Y^2 = 4X^5 - 3^j$ to the curve

$$\Gamma_j\colon\ y^2 = x^5 - 2^8 \cdot 3^j.$$

So for $n = 5$ only $j = (2k - 3) \bmod 10 \in \{1, 3, 5, 7, 9\}$ matters, and for $n = 4$ only $(2k - 3) \bmod 4$.

The exponent 4.

Proof of Theorem 12.3 (a). If $z = 0$ then $y = -x$ and $|x| = \gcd(x, y) = 1$. Let $z \neq 0$ and k odd. Then $2k - 3 \equiv 3 \pmod 4$, and Lemma 12.12 with the maps above gives an affine rational point of

$$H\colon\ Y^2 = 4X^4 - 3^7.$$

At such a point $Y + 2X^2 \neq 0$ (otherwise $Y^2 - 4X^4 = 0$), so we may put $u = (Y + 2X^2)/9$ and $v = 2X(Y + 2X^2)/27$. From $(Y - 2X^2)(Y + 2X^2) = -3^7$ we get $Y - 2X^2 = -3^5/u$, hence $4X^2 = 9u + 3^5/u$, and $v^2 = 4X^2(Y + 2X^2)^2/27^2 = u^3 + 27u$. So the elliptic curve

$$E\colon\ v^2 = u^3 + 27u$$

has a rational point with $u \neq 0$. We show that $E(\mathbb{Q}) = \{O, (0, 0)\}$, which is a contradiction.

Torsion. As 27 is not divisible by a fourth power, is not 4, and -27 is not a square, $E(\mathbb{Q})_{\text{tors}} = \{O, (0, 0)\}$ [106, Proposition X.6.1(a)].

Rank. We use the descent by the 2-isogeny $\phi\colon E \to \hat{E}$, $\hat{E}\colon y^2 = x^3 - 108x$ [106, X.4.9]. With the maps $\alpha\colon E(\mathbb{Q}) \to \mathbb{Q}^\times/\mathbb{Q}^{\times 2}$ and $\alpha'\colon \hat{E}(\mathbb{Q}) \to \mathbb{Q}^\times/\mathbb{Q}^{\times 2}$ defined there, $\operatorname{rank} E(\mathbb{Q}) = \log_2\bigl(|\alpha(E(\mathbb{Q}))| \cdot |\alpha'(\hat{E}(\mathbb{Q}))|/4\bigr)$ [107, Chapter III, §6]. The image of α lies in $\{\pm 1, \pm 3\}$ and contains 1 and $\alpha(0, 0) = 27 \equiv 3$; a class d lies in it only if $N^2 = dM^4 + (27/d)e^4$ has a rational solution with $(M, e) \neq (0, 0)$, and for $d = -1, -3$ the right side is negative. So $|\alpha(E(\mathbb{Q}))| = 2$. The image of α' lies in $\{\pm 1, \pm 2, \pm 3, \pm 6\}$ and contains 1 and $\alpha'(0, 0) = -108 \equiv -3$; a class d lies in it only if $N^2 = dM^4 - (108/d)e^4$ has a solution in every completion of $\mathbb{Q}$ with $(M, e) \neq (0, 0)$, and we may take (M, e) primitive. For $d = -1$ and $d = 2$ there is no solution in $\mathbb{Q}_3$: if $3 \nmid M$ the right side is $\equiv d \equiv 2 \pmod 3$; if $3 \mid M$ then $3 \nmid e$ and the right side has 3-adic valuation 3. For $d = -2$ there is no solution in $\mathbb{Q}_2$: the right side is $2(27e^4 - M^4)$; if exactly one of M, e is even it has 2-adic valuation 1, and if both are odd, $27e^4 - M^4 \equiv 10 \pmod{16}$ and the right side is $4w$ with $w \equiv 5 \pmod 8$. As the image is a group containing -3, it contains neither -1 nor 3, neither 2 nor -6, and neither -2 nor 6; so $|\alpha'(\hat{E}(\mathbb{Q}))| = 2$, and $\operatorname{rank} E(\mathbb{Q}) = 0$. Item S18 of the Supplement checks these local conditions by exhaustion. □

The map $(X, Y) \mapsto (X/3, Y/9)$ is an isomorphism from H to the curve $C_{4,1}\colon Y^2 = 4X^4 - 27$ of [26, §§2–3], one of the three curves of genus one to which Bruin's descent reduces $x^3 + y^3 = z^4$; Bruin notes that the other two, $C_{4,-1}$ and $C_{4,0}$, have rank one, and treats that equation through curves of higher genus. The proof above shows that $C_{4,1}$ has no affine rational point.

The exponent 5: a 2-descent. Let $j \in \{1,3,5,7,9\}$, $f(x) = x^5 - A$ with $A = 2^8 \cdot 3^j$, J_j the Jacobian of Γ_j (which has one point ∞ at infinity), $L = \mathbb{Q}[T]/(f(T))$ and θ the class of T. We use the 2-descent on Jacobians of curves $y^2 = f(x)$ with f of odd degree [98, 108] (see also [29, Chapter 6]). For a field $F \supseteq \mathbb{Q}$, the map that sends the class of $P_1 + \cdots + P_r - r\infty$ (the P_i affine with $y(P_i) \neq 0$) to $\prod_i (x(P_i) - \theta)$ induces an injective homomorphism $J_j(F)/2J_j(F) \to (L \otimes F)^\times/(L \otimes F)^{\times 2}$, with image in the kernel of the norm to $F^\times/F^{\times 2}$. For a place v of $\mathbb{Q}$ let $\mathcal{I}_v$ be the image for $F = \mathbb{Q}_v$. Then $\dim_{\mathbb{F}_2} \mathcal{I}_v = \dim J_j(\mathbb{Q}_v)[2]$ for v odd, $\dim \mathcal{I}_2 = \dim J_j(\mathbb{Q}_2)[2] + 2$ and $\dim \mathcal{I}_\infty = \dim J_j(\mathbb{R})[2] - 2$, where $\dim J_j(\mathbb{Q}_v)[2]$ is the number of irreducible factors of f over $\mathbb{Q}_v$ minus one. At an odd prime of good reduction $\mathcal{I}_v$ is the unramified subgroup. The Selmer group

$$\mathrm{Sel}^2(J_j/\mathbb{Q}) = \{\delta \in L^\times/L^{\times 2} : \ \mathrm{N}(\delta) \in \mathbb{Q}^{\times 2},\ \delta \in \mathcal{I}_v \text{ in } (L \otimes \mathbb{Q}_v)^\times/(L \otimes \mathbb{Q}_v)^{\times 2} \text{ for all } v\}$$

contains the image of $J_j(\mathbb{Q})/2J_j(\mathbb{Q})$. The torsion subgroup $J_j(\mathbb{Q})_{\mathrm{tors}}$ injects into $J_j(\mathbb{F}_\ell)$ for every odd prime ℓ of good reduction, that is $\ell \nmid 30$ [73, Appendix].

Proposition 12.13. *For $j = 9$ and $j = 3$, $\mathrm{Sel}^2(J_j/\mathbb{Q}) = 0$ and $J_j(\mathbb{Q}) = 0$. Hence $\Gamma_9(\mathbb{Q}) = \Gamma_3(\mathbb{Q}) = \{\infty\}$.*

Proof. $j = 9$. Here $L = \mathbb{Q}(\eta)$ with $\eta^5 = 12$ and $\theta = 3\eta^4$; its discriminant is $2^4 \cdot 3^4 \cdot 5^5$, and 2, 3, 5 are totally ramified in L. The polynomial f is irreducible over $\mathbb{Q}_2$ and $\mathbb{Q}_3$ (its Newton polygons have one slope, 8/5 and 9/5) and over $\mathbb{Q}_5$ ($A \equiv 23 \pmod{25}$ is not a fifth power in $\mathbb{Q}_5$, since the fifth powers of 5-adic units are $\equiv \pm 1, \pm 7 \pmod{25}$), and it has one real root. Hence $\mathcal{I}_3 = \mathcal{I}_5 = \mathcal{I}_\infty = 0$ and $\dim \mathcal{I}_2 = 2$: an element of the Selmer group is a square at the primes above 3 and 5 and positive at the real place of L, and it has even valuation at every prime of L not above 2. The class group of L is trivial: the Minkowski bound is below 125.3, and each of the 29 prime ideals of norm at most 125 is principal, with an explicit generator. The units $\varepsilon_1 = \frac{1}{2}\eta^4 - \frac{5}{2}\eta^3 + 3\eta^2 - 5\eta - 1$ and $\varepsilon_2 = -\frac{1}{2}\eta^4 + 2\eta^3 - 4\eta^2 + 4\eta - 1$ have norm -1, and no product of a nonempty subset of $\{-1, \varepsilon_1, \varepsilon_2\}$ is a square in L; since a subgroup $V \ni -1$ of finite index in $\mathcal{O}_L^\times$ has odd index if and only if $V \cap \mathcal{O}_L^{\times 2} = V^2$, the elements $-1, \varepsilon_1, \varepsilon_2$ span $\mathcal{O}_L^\times/\mathcal{O}_L^{\times 2}$. Finally $2\mathcal{O}_L = \mathfrak{p}_2^5$ with $\mathfrak{p}_2 = (\pi_2)$, $\pi_2 = \frac{1}{2}\eta^4 + \frac{1}{2}\eta^3 + \eta^2 + 2\eta + 2$. So the classes with even valuation away from 2 form the $\mathbb{F}_2$-space with basis $-1, \varepsilon_1, \varepsilon_2, \pi_2$. Of its sixteen elements, exactly 1, $-\varepsilon_1$, $-\varepsilon_2$, $\varepsilon_1\varepsilon_2$ have square norm, are positive at the real place and are squares at the primes above 3 and 5. The group $\mathcal{I}_2$ is spanned by the images of the points of $\Gamma_9(\mathbb{Q}_2)$ with $x = -199$ and $x = -196$, and it contains none of $-\varepsilon_1, -\varepsilon_2, \varepsilon_1\varepsilon_2$. So $\mathrm{Sel}^2(J_9/\mathbb{Q}) = 0$ and $J_9(\mathbb{Q})$ is finite of odd order. As $\#J_9(\mathbb{F}_7) = 50$ and $\#J_9(\mathbb{F}_{41}) = 2131$ are coprime, $J_9(\mathbb{Q}) = 0$.

$j = 3$. Here $L = \mathbb{Q}(\xi)$ with $\xi^5 = 6$ and $\theta = 2\xi^3$, again of discriminant $2^4 \cdot 3^4 \cdot 5^5$; f is irreducible over $\mathbb{Q}_2$, $\mathbb{Q}_3$ (slopes 8/5, 3/5) and $\mathbb{Q}_5$ ($A \equiv 12 \pmod{25}$), with one real root. The same computation applies: the class group is trivial (each of the 34 prime ideals of norm at most 125 is principal, with an explicit generator), -1 and two units of norm 1 span $\mathcal{O}_L^\times/\mathcal{O}_L^{\times 2}$, $2\mathcal{O}_L = (\pi_2)^5$ with $\pi_2 = -2 + \xi - \xi^2$, four of the sixteen classes pass the conditions at the norm, the real place, 3 and 5, and only the trivial one lies in $\mathcal{I}_2$, which is spanned by the images of the points of $\Gamma_3(\mathbb{Q}_2)$ with $x = -199$ and $x = -196$. So $\mathrm{Sel}^2(J_3/\mathbb{Q}) = 0$; and $\#J_3(\mathbb{F}_7) = 50$, $\#J_3(\mathbb{F}_{11}) = 41$ give $J_3(\mathbb{Q}) = 0$.

In both cases $P \mapsto [P - \infty]$ embeds $\Gamma_j(\mathbb{Q})$ in $J_j(\mathbb{Q}) = 0$. The computations in the fields L and in the groups $J_j(\mathbb{F}_\ell)$ are items S19 and S20 of the Supplement. □

Proof of Theorem 12.3 (b). If $z = 0$ then $(x, y, z) = \pm(1, -1, 0)$. Let $z \neq 0$ and $k \equiv 1$ or $3 \pmod 5$. Then $(2k - 3) \bmod 10$ is 9 or 3, and Lemma 12.12 with the maps above gives an affine rational point of Γ_9 or Γ_3, which Proposition 12.13 excludes. □

The curves Γ_7, Γ_5 and Γ_3 are the curves C_1, C_2 and C_3 of [26, §4], which arise there from $x^3 + y^3 = z^5$. Bruin shows that C_3 has only its point at infinity, and the proof above for Γ_3 is independent of his. The curves Γ_9 and Γ_1 do not occur in [26].

The exponent 5 with the coefficient 9. For $k \equiv 2 \pmod 5$ the curve is $\Gamma_1\colon y^2 = x^5 - 768$, which has the rational points $(4, \pm 16)$, coming from $2^3 + 1^3 = 9 \cdot 1^5$. Write $J = J_1$, $D = [(4, 16) - \infty] \in J(\mathbb{Q})$, and let ι be the hyperelliptic involution.

Proposition 12.14. $\Gamma_1(\mathbb{Q}) = \{\infty, (4, 16), (4, -16)\}$.

Proof. Step 1: $J(\mathbb{Q})$ is infinite cyclic. Here $L = \mathbb{Q}(768^{1/5}) = \mathbb{Q}(18^{1/5})$, of discriminant $2^4 \cdot 3^4 \cdot 5^3$ and signature $(1, 2)$; its class group is trivial (Minkowski bound below 25.1; every prime ideal of norm at most 25 has an explicit generator). Over $\mathbb{Q}_2$ and $\mathbb{Q}_3$, $f = x^5 - 768$ is irreducible. Over $\mathbb{Q}_5$ it has a root ($768 \equiv 3^5 \pmod{25}$) and an irreducible factor of degree 4, and it has one real root. So $\mathcal{I}_3 = \mathcal{I}_\infty = 0$, $\dim \mathcal{I}_2 = 2$ and $\dim \mathcal{I}_5 = 1$, and the Selmer group lies in the group of classes with even valuation at every prime not above 2, 3 or 5, of dimension 7 over $\mathbb{F}_2$ (generated by -1, two units and generators of the primes above 2, 3 and of the two primes above 5). The group $\mathcal{I}_2$ is spanned by the images of the points of $\Gamma_1(\mathbb{Q}_2)$ with $x = -300/7$ and $x = -299/5$, and $\mathcal{I}_5$ by the image of the point of $\Gamma_1(\mathbb{Q}_5)$ with $x = -299/2$. These local conditions leave a Selmer group of dimension 1, whose nonzero element is the image of the point D' of Step 2. As f is irreducible over $\mathbb{Q}$, $J(\mathbb{Q})[2] = 0$, so $J(\mathbb{Q})$ has rank at most 1. The orders $\#J(\mathbb{F}_\ell)$, $7 \leq \ell \leq 71$, have greatest common divisor 1, so $J(\mathbb{Q})_{\mathrm{tors}} = 0$; as $D \neq 0$, $J(\mathbb{Q}) = \mathbb{Z}G$ for a generator G.

Step 2: a half of D. Let $Q_{1,2} = (\pm 4i, 16 \pm 32i)$ and $D' = [Q_1 + Q_2 - 2\infty] \in J(\mathbb{Q})$, the class of the Mumford pair $(x^2 + 16,\ 8x + 16)$; it is rational because $f - (8x + 16)^2 = (x^2 + 16)(x^3 - 16x - 64)$. With $q = -2x^2 + 8x - 16$ one has $f - q^2 = (x - 4)(x^2 + 16)^2$, and $q(\pm 4i) = 16 \pm 32i \neq 0$, so the function $y - q(x)$ has divisor $2Q_1 + 2Q_2 + (4, -16) - 5\infty$. Hence $2D' = -[(4, -16) - \infty] = D$. Write $D' = mG$. The image of D' under the descent map is the class of $\theta^2 + 16$, which is not a square in L: at the prime of degree one above 17 at which $\theta \equiv 12$, it reduces to 7, a non-square modulo 17. So $D' \notin 2J(\mathbb{Q})$ and m is odd. Further $\#J(\mathbb{F}_7) = 50$, and the reduction $\bar{D}'$ has order 25, so the 5-primary part of $J(\mathbb{F}_7)$ is cyclic, generated by $\bar{D}'$, and $\bar{D}' \notin 5J(\mathbb{F}_7)$; hence $5 \nmid m$.

Step 3: sieving. The image of $J(\mathbb{Q})$ in $J(\mathbb{F}_7)$ is $\langle \bar{G} \rangle = \langle \bar{D}' \rangle$, of order 25, as $\gcd(m, 50) = 1$. The points of $\Gamma_1(\mathbb{F}_7)$ are ∞, $(0, \pm 3)$, $(3, 0)$, $(4, \pm 2)$, $(6, \pm 1)$. The classes $[\bar{R} - \infty]$ for $\bar{R} = (3, 0), (6, \pm 1)$ are not in $\langle \bar{D}' \rangle$, so no rational point reduces to these. For the others $[\bar{R} - \infty] = t\bar{D}'$ with $t \equiv 0$ (∞), 2 ($(4, 2)$), 23 ($(4, -2)$), 15 ($(0, 3)$), 10 ($(0, -3)$) modulo 25. For $R \in \Gamma_1(\mathbb{Q})$ write $[R - \infty] = nG$ and $\tau = n/m \in \mathbb{Z}_5$. For every prime $\ell \nmid 30$, the projection π_ℓ of $J(\mathbb{F}_\ell)$ onto its 5-primary part satisfies $\pi_\ell([\bar{R} - \infty]) = \tau\, \pi_\ell(\bar{D}')$, and at $\ell = 7$, $\tau \equiv t \pmod{25}$. At $\ell = 149$, $\#J(\mathbb{F}_{149}) = 22\,500 = 2^2 \cdot 3^2 \cdot 5^4$, $\pi_{149}(\bar{D}')$ has order 25, and the values of τ modulo 25 realized by the points of $\Gamma_1(\mathbb{F}_{149})$ are $0, 2, 5, 9, 16, 20, 23$. So $t \not\equiv 10, 15$, and every rational point reduces modulo 7 to ∞ or $(4, \pm 2)$. The computations of Steps 1–3 are item S21 of the Supplement.

Step 4: Chabauty's method at 7. Let $\omega_i = x^i\, dx/(2y)$ $(i = 0, 1)$, a basis of the regular differentials, and $\log\colon J(\mathbb{Q}_7) \to \mathbb{Q}_7^2$ the logarithm with respect to it, a homomorphism with $\log([P - \infty]) = \left(\int_\infty^P \omega_0, \int_\infty^P \omega_1\right)$ (Coleman integrals); on a residue disc the integrals are given

by termwise integration of power series [32, 85]. Put $(L_0, L_1) = \log(D)$. We computed it, without general Coleman integration, as $\log(25D)/25$: the multiple $25D$, computed over $\mathbb{Q}$ by Cantor's algorithm, is $[P_1 + P_2 - 2\infty]$ with $x(P_1), x(P_2) \in \mathbb{Z}_7$, both $\equiv 6 \pmod 7$, and P_2 in the residue disc of ιP_1; as $\iota^*\omega_i = -\omega_i$ and $\iota(\infty) = \infty$, $\log(25D) = \int_{\iota P_2}^{P_1}(\omega_0, \omega_1)$ is an integral inside one residue disc, where $x^i/(2y)$ is a power series in $x - x(P_2)$ with coefficients in $\mathbb{Z}_7$. Working modulo 7^{40} with 80 terms (the terms left out have valuation at least 79), this gives

$$L_0 = 2 \cdot 7 + 7^2 + 6 \cdot 7^3 + O(7^4), \qquad L_1 = 5 \cdot 7 + 5 \cdot 7^2 + 5 \cdot 7^3 + O(7^4)$$

(the Supplement, item S22; Appendix A lists the checks). Since $J(\mathbb{Q}) = \mathbb{Z}G$ and $D = 2mG \neq 0$, the differential $\eta = L_1\omega_0 - L_0\omega_1$ satisfies $\int_\infty^R \eta = 0$ for every $R \in \Gamma_1(\mathbb{Q})$. Divided by 7, $\eta/7 = \alpha\omega_0 + \beta\omega_1$ with $\alpha, \beta \in \mathbb{Z}_7$ and $\alpha \equiv \beta \equiv 5 \pmod 7$.

On the disc of ∞ take the parameter $t = x^2/y$; then $1/x = t^2(1 + t^{10}g(t))$ with $g \in \mathbb{Z}[[t]]$, and $\omega_0 = -t^2(1 + O(t^{10}))\,dt$, $\omega_1 = -(1 + O(t^{10}))\,dt$ with coefficients in $\mathbb{Z}[\frac{1}{2}]$. So $F(t) = \int_\infty^{P(t)} \eta/7 = \sum_{i \geq 1} \lambda_i t^i$ with $\lambda_1 = -\beta \not\equiv 0 \pmod 7$ and $i\lambda_i \in \mathbb{Z}_7$. On the discs of $(4, \pm 16)$ take $s = x - 4$: then $y = \pm 16(1 + (f(4 + s) - 256)/256)^{1/2}$ has coefficients in $\mathbb{Z}_7$, and $F(s) = \int_{(4,\pm 16)}^{P(s)} \eta/7 = \sum_{i \geq 1} \lambda_i s^i$ with $\lambda_1 = (\alpha + 4\beta)/(\pm 32) \not\equiv 0 \pmod 7$ and $i\lambda_i \in \mathbb{Z}_7$ (note that $\int_\infty^{(4,\pm 16)} \eta = 0$). On each disc write the parameter as $7r$ with $r \in \mathbb{Z}_7$: the coefficient of r is $7\lambda_1$, of valuation 1, and that of r^i has valuation at least $i - v_7(i) \geq 2$ for $i \geq 2$. By Strassmann's theorem F has at most one zero on each disc, and the known point is one. With Step 3, $\Gamma_1(\mathbb{Q}) = \{\infty, (4, \pm 16)\}$. □

Proof of Theorem 12.3 (c). Let (x, y, z) be a solution of $x^3 + y^3 = 3^k z^5$ with $k \equiv 2 \pmod 5$. If $k = 2$, Lemma 12.12 gives the point $(X, Y) = (b/c^2, (x - y)/c^5)$ of $Y^2 = 4X^5 - 3$, and $(4X, 16Y) \in \Gamma_1(\mathbb{Q})$ is affine, so $X = 1$ by Proposition 12.14. Then $b = c^2$, and $\gcd(b, c) = 1$ gives $c = \pm 1$, $b = 1$: $x + y = \pm 3$ and $x^2 - xy + y^2 = 3$, so $(x - y)^2 = 1$, and (x, y, z) is one of the four solutions listed ($z = c$). If $k = 5m + 2$ with $m \geq 1$, the point $(X/3^{2m}, Y/3^{5m})$ of $Y^2 = 4X^5 - 3$ gives in the same way $X = 3^{2m}$, that is $b = 3^{2m}c^2$, against $3 \nmid b$. □

The exponent 5 with $k \equiv 0$ or $4 \pmod 5$. For $k \equiv 4 \pmod 5$ the curve is $\Gamma_5 \colon y^2 = x^5 - 62\,208$, and for $k \equiv 0 \pmod 5$, $k \geq 5$, it is $\Gamma_7 \colon y^2 = x^5 - 559\,872$. The curve Γ_5 has the rational points $(12, \pm 432)$, since $12^5 - 62\,208 = 186\,624 = 432^2$.[1] We use the notation of the 2-descent above, with $j = 5$ and $j = 7$; in both cases f is irreducible over $\mathbb{Q}$, so $J_j(\mathbb{Q})[2] = 0$.

Proposition 12.15. $\Gamma_5(\mathbb{Q}) = \{\infty, (12, 432), (12, -432)\}$.

Proof. Write $J = J_5$ and $D = [(12, 432) - \infty] \in J(\mathbb{Q})$.

Step 1: $J(\mathbb{Q})$ is infinite cyclic. Here $L = \mathbb{Q}(2^{1/5})$, with $\theta = 6 \cdot 2^{3/5}$, of discriminant $2^4 \cdot 5^5$ and signature $(1, 2)$; its class group is trivial (Minkowski bound below 14; each of the five prime ideals of norm at most 13 has an explicit generator), and -1 and two units of norm 1 span $\mathcal{O}_L^\times/\mathcal{O}_L^{\times 2}$. The polynomial $f = x^5 - 62\,208$ is irreducible over $\mathbb{Q}_2$ (its Newton polygon has the one slope $8/5$) and over $\mathbb{Q}_5$ ($62\,208 \equiv 8 \pmod{25}$ is not a fifth power in $\mathbb{Q}_5$); over $\mathbb{Q}_3$ it is the product of a linear factor and an irreducible quartic factor, as $62\,208 = 2^8 \cdot 3^5$ is a fifth power in $\mathbb{Q}_3$; and it has one real root. So $\mathcal{I}_5 = \mathcal{I}_\infty = 0$, $\dim \mathcal{I}_3 = 1$ and $\dim \mathcal{I}_2 = 2$; $\mathcal{I}_3$ is spanned by the image of the point of $\Gamma_5(\mathbb{Q}_3)$ with $x = -300/11$, and $\mathcal{I}_2$ by the images of

[1] In the version of [26] posted by its author, the X-coordinate 12 found in Lemma 10 is set aside in the sentence that follows, and Lemma 8 states $C_2(\mathbb{Q}) = \{\infty\}$; Theorem 2 there is not affected, since these two points give only solutions with $xy = 0$, as in the proof of Corollary 12.17 below.

the points of $\Gamma_5(\mathbb{Q}_2)$ with $x = -300/7$ and $x = -299/5$. The local conditions leave a Selmer group of dimension 1, so $J(\mathbb{Q})$ has rank at most 1. As $\#J(\mathbb{F}_7) = 50$ and $\#J(\mathbb{F}_{11}) = 101$ are coprime, $J(\mathbb{Q})_{\mathrm{tors}} = 0$; as $D \neq 0$, $J(\mathbb{Q}) = \mathbb{Z}G$ for a generator G. Write $D = mG$. The reduction $\bar{D}$ has order $50 = \#J(\mathbb{F}_7)$, so it generates $J(\mathbb{F}_7)$, and therefore $\gcd(m, 50) = 1$.

Step 2: sieving. For $R \in \Gamma_5(\mathbb{Q})$ write $[R - \infty] = nG$ and $\tau = n/m$, an element of $\mathbb{Z}_2$ and of $\mathbb{Z}_5$. For every prime $\ell \nmid 30$, the projection π_ℓ of $J(\mathbb{F}_\ell)$ onto its $\{2,5\}$-primary part satisfies $\pi_\ell([\bar{R} - \infty]) = \tau\,\pi_\ell(\bar{D})$, because $m[R - \infty] = nD$ and m is invertible on that part. So τ modulo the order of $\pi_\ell(\bar{D})$ is among the residues realized by the points of $\Gamma_5(\mathbb{F}_\ell)$. Combining these conditions for the primes $7 \leq \ell \leq 199$ modulo $2000 = 2^4 \cdot 5^3$, a common multiple of the orders of $\pi_\ell(\bar{D})$ for these primes, leaves only $\tau \equiv 0, \pm 1 \pmod{50}$ (the primes 7, 19, 59, 79 and 199 suffice; with $\ell \leq 149$ only, $\tau \equiv \pm 10$ would also remain). At these five primes the order of $\pi_\ell(\bar{D})$ and the residues of τ modulo it that the points of $\Gamma_5(\mathbb{F}_\ell)$ realize are:

ℓ	order of $\pi_\ell(\bar{D})$	residues of τ realized by $\Gamma_5(\mathbb{F}_\ell)$
7	50	$0, 1, 10, 22, 25, 28, 40, 49$
19	20	$0, 1, 10, 19$
59	4	$0, 1, 3$
79	80	$0, 1, 79$
199	100	$0, 1, 99$

At $\ell = 7$, where $\bar{D}$ generates $J(\mathbb{F}_7)$, this gives $[\bar{R} - \infty] \in \{0, \pm\bar{D}\}$, so $\bar{R}$ is ∞ or $(5, \pm 5)$, the reductions of $(12, \pm 432)$. The computations of Steps 1 and 2 are item S23 of the Supplement.

Step 3: Chabauty's method at 7. With ω_0, ω_1 and log as in Step 4 of the proof of Proposition 12.14, put $(L_0, L_1) = \log(D)$. We computed it as $\log(50D)/50$. The multiple $50D$, computed over $\mathbb{Q}$ by Cantor's algorithm, is $[P_1 + P_2 - 2\infty]$ with $x(P_1), x(P_2)$ the roots of a polynomial u with 7-integral coefficients and $u \equiv (x - 4)^2 \pmod 7$. As $f(4) \equiv 3$ is not a square modulo 7, P_1 and P_2 are conjugate over the unramified quadratic extension of $\mathbb{Q}_7$, and P_1 and ιP_2 lie in one residue disc; so $\log(50D) = \int_{\iota P_2}^{P_1}(\omega_0, \omega_1)$ is an integral inside one residue disc, computed as in Step 4 of the proof of Proposition 12.14 (modulo 7^{40}, with 120 terms). This gives

$$L_0 = 3 \cdot 7 + 5 \cdot 7^2 + 2 \cdot 7^3 + O(7^4), \qquad L_1 = 5 \cdot 7 + 6 \cdot 7^2 + 3 \cdot 7^3 + O(7^4)$$

(the Supplement, item S24). So $\eta = L_1\omega_0 - L_0\omega_1$ satisfies $\int_\infty^R \eta = 0$ for every $R \in \Gamma_5(\mathbb{Q})$, and $\eta/7 = \alpha\omega_0 + \beta\omega_1$ with $\alpha, \beta \in \mathbb{Z}_7$, $\alpha \equiv 5$ and $\beta \equiv 4 \pmod 7$. On the disc of ∞, with the parameter $t = x^2/y$ as in the proof of Proposition 12.14, the linear coefficient of $\int_\infty \eta/7$ is $-\beta \not\equiv 0 \pmod 7$. On the discs of $(12, \pm 432)$ take $s = x - 12$: then $y = \pm 432(1 + (f(12 + s) - 432^2)/432^2)^{1/2}$ has coefficients in $\mathbb{Z}_7$, and the linear coefficient of $\int_{(12,\pm 432)} \eta/7$ is $(\alpha + 12\beta)/(\pm 864) \equiv \pm 6 \not\equiv 0 \pmod 7$. The Strassmann argument of Step 4 of the proof of Proposition 12.14 shows that each of these three discs contains at most one rational point, and with Step 2, $\Gamma_5(\mathbb{Q}) = \{\infty, (12, \pm 432)\}$. □

Proposition 12.16. $\Gamma_7(\mathbb{Q}) = \{\infty\}$.

Proof. Write $J = J_7$. The Mumford pair $(x^2 + 432,\ 72x + 1296)$ defines a point $G_1 \in J(\mathbb{Q})$ [26, §4], since $f - (72x + 1296)^2 = (x^2 + 432)(x^3 - 432x - 5184)$.

Step 1. Here $L = \mathbb{Q}(72^{1/5})$, with $\theta = 6 \cdot 72^{1/5}$, of discriminant $2^4 \cdot 3^4 \cdot 5^5$ and signature $(1, 2)$; its class group is trivial (each of the 34 prime ideals of norm at most 125 has an explicit generator), and -1 and two units span $\mathcal{O}_L^\times/\mathcal{O}_L^{\times 2}$. The polynomial $f = x^5 - 559\,872$ is irreducible over $\mathbb{Q}_2$, $\mathbb{Q}_3$ (slopes $8/5$, $7/5$) and $\mathbb{Q}_5$ ($559\,872 \equiv 22 \pmod{25}$), with one real

root, so $\mathcal{I}_3 = \mathcal{I}_5 = \mathcal{I}_\infty = 0$ and $\dim \mathcal{I}_2 = 2$, spanned by the images of the points of $\Gamma_7(\mathbb{Q}_2)$ with $x = -199$ and $x = -196$. Of the four classes with even valuation away from 2 that have square norm, are positive at the real place and are squares at the primes above 3 and 5, two lie in $\mathcal{I}_2$: the Selmer group has dimension 1. As $\#J(\mathbb{F}_7) = 50$ and $\#J(\mathbb{F}_{11}) = 131$ are coprime, $J(\mathbb{Q})_{\text{tors}} = 0$; as $G_1 \neq 0$, $J(\mathbb{Q}) = \mathbb{Z}G$ and $G_1 = mG$. The reduction $\bar{G}_1$ has order $50 = \#J(\mathbb{F}_7)$, so $\gcd(m, 50) = 1$.

Step 2. The sieve of Step 2 of the proof of Proposition 12.15, with G_1 in place of D and the primes $7 \leq \ell \leq 149$ (of which 7, 19, 43 and 149 suffice), leaves only $\tau \equiv 0 \pmod{50}$. At these four primes the order of $\pi_\ell(\bar{G}_1)$ and the residues of τ that the points of $\Gamma_7(\mathbb{F}_\ell)$ realize are:

ℓ	order of $\pi_\ell(\bar{G}_1)$	residues of τ realized by $\Gamma_7(\mathbb{F}_\ell)$
7	50	$0, 17, 20, 24, 25, 26, 30, 33$
19	20	$0, 4, 16$
43	10	$0, 1, 2, 3, 5, 7, 8, 9$
149	50	$0, 17, 33$

As $\bar{G}_1$ generates $J(\mathbb{F}_7)$, every $R \in \Gamma_7(\mathbb{Q})$ reduces modulo 7 to ∞. The computations of Steps 1 and 2 are also in item S23 of the Supplement.

Step 3. Put $(L_0, L_1) = \log(G_1) = \log(50G_1)/50$. Here $50G_1 = [P_1 + P_2 - 2\infty]$ with $u \equiv (x-3)^2 \pmod 7$, and $f(3) \equiv 0 \pmod 7$, so P_1 and P_2 lie in the residue disc of the point $(e, 0)$ with $e \in \mathbb{Z}_7$, $e \equiv 3 \pmod 7$, a Weierstrass point. On that disc y is a parameter and x a power series in y^2, and $\int_\infty^{(e,0)} \omega_i = 0$ because $[(e,0) - \infty]$ has order 2; so $\log(50G_1) = \int_{(e,0)}^{P_1}(\omega_0, \omega_1) + \int_{(e,0)}^{P_2}(\omega_0, \omega_1)$ is computed by termwise integration in y. This gives

$$L_0 = 4 \cdot 7 + 3 \cdot 7^2 + O(7^4), \qquad L_1 = 5 \cdot 7 + 5 \cdot 7^2 + 5 \cdot 7^3 + O(7^4)$$

(the Supplement, item S24). Then $\eta/7 = \alpha\omega_0 + \beta\omega_1$ with $\beta = -L_0/7 \equiv 3 \not\equiv 0 \pmod 7$, so, as in Step 3 of the proof of Proposition 12.15, the disc of ∞ contains no rational point other than ∞. □

Corollary 12.17. *Let $k \geq 0$ be an integer with $k \not\equiv 2 \pmod 5$, and let x, y, z be integers with $\gcd(x, y) = 1$, $z \neq 0$ and $x^3 + y^3 = 3^k z^5$. Then $k = 0$ and $xy = 0$.*

Proof. For $k \equiv 1, 3 \pmod 5$ this is Theorem 12.3 (b). Let $k = 5m + 4$ with $m \geq 0$. Then $2k - 3 = 10m + 5$, and Lemma 12.12 with the maps above gives the affine point $(4b/(3^{2m}c^2), 16(x-y)/(3^{5m}c^5))$ of Γ_5. By Proposition 12.15, $4b/(3^{2m}c^2) = 12$, that is $b = 3^{2m+1}c^2$, against $3 \nmid b$. Let $k = 5m$ with $m \geq 1$. Then $2k - 3 = 10(m-1) + 7$, and Lemma 12.12 gives an affine rational point of Γ_7, which Proposition 12.16 excludes.

Let $k = 0$. As $x^3 + y^3 \equiv x + y \pmod 3$, $3 \mid z$ if and only if $3 \mid x + y$. If $3 \mid z$, then $(x, y, z/3)$ is a solution for $k = 5$, which we have excluded. If $3 \nmid z$, then $x + y$ and $x^2 - xy + y^2$ are coprime (a common prime factor divides $3xy$, hence is 3, but $3 \nmid x + y$), so $x + y = c^5$ and $x^2 - xy + y^2 = b^5$ with $c \neq 0$, $b \geq 1$ and $\gcd(b, c) = 1$. From $4b^5 = c^{10} + 3(x-y)^2$ we get the affine point $(12b/c^2, 432(x-y)/c^5)$ of Γ_5, so $b = c^2$ by Proposition 12.15, and $\gcd(b, c) = 1$ gives $c = \pm 1$, $b = 1$. Then $x + y = \pm 1$ and $(x+y)^2 - 3xy = x^2 - xy + y^2 = 1$, so $xy = 0$. □

With Theorem 12.3 (c), Corollary 12.17 determines all the solutions of $x^3 + y^3 = 3^k z^5$ with $\gcd(x, y) = 1$ for every $k \geq 0$: those with $z = 0$, those with $xy = 0$ (for $k = 0$ only), and the four solutions of Theorem 12.3 (c) (for $k = 2$ only). For $k = 0$ the corollary is Bruin's theorem [26, Theorem 2].

12.7. **The Frey representation for $3^k c^p$, and p split or inert.** If $p \equiv 2 \pmod 3$ we write $v = p\mathcal{O}$ for the prime of K above p; then $K_v = \mathbb{Q}_{p^2}$ is the unramified quadratic extension of $\mathbb{Q}_p$, and it has two embeddings in $\overline{\mathbb{Q}}_p$, which restrict to the two embeddings of K. We need Proposition 5.6 at this prime.

Lemma 12.18. *Proposition 5.6 holds for every prime $p \geq 5$ and every prime v of K above p, split or inert, with "Hodge–Tate weights $\{0,1,2\}$" at each of the embeddings of K_v in $\overline{\mathbb{Q}}_p$.*

Proof. The proof of Proposition 5.6, with Lemmas 5.7, 5.8 and 5.9, is written for every prime $p \geq 5$ and every prime v of K above p: the only properties of p it uses are that $p \neq 3$ (Proposition 3.4 is over $\mathcal{O}[1/3]$, and the Fermat surface of degree 9 is smooth in residue characteristic p) and that K_v and $K_v(\zeta_9)$ are unramified over $\mathbb{Q}_p$. All of this holds for v inert. For the weights, let τ be an embedding of $F = K_v(\zeta_9)$ in $\overline{\mathbb{Q}}_p$. By the comparison theorem, compatible with the action of H, the τ-part of D_{dR} of the χ^m-part of H^2 is the χ'-part of $H^2_{\mathrm{dR}}(\tilde{X}_{s_0}/F) \otimes_{F,\tau} \overline{\mathbb{Q}}_p$, where $\chi' = \tau^{-1} \circ \chi^m$ is one of the characters $\chi^{m'}$, $m' \in (\mathbb{Z}/9)^\times$ (it is fixed by G_K and has order 9 on each factor, Lemma 3.1). By Lemma 3.5, which holds for every $m' \in (\mathbb{Z}/9)^\times$ and every complex embedding, each of these parts has Hodge numbers $(1,1,1)$. So the Hodge–Tate weights are $\{0,1,2\}$ at every embedding of K_v. □

Let $p \geq 17$ be a prime, $k \geq 1$, and (a,b,c) a solution of $x^3 + y^3 = 3^k z^p$ with

$$\nu = k + p\, v_3(c) \geq 8, \quad \text{that is, } 3 \mid c \ \text{ or } \ k \geq 8.$$

(For $k = 1$ this holds, since $3 \mid c$ by Lemma 12.6 (ii).) As $\gcd(a,b) = 1$, p divides at most one of a, b. Choose $(u,w) \in \{(a,b),(b,a)\}$ with $p \nmid u$, and put

$$s_0 = \frac{3^k c^p}{u^3} = 1 + \left(\frac{w}{u}\right)^3 \in \mathbb{Q} \smallsetminus \{0,1\}, \qquad \rho = \mathbb{V}_{s_0} \otimes \kappa_u^{-n_\infty} \colon G_K \to \mathrm{GL}_3(\overline{\mathbb{Q}}_p),$$

with $\ell = p$ in Definition 3.2, and let $\bar\rho$ be the reduction of ρ (Section 2). This is Definition 5.4 with c^p replaced by $3^k c^p$.

Proposition 12.19. *The representation ρ has the following properties.*

(a) *ρ is unramified at every prime $\mathfrak{q} \nmid 3pabc$, and the characteristic polynomial of $\rho(\mathrm{Frob}_\mathfrak{q})$ has coefficients in $\mathcal{O}$.*

(b) *$\bar\rho$ is unramified at every prime $\mathfrak{q} \nmid 3p$.*

(c) *$\rho^{\mathsf{c}} \cong \rho^\vee \otimes \varepsilon_p^{-2}$.*

(d) *$I_\mathfrak{p}$ acts on ρ through $\kappa_u^{-n_\infty}|_{I_\mathfrak{p}}$ times a unipotent representation.*

(e) *ρ is unramified at $\mathfrak{l}$ and $\bar{\mathfrak{l}}$, and the characteristic polynomial of $\rho(\mathrm{Frob}_\mathfrak{q})$, $\mathfrak{q} \in \{\mathfrak{l}, \bar{\mathfrak{l}}\}$, is $P_\mathfrak{q}(\xi_\mathfrak{q}^{-1} T)$ with $\xi_\mathfrak{q} = \kappa_u(\mathrm{Frob}_\mathfrak{q})^{-n_\infty} \in \mu_3$ and $P_\mathfrak{q}$ as in Proposition 3.9.*

(f) *For each prime $v \mid p$ of K, $\rho|_{G_{K_v}}$ is crystalline, with Hodge–Tate weights $\{0,1,2\}$ at each embedding of K_v in $\overline{\mathbb{Q}}_p$.*

Proof. We follow the proof of Proposition 5.5. By Theorem 12.9 (iv), (v), which hold for every solution, $p \nmid c$, $7 \nmid abc$ and $a^3 \equiv b^3 \pmod 7$; and $3 \nmid u$ (Lemma 12.6 (i)), so $v_3(s_0) = \nu$.

(a) If $\mathfrak{q} \nmid 3pabc$, then s_0 and $s_0 - 1$ are $\mathfrak{q}$-units and Lemma 5.3 (a) applies; κ_u is unramified outside $3u$; the coefficients lie in $\mathcal{O}$ by Lemma 3.7.

(b) Let $\mathfrak{q} \nmid 3p$ lie above the rational prime r. By Lemma 12.6 (i), r divides at most one of u, w, c. If $r \nmid uwc$ use (a). If $r \mid c$, then $v_\mathfrak{q}(s_0) = p\, v_r(c)$, and by Lemma 5.3 (b) $I_\mathfrak{q}$ acts on a stable lattice through powers of $\gamma_0^{p\, v_r(c)}$, which is $\equiv 1 \pmod p$ as in the proof of Proposition 5.5 (b); κ_u is unramified at $\mathfrak{q}$. If $r \mid u$, then $s_0 = z_0/u^3$ with $z_0 = 3^k c^p$ prime

to $\mathfrak{q}$, and by Lemma 5.3 (d) $I_{\mathfrak{q}}$ acts on $\mathbb{V}_{s_0}$ by $\kappa_u^{n_\infty}$, which the twist cancels. If $r \mid w$, then $v_{\mathfrak{q}}(s_0 - 1) = 3v_r(w)$ and Lemma 5.3 (c) applies; κ_u is unramified at $\mathfrak{q}$.

(c) Lemma 3.6 ($s_0 \in \mathbb{Q}$) and $\kappa_u^{\mathsf{c}} = \kappa_u^{-1}$.

(d) $v_3(s_0) = \nu \geq 8 > 15/2$, so $I_{\mathfrak{p}}$ acts unipotently on $\mathbb{V}_{s_0}$ by Theorem 4.1.

(e) $7 \nmid u$ and $(w/u)^3 \equiv 1 \pmod 7$, so $s_0 \equiv 2 \pmod 7$, and we conclude as in the proof of Proposition 5.5 (e).

(f) $p \nmid u$ and $p \nmid c$, so $v_p(s_0) = 0$. If $p \nmid w$ then $s_0 - 1 = (w/u)^3$ is a p-adic unit, and if $p \mid w$ then $s_0 - 1 = t_1^3$ with $t_1 = w/u \in p\mathbb{Z}_{(p)}$. So Lemma 12.18 applies, and κ_u is unramified at v and of finite order. □

So ρ has the properties (F1)–(F5) of Section 7.1, where, for p inert, $\{\mathfrak{p}, v, \bar{v}\}$ in (F1) is to be read as $\{\mathfrak{p}, v\}$ and (F2) as: $\rho|_{G_{K_v}}$ is crystalline with Hodge–Tate weights $\{0, 1, 2\}$ at both embeddings of K_v. In (F3) the character is $\kappa = \kappa_u^{-n_\infty}$, and Lemma 6.1 applies to it, as u is an integer prime to 3. Moreover ρ is unramified at all but finitely many primes, by (a).

Proposition 12.20. *Let $p \geq 17$ be a prime, split or inert in K, and let $\rho\colon G_K \to \mathrm{GL}_3(\overline{\mathbb{Q}}_p)$ be a continuous representation with the properties* (F1), (F2), (F3) *and* (F5) *(read as above if p is inert). Then $\bar{\rho}$ is absolutely irreducible. In particular the representation ρ of Proposition 12.19 has the properties* (F1)–(F6).

Proof. For p split this is the proof of Theorem 6.2, which uses only these properties of ρ. Let p be inert, $v = p\mathcal{O}$, and suppose that $\bar{\rho}$ has a one-dimensional constituent θ. Let τ_0 be the embedding of K_v in $\overline{\mathbb{Q}}_p$ that extends the embedding of K given by ι_p, and $\tau_0\mathsf{c}$ the other one.

Steps 1 and 2. By (F2) and Fontaine–Laffaille theory in the normalization of [10, §1.4] (the weights lie in $[0, p-2]$), the argument of Lemma 9.1 (i), (ii), with $\mathbb{Q}_{p^2}$ and p in place of $\mathbb{Q}_{25}$ and 5, shows: $\theta|_{G_{K_v}}$ is the reduction of a crystalline character of G_{K_v} with Hodge–Tate weights $(h, h') \in \{0, 1, 2\}^2$ at $(\tau_0, \tau_0\mathsf{c})$; on the image of $\mathcal{O}_v^\times = \mathbb{Z}_{p^2}^\times$ in the inertia group it is $x \mapsto \bar{x}^{\pm(h+ph')}$; by (F1) and (F3), θ is unramified outside $\{\mathfrak{p}, v\}$ and $\theta|_{I_{\mathfrak{p}}} = \bar{\kappa}|_{I_{\mathfrak{p}}}$ has order dividing 3. The idele class character of θ is trivial on $\mu_6 \subset K^\times$ and on the units at the places where θ is unramified. The unit -1 acts at v by $(-1)^{h+ph'} = (-1)^{h+h'}$, and at $\mathfrak{p}$ by an element of order dividing 2 and 3, that is, trivially. So $(-1)^{h+h'} = 1$ and $(h, h') \in \mathcal{T}$.

Step 3. Among the five Hecke characters ψ of Step 3 of the proof of Theorem 6.2, the one of infinity type (h, h') or (h', h), chosen so that its p-adic realization has the same Hodge–Tate weights at $(\tau_0, \tau_0\mathsf{c})$ as $\theta|_{G_{K_v}}$, has a reduction $\bar{\psi}$ with $\theta\bar{\psi}^{-1}$ unramified at v (two crystalline characters with the same weights agree on inertia). So $\theta\bar{\psi}^{-1}$ is a character of $\mathrm{Cl}_{\mathfrak{p}^2}(K)$, which is trivial, and $\theta = \bar{\psi}$.

Steps 4 and 5. As in the proof of Theorem 6.2, (F5) gives $(k, k') \in \mathcal{T}$ and $\zeta_1, \zeta_2 \in \mu_3$ with (6.1), where now $\mathfrak{P} = p\mathcal{O}$. By Appendix A, item C2, all the prime factors of the ideal generated by the two elements of (6.1) lie above 2, 3, 7 or 13, so none is $p\mathcal{O}$. □

12.8. **Part II at an inert prime.** Parts II and III assume $p \equiv 1 \pmod 3$, but they use only the properties (F1)–(F6) of the Frey representation (Section 7.1) and, in the proof of Lemma 7.4, the fact that ρ is unramified at all but finitely many primes. For $p \equiv 2 \pmod 3$ two steps have to be redone: the construction of the compatible system (Theorem 7.3 and Lemma 7.5), and the proof of Proposition 9.5, which constructs a second system (Section 12.10).

We give a construction through a lifting lemma, Lemma 12.21, whose proof is that of the lifting theorem of Bellovin and Gee [13, Theorem 5.2.1], written out for the group $\mathcal{G}_3$ over $\mathbb{Q}$. We do not cite that theorem itself: its statement asks that the components at the places

above p be potentially diagonalizable, a notion defined in [10, §1.4] only for GL_n-valued representations, and at an inert prime the place p of $\mathbb{Q}$ does not split in K. The proof below uses potential diagonalizability only over a field in which the places above p split.

In this subsection and the next, $p \geq 17$ is a prime with $p \equiv 2 \pmod 3$, $v = p\mathcal{O}$, $\mu = \varepsilon_p^{-2}\delta_{K/\mathbb{Q}}$, and $\rho\colon G_K \to \mathrm{GL}_3(\overline{\mathbb{Z}}_p)$ is a continuous representation, unramified at all but finitely many primes, with the properties (F1)–(F6) read as in Section 12.7.

Polarization. Lemma 7.1 and its proof are unchanged (they use (F4) and (F6)); let $\rho_{\mathcal{G}}\colon G_{\mathbb{Q}} \to \mathcal{G}_3(\overline{\mathbb{Z}}_p)$ and $\bar\rho_{\mathcal{G}}$ be the prolongations defined by Ψ_ρ and its reduction, with multiplier $\varepsilon_p^{-2}\delta_{K/\mathbb{Q}}$.

$\bar\rho$ is reasonable. It is polarized, $p > 8$ and $\zeta_p \notin K$. The extension $K(\zeta_p)/K$ is cyclic of degree $p-1$, which is prime to 3. If $\bar\rho|_{G_{K(\zeta_p)}}$ were reducible, then by Clifford's theorem it would be either isotypic with a constituent of dimension 1, so that $\bar\rho(G_{K(\zeta_p)})$ would consist of scalars and $\bar\rho(G_K)$, generated by it and one more element, would be abelian, contradicting (F6); or a sum of three distinct characters permuted transitively by G_K, with a stabilizer of index 3 in G_K containing $G_{K(\zeta_p)}$, which does not exist. (This argument replaces the Fontaine–Laffaille analysis in the proof of Proposition 7.2.)

The component at p. The restriction $\rho_{\mathcal{G}}|_{G_{\mathbb{Q}_p}}$ is crystalline, in the sense of [13, §2.8] (all its compositions with representations of $\mathcal{G}_3$ are crystalline), because its restriction to the subgroup G_{K_v} of index 2 is crystalline by (F2) and $K_v/\mathbb{Q}_p$ is unramified. Its Hodge type is regular (weights $\{0,1,2\}$ at both embeddings of K_v). In the generic fiber of the ring of framed liftings of $\bar\rho_{\mathcal{G}}|_{G_{\mathbb{Q}_p}}$ to $\mathcal{G}_3$ with multiplier $\varepsilon_p^{-2}\delta_{K/\mathbb{Q}}$, trivial inertial type and this Hodge type, the locus where the monodromy operator vanishes is a union of irreducible components, and it is regular [13, Theorems 3.3.2 and 3.3.7] (these are stated for possibly disconnected reductive groups and any finite extension of $\mathbb{Q}_p$). Let $\mathcal{C}_p$ be its component through $\rho_{\mathcal{G}}|_{G_{\mathbb{Q}_p}}$. Every point of $\mathcal{C}_p$ is crystalline, with Hodge–Tate weights $\{0,1,2\}$ at both embeddings of K_v, and its restriction to G_{K_v} is potentially diagonalizable by [10, Lemma 1.4.3 (2)] ($K_v/\mathbb{Q}_p$ is unramified and the weights lie in $[0, p-2]$).

12.9. **A lifting lemma, and the compatible system.**

Lemma 12.21. *Let $\mathcal{C}_3$ be a polarized component at 3 (Section 7.4), and let $\mathcal{C}_p$ be the component at p defined above. There is a continuous homomorphism $\tilde\rho\colon G_{\mathbb{Q}} \to \mathcal{G}_3(\overline{\mathbb{Z}}_p)$ lifting $\bar\rho_{\mathcal{G}}$, unramified outside $\{3, p\}$, with $\mathrm{mult}\circ\tilde\rho = \mu$, whose restrictions to $G_{\mathbb{Q}_3}$ and to $G_{\mathbb{Q}_p}$ are points of $\mathcal{C}_3$ and of $\mathcal{C}_p$.*

We do not deduce the lemma from [27, Theorem 4.2.11]; Remark 12.23 says why. Step 1 of the proof checks the hypotheses of [13, Corollary 5.1.1] over K, Step 2 those of [10, Corollary 4.5.3] over a field F_1 in which the places above 3 and p split, and Step 5 those of [7, Theorem A.4.1] and [10, Theorem 2.3.2] over an extension F' of F_1.

Proof. All framed lifting rings below are taken over the ring of integers $\mathcal{O}_E$ of a sufficiently large finite extension E of $\mathbb{Q}_p$. Their generic fibers are their spectra with p inverted, in which closed points are dense and have residue fields finite over E [10, §1.2]. Lifting rings commute with finite extensions of scalars [10, Lemma 1.2.1] (stated there for GL_n; the same proof applies to the $\mathcal{G}_3$-valued rings with fixed multiplier). So, enlarging E (the fields F_1 and F' of Step 2 do not depend on it) and replacing $\mathcal{C}_3$ by an irreducible component of its extension of scalars and $\mathcal{C}_p$ by the one through $\rho_{\mathcal{G}}|_{G_{\mathbb{Q}_p}}$, which only strengthens the conclusion, we may assume that every irreducible component of the finitely many generic fibers considered below stays irreducible after any finite extension of scalars; these are then the components over $\overline{\mathbb{Q}}_p$

used in [10] and [7]. For an irreducible component C of a generic fiber we write R_C for the quotient of the lifting ring that is reduced, without p-torsion, and whose generic fiber is C [10, §§1.3, 1.4], [13, §4.2].

Step 1: a deformation ring of dimension at least one. Let $\mathcal{A}$ be the universal ring for deformations of $\bar\rho_{\mathcal{G}}$ with multiplier μ that are unramified outside $\{3,p\}$ and whose restrictions to $G_{\mathbb{Q}_3}$ and $G_{\mathbb{Q}_p}$ lie on $\mathcal{C}_3$ and $\mathcal{C}_p$, that is, the corresponding maps from the framed lifting rings factor through $R_{\mathcal{C}_3}$ and $R_{\mathcal{C}_p}$. This condition is invariant under conjugation by [13, Lemma 3.4.1], which is stated for conjugation by residually trivial elements of $\mathcal{G}_3(\mathcal{O}_{E'})$ for finite extensions E' of E. The case of elements with values in an arbitrary coefficient ring follows from it by the density argument in the proof of [10, Lemma 1.2.2], applied to the reduced, p-torsion-free ring $R_C[[X_1,\dots,X_{10}]]$ that carries the universal residually trivial element of $\mathcal{G}_3$, which is how [13, §4.2] use it.

By [13, Corollary 5.1.1], $\mathcal{A}$ has Krull dimension at least 1. We check its hypotheses, for $F^+=\mathbb{Q}$, $F=K$, $n=3$, $l=p$ and the set of places $\{3,p,\infty\}$, which is not required to consist of places that split in K. The prime p is odd, $\zeta_p\notin K$, and $\bar\rho|_{G_{K(\zeta_p)}}$ is absolutely irreducible (paragraph "$\bar\rho$ is reasonable"). The representation $\bar\rho_{\mathcal{G}}$ is discrete series and odd in the sense of [13, Definition 4.2.1]: for $\mathcal{G}_3$ this means that the multiplier takes the value -1 on complex conjugation [13, §5.1], and $\mu(\tilde{\mathfrak{c}})=\varepsilon_p(\tilde{\mathfrak{c}})^{-2}\delta_{K/\mathbb{Q}}(\tilde{\mathfrak{c}})=-1$. The character μ is a de Rham lift of $\bar\mu$, and $\bar\rho$ and μ are unramified outside $\{3,p\}$ by (F1) and the definition of μ. The Hodge type at p is regular [13, Definition 4.2.3], since the weights $0,1,2$ are distinct. Finally $\mathcal{C}_3$ is an irreducible component of the generic fiber of the lifting ring of its inertial type, by definition, and $\mathcal{C}_p$ is one of the generic fiber of the lifting ring of trivial inertial type and this Hodge type, because the locus where the monodromy operator vanishes is a union of such components [13, Theorem 3.3.7 and the paragraph before it].

Step 2: auxiliary fields. Let $d\neq p$ be a prime with $d\equiv 2 \pmod 3$ and $\left(\frac{d}{p}\right)=-\left(\frac{3}{p}\right)$ (Dirichlet's theorem), and put $F_1=K(\sqrt{3d})$, a CM field with maximal totally real subfield $F_1^+=\mathbb{Q}(\sqrt{3d})$. As $-d\equiv 1 \pmod 3$ is a square in $\mathbb{Z}_3$, $\mathbb{Q}_3(\sqrt{3d})=\mathbb{Q}_3(\sqrt{-3})$, so the place of F_1^+ above 3 splits in F_1. As $\left(\frac{3d}{p}\right)=-1$, p is inert in F_1^+, with completion $\mathbb{Q}_{p^2}\ni\sqrt{-3}$, so the place of F_1^+ above p splits in F_1. The field F_1 is unramified at p, so $\zeta_p\notin F_1$; and $\bar\rho|_{G_{F_1(\zeta_p)}}$ is irreducible, because $G_{F_1(\zeta_p)}$ has index at most 2 in $G_{K(\zeta_p)}$ (by Clifford's theorem a reducible restriction would be scalar, and then $\bar\rho(G_{K(\zeta_p)})$ would be abelian).

Apply [10, Corollary 4.5.3] with $F=F_0=F_1$, the polarized representation $(\bar\rho|_{G_{F_1}},\bar\mu|_{G_{F_1^+}})$, the lift $\mu|_{G_{F_1^+}}$ of its multiplier, the set S_1 of primes of F_1 above 3 and p (it contains the primes above p and those at which $\bar\rho|_{G_{F_1}}$ ramifies, by (F1)), the local lifts $\rho|_{G_{F_{1,y}}}$ at $y\in S_1$ (polarized by (F4); at $y\mid p$ crystalline with Hodge–Tate weights $\{0,1,2\}$ at every embedding, $F_{1,y}=K_v$ being unramified over $\mathbb{Q}_p$, hence potentially diagonalizable [10, Lemma 1.4.3 (2)]), and $F^{(\mathrm{avoid})}=F_1\overline{K}^{\ker\bar\rho}(\zeta_p)$. Its condition $p\geq 2(d'+1)$, where $d'\leq 3$ is the largest dimension of an irreducible constituent of $\bar\rho$ restricted to the subgroup generated by the Sylow pro-p-subgroups, holds as $p\geq 17$. It gives a finite CM extension F'/F_1, linearly disjoint from $F^{(\mathrm{avoid})}$ over F_1, and a regular algebraic cuspidal polarized automorphic representation (π',χ') of $\mathrm{GL}_3(\mathbb{A}_{F'})$, of level potentially prime to p, unramified at the primes of F' not above S_1, whose p-adic Galois representation $r(\pi')$ lifts $\bar\rho|_{G_{F'}}$ with multiplier $\mu|_{G_{(F')^+}}$ and satisfies $r(\pi')|_{G_{F'_u}}\sim\rho|_{G_{F'_u}}$ at every place $u\mid p$, where $\sim$ is the relation "connects" of [10, §§1.3, 1.4]. As $\rho|_{G_{F'_u}}$ is potentially diagonalizable [10, §1.4], so is $r(\pi')|_{G_{F'_u}}$ (connecting is an equivalence

relation, preserved by restriction, loc. cit.). The field F' has the following properties, which are used below.

(a) The places of $(F')^+$ above 3 and p split in F', because those of F_1^+ split in F_1 and $F' = (F')^+F_1$.

(b) The field F' does not contain ζ_p, and $\bar\rho(G_{F'(\zeta_p)}) = \bar\rho(G_{F_1(\zeta_p)})$, because F' is linearly disjoint over F_1 from the Galois extension $F^{(\mathrm{avoid})}$, which contains ζ_p and through which $\bar\rho|_{G_{F_1}}$ factors.

(c) By (b), $\bar\rho(G_{F'(\zeta_p)})$ acts irreducibly, as $\bar\rho|_{G_{F_1(\zeta_p)}}$ does, and it is adequate by [10, Proposition 2.1.2], as $p \geq 2(3+1)$.

Step 3: components over F', and a second deformation ring. Let S' be the set of places of $(F')^+$ above 3 and p, and for $w \in S'$ fix a place $\tilde w$ of F' above w. As w splits in F' (Step 2 (a)), $F'_{\tilde w} = (F')^+_w$, and this field contains $K_{\mathfrak p}$ or K_v. So $G_{(F')^+_w} = G_{F'_{\tilde w}}$ is contained in $G_{K_{\mathfrak p}}$ or G_{K_v}. Here a decomposition group at $\tilde w$ is $G_{\mathbb Q}$-conjugate to a subgroup of the decomposition group at 3 or p used to define $\mathcal{C}_3$ and $\mathcal{C}_p$, and we transport these components by the conjugation; by [13, Lemma 3.4.1], the result does not depend on the choices. The restriction to $G_{(F')^+_w}$ of a lifting of $\bar\rho_{\mathcal G}|_{G_{\mathbb Q_3}}$ or $\bar\rho_{\mathcal G}|_{G_{\mathbb Q_p}}$ with multiplier μ has values in $\mathcal{G}_3^0 = \mathrm{GL}_3 \times \mathrm{GL}_1$: it is $\sigma \mapsto (r(\sigma), \mu(\sigma))$, with r a lifting of $\bar\rho|_{G_{F'_{\tilde w}}}$. If $w \mid 3$, let D_w be an irreducible component of the generic fiber of the framed lifting ring of $\bar\rho|_{G_{F'_{\tilde w}}}$ that contains the image of $\mathcal{C}_3$ under this restriction; one exists, the image being irreducible. If $w \mid p$, let D_w be the irreducible component through $\rho|_{G_{F'_{\tilde w}}}$ of the generic fiber of the ring of crystalline liftings of $\bar\rho|_{G_{F'_{\tilde w}}}$ with Hodge–Tate weights $\{0,1,2\}$ at every embedding. That generic fiber is formally smooth [10, §1.4], so its irreducible components are disjoint; the image of $\mathcal{C}_p$ lies in it (the points of $\mathcal{C}_p$ are crystalline with weights $\{0,1,2\}$ at both embeddings of K_v), is irreducible and contains $\rho|_{G_{F'_{\tilde w}}}$, so it lies in D_w. Let $\mathcal{A}'$ be the universal deformation ring of the deformation problem

$$\mathcal{S}' = \left(F'/(F')^+,\, S',\, \{\tilde w\}_{w\in S'},\, \mathcal{O}_E,\, \bar\rho_{\mathcal G}|_{G_{(F')^+}},\, \mu|_{G_{(F')^+}},\, \{\mathcal{D}_w\}_{w\in S'}\right)$$

in the sense of [31, §2.3] and [10, §1.5], where $\mathcal{D}_w$ consists of the liftings that factor through R_{D_w} [10, §§1.3, 1.4]. The restriction to $G_{(F')^+}$ of the universal deformation over $\mathcal{A}$ is of type $\mathcal{S}'$: it is unramified outside S'; and at $w \in S'$ the map from the framed lifting ring of $\bar\rho|_{G_{F'_{\tilde w}}}$ to $\mathcal{A}$ factors through $R_{\mathcal{C}_3}$ or $R_{\mathcal{C}_p}$, which are reduced and without p-torsion, with dense sets of closed points in their generic fibers, all of which restrict to points of D_w, so it kills the kernel of the map to R_{D_w}. This gives a homomorphism $\mathcal{A}' \to \mathcal{A}$.

Step 4: $\mathcal{A}$ is finite over $\mathcal{A}'$. Let L_0 be the field cut out by $\bar\rho_{\mathcal G}$, and Ω_{3p} the maximal pro-p extension of L_0 unramified outside the places above $3p$. Every deformation counted by $\mathcal{A}$ factors through $\Gamma = \mathrm{Gal}(\Omega_{3p}/\mathbb Q)$ (the kernel of $\mathcal{G}_3(A) \to \mathcal{G}_3(\overline{\mathbb F}_p)$ is pro-p), and Γ is topologically finitely generated: $\mathrm{Gal}(\Omega_{3p}/L_0)$ is a pro-p group with finite Frattini quotient, as there are finitely many cyclic extensions of degree p of L_0 unramified outside $3p$ (Hermite's theorem). Let $\Delta = \mathrm{Gal}(\Omega_{3p}/K)$, and let $\Sigma \subset \Gamma$ be the image of $G_{(F')^+}$, a subgroup of finite index. It is not contained in Δ, as $(F')^+$ is totally real, and $\Sigma \cap \Delta$ contains the image of $G_{F'}$, on which $\bar\rho$ is absolutely irreducible. By [10, Lemma 1.2.3 (1)], the universal deformation ring of $\bar\rho_{\mathcal G}|_\Gamma$ is finite over that of $\bar\rho_{\mathcal G}|_\Sigma$. The ring $\mathcal{A}$ is a quotient of the former. Every deformation of $\bar\rho_{\mathcal G}|_\Sigma$ is, by inflation, a deformation of $\bar\rho_{\mathcal G}|_{G_{(F')^+}}$ unramified outside S', and the resulting map from the universal deformation ring of $\bar\rho_{\mathcal G}|_{G_{(F')^+}}$ unramified outside S' to that of $\bar\rho_{\mathcal G}|_\Sigma$ is surjective, because inflation from Σ to $G_{(F')^+}$ is injective on tangent spaces. So the image

in $\mathcal{A}$ of the universal deformation ring of $\bar\rho_{\mathcal{G}}|_\Sigma$ is the image of the universal deformation ring of $\bar\rho_{\mathcal{G}}|_{G_{(F')^+}}$ unramified outside S', which by Step 3 is the image of $\mathcal{A}'$. Hence $\mathcal{A}$ is a finite $\mathcal{A}'$-algebra.

Step 5: $\mathcal{A}'$ is finite over $\mathcal{O}_E$. For $w \in S'$ choose a lift ρ_w of $\bar\rho|_{G_{F'_{\tilde w}}}$: if $w \mid p$, $\rho_w = \rho|_{G_{F'_{\tilde w}}}$, which is potentially diagonalizable with weights $\{0,1,2\}$ at every embedding (Step 2); if $w \mid 3$, a closed point of D_w that lies on no other irreducible component (the complement in D_w of the other components is a nonempty open subset). We apply [7, Theorem A.4.1] with its fields F and F' both equal to our F', its set S equal to S', the places $\tilde w$, the character $\mu|_{G_{(F')^+}}$, the representation $\bar\rho_{\mathcal{G}}|_{G_{(F')^+}}$, the lifts ρ_w, and (π',χ'). Its hypotheses hold by Step 2 (a)–(c), together with the following: F' is CM; S' contains the places above p; $\mu|_{G_{(F')^+}}$ is continuous, totally odd and de Rham, and unramified outside S' (the extension $F' = (F')^+K$ of $(F')^+$ is unramified outside the places above 3); $\bar\rho_{\mathcal{G}}|_{G_{(F')^+}}$ is unramified outside S', has multiplier $\bar\mu$ and maps exactly $G_{F'}$ into $\mathcal{G}_3^0$; for $w \mid p$, ρ_w is potentially diagonalizable with three distinct Hodge–Tate numbers at each embedding; and (π',χ') is unramified outside the places above S', lifts $\bar\rho|_{G_{F'}}$ with multiplier $\bar\mu$, and is potentially diagonalizable at the places above p (Step 2).[2] That χ' is unramified outside the places above S' follows from [10, Corollary 4.5.3 (4)]: $r(\chi') = \mu\varepsilon_p^2|_{G_{(F')^+}}$ is the character of $F'/(F')^+$, which is unramified at every finite place, as shown below for χ''. So [7, Theorem A.4.1] applies. It gives a lift $r'' \colon G_{(F')^+} \to \mathcal{G}_3(\overline{\mathbb{Z}}_p)$ of $\bar\rho_{\mathcal{G}}|_{G_{(F')^+}}$ with multiplier μ, unramified outside S'. Let s'' be the GL_3-component of $r''|_{G_{F'}}$. By the theorem, $s''|_{G_{F'_{\tilde w}}} \sim \rho_w$ for $w \in S'$, and $s'' \cong r(\pi'')$ for a regular algebraic cuspidal polarized automorphic representation (π'',χ'') of $\mathrm{GL}_3(\mathbb{A}_{F'})$ of level potentially prime to p. By [10, Theorem 2.1.1 (2)], π'' is unramified at the places not above S', since r'' is.

We show that $s''|_{G_{F'_{\tilde w}}}$ lies on D_w for every $w \in S'$. If $w \mid 3$, "$\sim$" means that $s''|_{G_{F'_{\tilde w}}}$ and ρ_w lie on a common irreducible component [10, §1.3], and ρ_w lies only on D_w. If $w \mid p$, "$\sim$" means that $s''|_{G_{F'_{\tilde w}}}$ and ρ_w are points of the same irreducible component of the generic fiber of the ring of potentially crystalline liftings with weights $\{0,1,2\}$, crystalline over K', for all sufficiently large finite $K'/F'_{\tilde w}$ [10, §1.4]; that generic fiber is formally smooth and contains the crystalline one as a union of irreducible components (loc. cit.), so this component is D_w, and $s''|_{G_{F'_{\tilde w}}}$ is crystalline and lies on D_w. Moreover, if $w \mid 3$ the point $s''|_{G_{F'_{\tilde w}}}$ lies on no other component: the local components of the cuspidal representation π'' are generic, so the point is smooth by [10, Lemma 1.3.2 (1)] and [10, Theorem 2.1.1 (2)], and the generic fiber is regular, hence locally irreducible, at a smooth point [10, §1.3]. So r'' defines a point of $\mathcal{A}'$, and the components D_w are those that [10, Theorem 2.3.2] attaches to π'' and S'. The remaining hypotheses of that theorem hold by Step 2 (a)–(c), together with the following: F' is imaginary CM; S' contains the places above p; and π'' is unramified outside S' and has level potentially prime to p.

We may take for χ'' the quadratic Hecke character $\delta_{F'/(F')^+}$ of $\mathbb{A}_{(F')^+}^\times/((F')^+)^\times$. Indeed, s'' is polarized with multiplier μ, and $\mu|_{G_{F'}} = \varepsilon_p^{-2}$ as $K \subset F'$, so $(s'')^{\mathsf{c}} \cong (s'')^\vee \otimes \varepsilon_p^{-2}$. In the normalization of [10, Theorem 2.1.1 (2)], applied also to π''^{c} and $\pi''^\vee$, which are again regular algebraic, cuspidal and polarized, $r(\pi''^{\mathsf{c}}) \cong r(\pi'')^{\mathsf{c}}$ and $r(\pi''^\vee) \cong r(\pi'')^\vee \otimes \varepsilon_p^{-2}$; so $r(\pi''^{\mathsf{c}}) \cong r(\pi''^\vee)$, hence $\pi''^{\mathsf{c}}_w \cong \pi''^\vee_w$ at every finite place $w \nmid p$ of F', and $\pi''^{\mathsf{c}} \cong \pi''^\vee$ by strong

[2] The hypothesis of [7, Theorem A.4.1] on (π',χ') is printed as $(\bar r_{l,\imath}(\pi'), \bar r_{l,\imath}(\chi')) \cong (\bar r|_{G_{F'}}, \bar\mu|_{G_{F'}})$; the proof there uses $r_{l,\imath}(\chi')\varepsilon_l^{1-n}$ as the multiplier, and we use the hypothesis in this sense, as [13] do.

multiplicity one [70, Theorem 4.4]. As $\delta_{F'/(F')^+} \circ \mathrm{N}_{F'/(F')^+} = 1$ and $\delta_{F'/(F')^+,x}(-1) = -1 = (-1)^3$ at every infinite place x of $(F')^+$, the pair $(\pi'', \delta_{F'/(F')^+})$ is polarized in the sense of [10, §2.1]; the character $\delta_{F'/(F')^+}$ is unramified at every finite place, because only the places above 3 can ramify in $F' = (F')^+K$, and they split; and $r(\delta_{F'/(F')^+}) = \delta_{K/\mathbb{Q}}|_{G_{(F')^+}}$, both being the character of $G_{(F')^+}$ with kernel $G_{F'}$. So the multiplier $r(\chi'')\varepsilon_p^{-2}$ of the deformation problem of [10, Theorem 2.3.2] is $\mu|_{G_{(F')^+}}$, and that problem is $\mathcal{S}'$: two prolongations of $\bar\rho|_{G_{F'}}$ with multiplier $\bar\mu$ are conjugate, as the pairing is unique up to a scalar by Schur's lemma (Section 7.2). The theorem is stated over the ring of integers $\mathcal{O}_L$ of a finite extension L of E containing the images of the embeddings of F' and the coefficients of $r(\pi'')$ and $r(\chi'')$ (the components D_w are defined over E by the choice of E); as deformation rings commute with finite extensions of scalars, $\mathcal{A}'$ is a finite $\mathcal{O}_E$-module.

Step 6: the lift. By Steps 4 and 5, $\mathcal{A}$ is a finite $\mathcal{O}_E$-algebra, and by Step 1 its Krull dimension is at least 1. So $\mathcal{A}$ has a minimal prime $\mathfrak{q}$ with $\dim \mathcal{A}/\mathfrak{q} \geq 1$; then $\mathfrak{q} \cap \mathcal{O}_E = 0$, and $\mathcal{A}/\mathfrak{q}$ is a domain, finite and torsion free over $\mathcal{O}_E$, which embeds in the ring of integers of a finite extension of E. The resulting homomorphism $\mathcal{A} \to \overline{\mathbb{Z}}_p$ is the lift $\tilde\rho$. □

Proposition 12.22. *Let $p \geq 17$ be a prime with $p \equiv 2 \pmod 3$, let $v = p\mathcal{O}$, and let $\rho\colon G_K \to \mathrm{GL}_3(\overline{\mathbb{Q}}_p)$ be a continuous representation, unramified at all but finitely many primes, with the properties* (F1)–(F6) *read as in Section 12.7. Then there is a regular, polarized and odd, weakly irreducible compatible system $\mathcal{R} = \{R_\lambda\}$ of three-dimensional representations of G_K, with multiplier $\varepsilon_\ell^{-2}\delta_{K/\mathbb{Q}}$, whose p-adic member R_p has the properties:*

- (P1) *R_p is a lift of $\bar\rho$ and is unramified outside $\{\mathfrak{p}, v\}$;*
- (P2) *R_p is crystalline at v with Hodge–Tate weights $\{0,1,2\}$ at both embeddings of K_v; hence $H_\tau = \{0,1,2\}$ for both embeddings τ of K;*
- (P3) *$R_p|_{I_\mathfrak{p}} \cong \kappa \otimes \exp(t_p N)$ for a nilpotent matrix N.*

Proof. Let $\mathcal{C}_3$ be, as in Section 7.5, an irreducible component through $\rho_\mathcal{G}|_{G_{\mathbb{Q}_3}}$ of the generic fiber of the lifting ring of its inertial type, and let $\tilde\rho$ be the lift given by Lemma 12.21 for $\mathcal{C}_3$ and $\mathcal{C}_p$.

The compatible system. Let R_p be the representation of G_K defined by $\tilde\rho$. It is unramified outside $\{\mathfrak{p}, v\}$, crystalline at v with Hodge–Tate weights $\{0,1,2\}$ at both embeddings (it lies on $\mathcal{C}_p$), hence potentially diagonalizable at v. It is polarized and odd with multiplier $\varepsilon_p^{-2}\delta_{K/\mathbb{Q}}$, and its reduction $\bar\rho$ is irreducible on $G_{K(\zeta_p)}$. The proof of Lemma 7.4 applies to R_p in place of ρ, with the polarization of R_p (defined by $\tilde\rho$) in place of (F4) and of the pairing of Lemma 7.1, the paragraph "$\bar\rho$ is reasonable" in place of Proposition 7.2, and the single place v, with $K_v = \mathbb{Q}_{p^2}$ unramified over $\mathbb{Q}_p$, in place of v and $\bar v$ (so [10, Lemma 1.4.3 (2)] still applies). So R_p is the p-adic member of a regular, weakly irreducible compatible system $\mathcal{R}$, polarized and odd with multiplier $\varepsilon_\ell^{-2}\delta_{K/\mathbb{Q}}$. This is how [27, Lemma 4.2.3] obtains a compatible system from such a lift, when the places above p split.

Then (P1) and (P2) hold by construction, and (P3) follows from Lemma 7.6 applied to $R_p|_{G_{K_\mathfrak{p}}}$, whose reduction restricted to $I_\mathfrak{p}$ is $\bar\kappa|_{I_\mathfrak{p}}$ times a unipotent representation by (F3) (as in (7.1)). □

Remark 12.23. The theorem of Calegari, Emerton and Gee used in Part II, [27, Theorem 4.2.11], is stated with no condition on how the places above p decompose in the CM field [27, §1.5.19, §1.5.25], and its hypotheses hold for $p \equiv 2 \pmod 3$ as well, with $F = K$, $S = \{3, p\}$, the component $\mathcal{C}_p$ and any polarized component at 3. They are checked as in the proof of Theorem 7.3, with the paragraph "$\bar\rho$ is reasonable" in place of

Proposition 7.2, except for the global realizability of $\mathcal{C}_p$ [27, Definition 2.1.9]. That holds with the field K and the place p of $\mathbb{Q}$, as in the proof of Lemma 7.5: the proof of Lemma 7.4, read with the same substitution and with the single place v in place of v and $\bar{v}$, puts ρ in a regular, polarized and odd, weakly irreducible compatible system, and $\rho_{\mathcal{G}}|_{G_{\mathbb{Q}_p}}$ lies on $\mathcal{C}_p$ by the definition of $\mathcal{C}_p$. We do not use that theorem for $p \equiv 2 \pmod 3$: a more direct argument suffices. Its proof reaches a globally realizable component at p by swapping components between compatible systems [27, §4.2]. Here the points of $\mathcal{C}_p$ are potentially diagonalizable on G_{K_v}, so the lifting argument of Bellovin and Gee [13, Theorem 5.2.1], run over a field in which the places above p split, gives the lift without that step (Lemma 12.21). Propositions 12.22 and 12.24 rest on this lemma (see the beginning of Section 12.8).

The same argument proves Theorem 7.3 for $p \equiv 1 \pmod 3$, for the component $\mathcal{C}_p$ of Section 7.5 and every polarized component $\mathcal{C}_3$ at 3, without [27, Theorem 4.2.11]. Indeed, Lemma 12.21 and its proof hold for $p \equiv 1 \pmod 3$, with the following changes. The representation ρ is that of Section 7.1, and Proposition 7.2 replaces the paragraph "$\bar{\rho}$ is reasonable". The component $\mathcal{C}_p$ is that of Section 7.5; by [27, Lemma 1.5.20], as p splits in K, it is the component defined in Section 12.8. In Step 2 the condition on $\left(\frac{d}{p}\right)$ is not needed, because, -3 being a square in $\mathbb{Q}_p$, the places above p split in every CM field containing K; and, as F_1 is unramified at p, the completions $F_{1,y}$, $y \mid p$, are $\mathbb{Q}_p$ or $\mathbb{Q}_{p^2}$, unramified over $\mathbb{Q}_p$ and containing K_v or $K_{\bar{v}}$, as [10, Lemma 1.4.3 (2)] requires. In Step 3, K_v becomes K_v or $K_{\bar{v}}$, both equal to $\mathbb{Q}_p$. The representation of G_K defined by the lift is crystalline at v with Hodge–Tate weights $\{0, 1, 2\}$, as its restriction to G_{K_v} lies on $\mathcal{C}_p$, and hence at $\bar{v}$, by its polarization, as in (P2) of Section 7.6. The proof of Lemma 7.4, applied to it, with the polarization given by the lift in place of (F4) and these properties in place of (F2), gives a compatible system with the properties stated in Theorem 7.3. With the component $\mathcal{C}_3'$ of the proof of Proposition 9.5 in place of $\mathcal{C}_3$, this proves step (5) of that proof as well.

With Proposition 12.22 in place of Theorem 7.3 and Lemma 7.5, the rest of Part II holds for $p \equiv 2 \pmod 3$, with $v = p\mathcal{O}$ and $\bar{v}$ omitted. The proof of Proposition 7.8, which gives (M1)–(M3), uses Lemma 7.7, which applies to $\mathcal{R}$ because it is regular, polarized and odd, and weakly irreducible. In the proof of that lemma a place y of F' above v still has $F'_y = K_v$, although y is now inert over $(F')^+$, and [10, Theorem 2.1.1 (2)] and [9, Theorem 1.1] are stated for all places, split or not. The same situation already occurs in the proof of (M2) at the inert prime 5. The proof of Proposition 7.9 uses (F5) at the prime $\mathfrak{P} = p\mathcal{O}$ and item C2, whose ideals have no prime factor above p. Sections 8 and 9, in particular Theorem 9.3, concern the members above 5 and use only (M1)–(M3), (F3), Proposition 7.9 and the polarization of these members, so p enters them only through $5 \notin \{3, 7, p\}$. That leaves Proposition 9.5, whose proof applies Theorem 7.3 again with another component at 3. It is proved for inert p in Section 12.10 (Proposition 12.24).

12.10. **Part III at an inert prime.** In this subsection $p \geq 17$ is a prime with $p \equiv 2 \pmod 3$, $v = p\mathcal{O}$, and ρ is as in Proposition 12.22. We first prove Proposition 9.5 for ρ.

Proposition 12.24. *The group $\bar{\rho}(I_{\mathfrak{p}})$ is not contained in the group of scalar matrices.*

Proof. Suppose that it is. We construct a compatible system with the properties stated in Proposition 12.22 whose matrix N in (P3) is zero. This contradicts Theorem 9.3 (2), which holds for such systems by the paragraph after Remark 12.23.

Steps (1)–(4) of the proof of Proposition 9.5 use only the properties (F3), (F4), (F6) of ρ and the prolongation $\bar{\rho}_{\mathcal{G}}$ (Lemma 7.1), and apply unchanged for inert p; the residue field

$\mathbb{F}'$ there can be taken to contain $\mathbb{F}_{p^2}$, and the element $t \equiv 1$ of step (2) exists because p is odd. They give a lift $\rho'_{\mathcal{G}}$ of $\bar\rho_{\mathcal{G}}|_{G_{\mathbb{Q}_3}}$ with multiplier $\varepsilon_p^{-2}\delta_{K/\mathbb{Q}}$, trivial on an open subgroup of the inertia group, and an irreducible component $\mathcal{C}'_3$ through it of the generic fiber of the lifting ring of its inertial type, at all of whose points the monodromy operator vanishes ([13, Theorem 3.3.7 and the paragraph before it], as in step (4) of the proof of Proposition 9.5).

Instead of step (5), apply Lemma 12.21 with $\mathcal{C}'_3$ in place of $\mathcal{C}_3$; the lemma allows any polarized component at 3. It gives a lift $\tilde\rho' \colon G_{\mathbb{Q}} \to \mathcal{G}_3(\overline{\mathbb{Z}}_p)$ of $\bar\rho_{\mathcal{G}}$, unramified outside $\{3, p\}$, with multiplier $\varepsilon_p^{-2}\delta_{K/\mathbb{Q}}$, whose restrictions to $G_{\mathbb{Q}_3}$ and $G_{\mathbb{Q}_p}$ lie on $\mathcal{C}'_3$ and $\mathcal{C}_p$. As in the proof of Proposition 12.22 (the proof of Lemma 7.4, with the substitutions made there, applied to the representation of G_K defined by $\tilde\rho'$), the representation of G_K defined by $\tilde\rho'$ is the p-adic member of a compatible system $\mathcal{R}'$ with the properties stated in Proposition 12.22. The restriction of $\tilde\rho'$ to $G_{\mathbb{Q}_3}$ lies on $\mathcal{C}'_3$, so the monodromy of the p-adic member of $\mathcal{R}'$ at $\mathfrak{p}$ is zero: $N = 0$ in (P3). □

With Proposition 12.24 in place of Proposition 9.5, Part III holds for $p \equiv 2 \pmod 3$, with $v = p\mathcal{O}$ and $\bar v$ omitted. The proof of Corollary 10.3 uses (F3), (F4), (F6), (P1), (P3) and Proposition 9.5, and applies Proposition 10.2 with $\ell = p \geq 17$ over a finite field of characteristic p, which can be taken to contain $\mathbb{F}_{p^2}$. Propositions 10.4 and 10.5 rest on Lemma 7.7, which applies to the system of Proposition 12.22 because it is regular, weakly irreducible, and polarized and odd (all its members are polarized, by the proof of Proposition 12.22). In the proof of that lemma, as $F' = (F')^+K$, a place y of F' above $\mathfrak{p}$ has $F'_y = K_{\mathfrak{p}}$, and a place y above v has $F'_y = \mathbb{Q}_p \otimes_{\mathbb{Q}} K = K_v = \mathbb{Q}_{p^2}$. Propositions 10.6 and 10.7 and Section 11 concern $K_{\mathfrak{p}}$ and the member at 3 only, and do not involve p. Consequently:

Proposition 12.25. *Let $p \geq 17$ be a prime, split or inert in K. There is no continuous representation $\rho \colon G_K \to \mathrm{GL}_3(\overline{\mathbb{Q}}_p)$, unramified at all but finitely many primes, with the properties* (F1)–(F6) *(read as in Section 12.7 if p is inert). Here* (F3) *means that $\rho|_{I_{\mathfrak{p}}}$ is $\kappa|_{I_{\mathfrak{p}}}$ times a unipotent representation for some character $\kappa \colon G_K \to \mu_3$ with $\kappa^{\mathsf{c}} = \kappa^{-1}$ whose restriction to $G_{K_{\mathfrak{p}}}$ is trivial or has conductor $\mathfrak{p}^2$, and in* (F5) *the $\xi_{\mathfrak{q}}$ are any elements of μ_3.*

Proof. For $p \equiv 1 \pmod 3$ this is what the proof of Theorem 11.18 shows, since it uses nothing else about ρ. For $p \equiv 2 \pmod 3$, take the system of Proposition 12.22 and argue in the same way, with Proposition 12.24 and the transfer of Parts II and III described above. □

12.11. The proof for $p \geq 17$, and the equations with $k \geq 2$.

Proof of Theorem 12.4. Let $p \geq 17$ and $k \geq 1$, and let (a, b, c) be a solution with $3 \mid c$, or with $k \geq 8$; for $k = 1$, $3 \mid c$ holds automatically (Lemma 12.6 (ii)). Then $\nu = k + p\,v_3(c) \geq 8$. The representation ρ of Section 12.7 is unramified at all but finitely many primes and has the properties (F1)–(F6) (Propositions 12.19 and 12.20). This contradicts Proposition 12.25. □

Remark 12.26 (the equations with $k \geq 2$). Let $k \geq 2$. If $k \geq p$, then $3^k z^p = 3^{k-p}(3z)^p$, so a solution for k is a solution for $k - p$ with $3 \mid z$; statements (1) and (2) below depend on k only through $2k - 3$ modulo p and through the condition "$3 \mid z$ or $k \geq 8$", and are compatible with this reduction.

(1) *For $p \geq 7$:* there is no solution unless $2k - 3$ is a nonzero square modulo p (Theorem 12.2 (a)). When it is, every solution has z odd, exactly one of x, y even and $\equiv 2 \pmod 4$, and $p \nmid z$; if $p \neq 7$, also $7 \nmid xyz$ and $x^3 \equiv y^3 \pmod 7$; and, for a normalized solution, $\bar\rho_{E'_{x,y},p} \cong \bar\rho_{W',p}$ (Theorem 12.9, Remark 12.10 (2)). For

$k \geq 8$ and $p \in \{7, 11, 13\}$ we know only what Theorem 12.2 gives, directly or after the reduction of k modulo p above.

(2) *For $p \geq 17$:* there is no solution with $3 \mid z$, and none at all if $k \geq 8$ (Theorem 12.4). So the solutions that are not excluded have $3 \nmid z$ and $2 \leq k \leq 7$, with $2k - 3 \in \{1, 3, 5, 7, 9, 11\}$ a square modulo p.

(3) $k = 2$. The solution $2^3 + 1^3 = 9 \cdot 1^p$ has $3 \nmid z$, as it must: its parameter has $v_3(s_0) = 2$, outside the disc of Theorem 4.1 (Section 13).

(4) $3 \leq k \leq 7$ *and* $3 \nmid z$. Here $v_3(s_0) = k \leq 7$, and Theorem 4.1 gives no information on $\mathbb{V}_{s_0}$ at $\mathfrak{p}$. For $7 \leq p \leq 10^6$ there is no solution (Theorem 12.2 (c)). There is no solution with $z = \pm 1$ for any $k \geq 3$: if $x^3 + y^3 = \pm 3^j$ with $\gcd(x, y) = 1$ and $j \geq 1$, then $x + y$ and $x^2 - xy + y^2$ are, up to sign, powers of 3, and $v_3(x^2 - xy + y^2) = 1$ (Lemma 12.6 (ii)), so $x^2 - xy + y^2 = 3$, whose solutions give $x^3 + y^3 \in \{0, \pm 9\}$.

Complements

13. Remarks

We explain why the Catalan solution $1^3 + 2^3 = 3^2$ plays no part in the proofs, how the arguments of Parts I–III carry over to the exponents $p \equiv 2 \pmod 3$, and which questions remain open.

13.1. **The obstructing point.** The Catalan solution $1^3 + 2^3 = 3^2$, of exponent 2, gives, with $(u, w) = (1, 2)$, the parameter $s_0 = 9$, and with $(u, w) = (2, 1)$ the parameter $s_0 = 9/8$; in both cases $v_3(s_0) = 2$, outside the disc of Theorem 4.1. So nothing in the proofs concerns these points, as must be the case, since $x^3 + y^3 = z^2$ has this solution. The exponent enters through $v_3(s_0) = p\, v_3(c)$, and also through the conditions $p \geq 17$ in Kraus's results, $p \notin \{2, 3, 7, 13\}$ in Theorem 6.2, $p \notin \{2, 3, 13\}$ in Lemma 7.6, and $p > 8$ in the theorem of Calegari, Emerton and Gee.

13.2. **Exponents $p \equiv 2 \pmod 3$.** For $p \equiv 2 \pmod 3$ the prime p is inert in K. For $x^3 + y^3 = z^p$ these exponents are settled by Freitas's theorem [58, Theorem 3]. Part IV carries out the arguments of Parts I–III at an inert prime, for $x^3 + y^3 = 3z^p$ (Sections 12.7 to 12.10). None of the arguments at $\mathfrak{p}$, $\mathfrak{l}$ and $\bar{\mathfrak{l}}$, nor those at 5 in Part II, depends on whether p splits in K. This transfer also proves Theorem A for the prime exponents $p \geq 17$ with $p \equiv 2 \pmod 3$, without Freitas's theorem: Proposition 5.1 and Lemma 5.2 hold for every $p \geq 17$, and for such p the proof of Proposition 5.5, with Lemma 12.18 in place of Proposition 5.6, together with Lemma 6.1 and Proposition 12.20, shows that the Frey representation, defined as in Definition 5.4, has all the properties that Proposition 12.25 excludes. That proof rests on Lemma 12.21; Corollary 11.19 uses Freitas's theorem instead, so that Theorem A does not depend on Part IV.

13.3. **Open questions.** Three questions remain open. The first is to find all solutions of $x^3 + y^3 = 9z^4$ (Remark 12.5). The second concerns the equations $x^3 + y^3 = 3^k z^p$ with $k \geq 2$ that Remark 12.26 leaves open, among them those with $3 \leq k \leq 7$, $3 \nmid z$ and $p > 10^6$, on whose parameters Theorem 4.1 gives no information. The third is whether the radius $15/2$ of Theorem 4.1 is optimal (Remark 4.17). Beyond these questions, the method relies on features of this case: the divisibility $3 \mid c$ (Proposition 5.1, Lemma 12.6), which puts the parameter of a solution in the disc of Theorem 4.1; a reasonable residual representation, so that a compatible system exists (Theorem 7.3 and Lemma 12.21); the Hodge–Tate weights

$\{0, 1, 2\}$, which lie in the Fontaine–Laffaille range at 5 and make the member at 3 ordinary once its monodromy operator is regular (Proposition 10.6); and two features of K: its single prime above 3 and its class number one imply that an inertia group at $\mathfrak{p}$ is the whole Galois group of the maximal pro-3 extension of K unramified outside $\mathfrak{p}$ (Lemma 11.16), and the ramification at $\mathfrak{p}$ bounds the root discriminants of the fields cut out by the reductions of the member by $3^{449/162} < 21.01$ (Proposition 11.11), below Odlyzko's bounds for fields of large degree. Theorem 4.1 and Proposition 11.21, by contrast, are statements about $\mathbb{V}$ and about representations of G_K, not about the equation. For another equation the same route would need a family that separates the solutions from the obstructing ones at some prime, as Theorem 4.1 does here at $\mathfrak{p}$, and then analogues of the other features above.

Appendix A. Computations

This appendix lists the computations on which the proofs of Parts I–III depend, with what each computes and its output: items C1–C3 concern Part I, item C4 Part II, which also uses C2, and item C5 Part III. They are finite exact computations in $\mathbb{Z}$, $\mathbb{Z}[\omega]$, $\mathbb{Z}[\zeta_9]$, number fields, finite fields and the rings $\mathbb{Z}/7^N$, except items C4 and C5, which are evaluations of integrals with certified error bounds, in interval and ball arithmetic [72]. The programs are written in PARI/GP [111] (version 2.17.3), Python 3.12 (with python-flint 0.8.0 on FLINT 3.3.0 for ball arithmetic, mpmath 1.4.1 and SymPy 1.14.0), GAP [110] 4.15.1 and SageMath 10.9 (used only for cross-checks), with one program in C. For each of the items C1–C5 the record [71] also contains a second, separately written program (for C1, at $\mathfrak{l}$ and for one m' in each class), which gives the same results. On a laptop each program for items C1–C5 runs in a minute or less, most in a few seconds, except the program of item C1 that checks Lemma 3.8 for $k = 1$ and $s = 2$ by counting the fixed points of $F \circ g$ directly, which takes about three minutes. The computations for Part IV are items S12–S24 of the Supplement; the subsection after item C5 summarizes the search of items S14–S16 and the 7-adic logarithms of items S22 and S24. We write ω for the image of $\omega \in K$ in the coefficients, and identify $\mathcal{O}/\mathfrak{l}$ and $\mathcal{O}/\bar{\mathfrak{l}}$ with $\mathbb{F}_7$ by $\omega \mapsto 2$ and $\omega \mapsto 4$.

C1. Traces of $\mathbb{V}$ at the primes above 7. This is the input of Proposition 3.9. For $\mathfrak{q} \in \{\mathfrak{l}, \bar{\mathfrak{l}}\}$, each $m' \in (\mathbb{Z}/9)^\times$, $k \in \{1, 2, 3\}$ and every $s \in \mathbb{F}_{7^k} \smallsetminus \{0, 1\}$, the sums of Lemma 3.8 were evaluated exactly, as integer combinations of powers of a primitive ninth root of unity. The character ϑ is the power map $z \mapsto z^{38}$ into $\mu_9(\mathbb{F}_{343})$, identified with the ninth roots of unity of the coefficients so that the cube roots of unity correspond to the reductions of $1, \omega, \omega^2$. Every value lies in $\mathbb{Z}[\omega]$. The results depend only on the class of m' modulo 3:

	class I	class II
traces at $s = 2$ $(k = 1, 2, 3)$	$6 - 3\omega,\ -99 - 87\omega,\ -267 - 486\omega$	$9 + 3\omega,\ -12 + 87\omega,\ 219 + 486\omega$
$P(T)$ at $s = 2$	$P^+(T)$	$P^-(T)$
power sums on H^1_c	$1 + 2\omega,\ 95 + 94\omega,\ -285$	$-1 - 2\omega,\ 1 - 94\omega,\ -285$
$\Omega(T)$	$(T-1)(T^2 - 2\omega T + 49\omega^2)$	$(T-1)(T^2 - 2\omega^2 T + 49\omega)$

At $\mathfrak{l}$, class I is $m' \equiv 2 \pmod 3$; at $\bar{\mathfrak{l}}$, it is $m' \equiv 1 \pmod 3$.

C2. The irreducibility test. This is Step 5 of the proof of Theorem 6.2; it is used again in the proof of Proposition 7.9. With $\varpi = 2 - \omega$, for each assignment $(P_\mathfrak{l}, P_{\bar{\mathfrak{l}}}) \in \{(P^+, P^-), (P^-, P^+)\}$, each type $(k, k') \in \mathcal{T}$ and each $(\zeta_1, \zeta_2) \in \mu_3^2$, the elements $P_\mathfrak{l}(\zeta_1 \varpi^k \bar{\varpi}^{k'})$ and $P_{\bar{\mathfrak{l}}}(\zeta_2 \bar{\varpi}^k \varpi^{k'})$ of $\mathcal{O}$ are nonzero, and the ideal they generate was factored. The rational primes below its prime factors, taken together over all (ζ_1, ζ_2), are:

type	$(0,0)$	$(1,1)$	$(2,2)$	$(0,2)$	$(2,0)$
(P^+,P^-)	$2,3$	$2,3,7$	$2,3,7$	$2,3,13$	$2,3,7$
(P^-,P^+)	$2,3$	$2,3,7$	$2,3,7$	$2,3,7$	$2,3,13$

No prime $p \geq 17$ occurs.

C3. Ray class groups. This is used in the proof of Proposition 4.16. The ray class groups $\mathrm{Cl}_{\mathfrak{p}^k}(K)$ for $k = 1, \dots, 8$ have orders $1, 1, 3, 9, 27, 81, 243, 729$; $\mathrm{Cl}_{\mathfrak{p}^4}(K) \cong (\mathbb{Z}/3)^2$. The classes of $\mathfrak{l} = (2-\omega)$ and $\overline{\mathfrak{l}} = (3+\omega)$ generate $\mathrm{Cl}_{\mathfrak{p}^4}(K)$. Equivalently, the images of $2-\omega$ and $3+\omega$ generate $(\mathcal{O}/\mathfrak{p}^4)^\times/\mu_6$, a group of order 9.

C4. Lower bounds for root discriminants. This is the input of Proposition 8.3. The right side of (8.2), with $r_1 = 0$ and the test function $\Phi_0(x/b)/\cosh(x/2)$ of Section 8.3, was evaluated with certified error bounds in the following cases. The third column gives the exponential of the value found, truncated, and the last the constant with which it is compared in the text.

n	b	bound for $\mathrm{rd}(L)$	constant
18	23/4	$9.27091\dots$	$3^{1/2}\cdot 5 = 8.66025\dots$
120	13	$16.98861\dots$	$3^{1/2}\cdot 5^{7/5} = 16.48612\dots$
2002	36	$21.41368\dots$	$3^{1/2}\cdot 5^{3/2} = 19.36491\dots$

The values of b are, to within $\frac{1}{4}$, those that maximize the bounds.

C5. Root discriminants. This is the input of Proposition 11.12, with the constants of Proposition 11.11. The right side of (8.2), with $r_1 = 0$ and the test function $\Phi_0(x/b)/\cosh(x/2)$, was evaluated in two ways, each with certified error bounds. The first uses ball arithmetic with Arb [72], at 160 bits. With $\delta = 10^{-8}$, the integral over $[\delta, b]$ is computed by Arb's rigorous numerical integration, and the integral over $[0,\delta]$ is bounded by $0 \leq \int_0^\delta (1 - \Phi_0(x/b)/\cosh(x/2)) \frac{dx}{2\sinh(x/2)} \leq (\frac{\pi+\pi^2}{2b^2} + \frac{1}{8})\frac{\delta^2}{2}$, an elementary consequence of $\Phi_0(0) = 1$, $\Phi_0'(0) = 0$, $0 \leq \Phi_0 \leq 1$ and $|\Phi_0''| \leq \pi + \pi^2$; the integral over $[b,\infty)$ is $-\log\tanh(b/4)$ in closed form, and $I_2 = 4b/\pi^2$. The second uses interval arithmetic with Taylor models of degree 12 on a dyadic subdivision, at 200 bits. The results, truncated:

n	b	bound for $\mathrm{rd}(L)$	constant	margin in $\log \mathrm{rd}$
1378	63/2	$21.1515190\dots$	$3^{449/162} = 21.0083345\dots$	$6.79\cdot 10^{-3}$
674	25	$20.4476673\dots$	$T_3 = 3^{437/162} = 19.3664184\dots$	$5.43\cdot 10^{-2}$
118	12	$16.9179477\dots$	$T_2 = 3^{137/54} = 16.2358224\dots$	$4.11\cdot 10^{-2}$
80	10	$15.6281490\dots$	$3^{5/2} = 15.5884572\dots$	$2.54\cdot 10^{-3}$
24	6	$10.5939560\dots$	$3^{11/6} = 7.4941485\dots$	0.346
20	6	$9.7691231\dots$	$T_1 = 3^{37/18} = 9.5664156\dots$	$2.09\cdot 10^{-2}$
4	2	$3.2422670\dots$	$3^{1/2} = 1.7320508\dots$	0.626

The last column is a lower bound for the logarithm of the bound minus that of the constant. The smallest margin, $2.54\cdot 10^{-3}$ at $n = 80$, is more than 10^5 times the width of the enclosures: both evaluations enclose each bound in an interval of width below $4\cdot 10^{-9}$ in $\log \mathrm{rd}$.

Part IV: the search and the 7-adic logarithms. *Items S14–S16.* For Theorem 12.2 (b) and (c) the program takes each prime p in a range and runs through $n = 2, 4, 6, \dots$ up to a bound, keeping the n for which $q = np + 1$ is prime. For such a q it computes $a_q(W)$ and tests (A) of Proposition 12.11; if (A) holds, it runs through the n elements ζ of $9^{1-k}\mu_n(\mathbb{F}_q)$,

tests whether $d_2 = (12\zeta - 1)/3$ is a square in $\mathbb{F}_q$, and if it is, computes $a_q(E_\zeta)$ for one square root d and compares $a_q(E_\zeta)^2$ with $a_q(W)^2$ modulo p. It records the least n for which (A) and (B_k) hold. The traces a_q are computed by PARI's `ellap`, and $\mu_n(\mathbb{F}_q)$ is generated by g^p for a primitive root g modulo q. For $k = 1$ the 5 761 453 primes $5 \le p < 10^8$ were treated with n up to 600, 2000 and 4000 for $p \le 10^5$, $10^5 < p < 10^7$ and $10^7 < p < 10^8$: such an n exists except for $p = 5$ and $p = 13$, the largest n needed in the three ranges is 112, 234 and 284, and the running times printed by the program add up to about an hour on a laptop (3 787 seconds). A second program, written separately, uses the curves $E'_{a',b'}$ and W' in place of E_ζ and W, and generates $\mu_n(\mathbb{F}_q)$ by x^p for the least $x \ge 2$ for which x^p has order n; on each range it gives the same exceptions, the same largest n, and the same number of primes for each least n. For $3 \le k \le 7$, $7 \le p \le 10^6$ and n up to 2000, both programs find such an n for every prime except those listed in the proof of Theorem 12.2 (c), with largest n equal to 220; each run takes less than thirty seconds.

Items S22 and S24. In the Chabauty steps of Propositions 12.14, 12.15 and 12.16, (L_0, L_1) is computed as $\log(ND)/N$ (with G_1 in place of D for Γ_7), where $N = 25$ for Γ_1 and $N = 50$ for Γ_5 and Γ_7. The multiple $ND = [P_1 + P_2 - 2\infty]$ is computed exactly over $\mathbb{Q}$ by Cantor's algorithm, and $\log(ND)$ is computed inside one residue disc by termwise integration of power series with coefficients in $\mathbb{Z}_7$, with 7-adic numbers to precision 7^{40} and 80 terms (for Γ_1) or 120 terms. This gives L_0 and L_1 modulo 7^{30} at least; the proofs use them only modulo 7^2. As checks, the same computation for other multiples of D (and of D', where $2D' = D$, for Γ_1) gives the same values of $\log(D)$ to that precision, and SageMath's implementation of Coleman integration, a different algorithm, gives the same digits of L_0 and L_1 (modulo 7^{20} for Γ_1, and 7^6 for Γ_5 and Γ_7). These programs run in less than half a minute.

Data availability. The programs, their outputs and the commands that run them are in [71].

Declarations

Research methodology. The author designed and operated the multi-agent research system used in this work, built on Anthropic Claude Opus 5.5. The system carried out literature analysis, mathematical development and computation, with checks assigned to agents separate from those developing the arguments.

Funding. This research did not receive any specific grant from funding agencies in the public, commercial, or not-for-profit sectors.

Declaration of competing interests. The author declares no competing financial interests or personal relationships that could have appeared to influence the work reported in this paper.

Declaration of generative AI and AI-assisted technologies in the manuscript preparation process. Anthropic Claude Opus 5.5 was used to draft and revise the manuscript. The author reviewed the material and takes full responsibility for the article.

References

1. Victor Abrashkin, *Modular representations of the Galois group of a local field and a generalization of a conjecture of Shafarevich*, Izv. Akad. Nauk SSSR Ser. Mat. **53** (1989), no. 6, 1135–1182, English translation: Math. USSR-Izv. **35** (1990), no. 3, 469–518.
2. ———, *Ramification estimate for Fontaine–Laffaille Galois modules*, J. Algebra **427** (2015), 319–328.

3. ———, *Groups of automorphisms of local fields of period p and nilpotent class $< p$, II*, Internat. J. Math. **28** (2017), no. 10, 1750066, Part I: Internat. J. Math. **28** (2017), no. 6, 1750043; cited by the numbering of arXiv:1403.4121v5.
4. ———, *Groups of automorphisms of local fields of period p^M and nilpotent class $< p$*, Ann. Inst. Fourier (Grenoble) **67** (2017), no. 2, 605–635.
5. Michael Artin, Alexander Grothendieck, and Jean-Louis Verdier, *Théorie des topos et cohomologie étale des schémas (SGA 4), Tome 3*, Lecture Notes in Math., vol. 305, Springer, 1973.
6. Meng Bai and Zhongfeng Zhang, *On the Diophantine equation $x^3 + y^3 = 2z^{2n}$*, J. Southwest China Normal Univ. Nat. Sci. Ed. **39** (2014), no. 6, 14–17, in Chinese.
7. Thomas Barnet-Lamb, Toby Gee, and David Geraghty, *Serre weights for rank two unitary groups*, Math. Ann. **356** (2013), no. 4, 1551–1598.
8. Thomas Barnet-Lamb, Toby Gee, David Geraghty, and Richard Taylor, *Local-global compatibility for $l = p$, I*, Ann. Fac. Sci. Toulouse Math. (6) **21** (2012), no. 1, 57–92.
9. ———, *Local-global compatibility for $l = p$, II*, Ann. Sci. Éc. Norm. Supér. (4) **47** (2014), no. 1, 165–179.
10. ———, *Potential automorphy and change of weight*, Ann. of Math. (2) **179** (2014), no. 2, 501–609.
11. Alexander Beilinson, *On the crystalline period map*, Camb. J. Math. **1** (2013), no. 1, 1–51, cited by the numbering of arXiv:1111.3316v4, whose §§1.15–1.17 differ from the journal version.
12. Joël Bellaïche and Gaëtan Chenevier, *Formes non tempérées pour $U(3)$ et conjectures de Bloch–Kato*, Ann. Sci. Éc. Norm. Supér. (4) **37** (2004), no. 4, 611–662.
13. Rebecca Bellovin and Toby Gee, *G-valued local deformation rings and global lifts*, Algebra Number Theory **13** (2019), no. 2, 333–378, in arXiv:1708.04885v3 the results of §3.3 are numbered one higher.
14. Michael A. Bennett, Carmen Bruni, and Nuno Freitas, *Sums of two cubes as twisted perfect powers, revisited*, Algebra Number Theory **12** (2018), no. 4, 959–999.
15. Michael A. Bennett and Pranabesh Das, *Gaps between cubes with perfect power sum*, Bull. Lond. Math. Soc. **57** (2025), no. 10, 3051–3060.
16. Michael A. Bennett, Florian Luca, and Jamie Mulholland, *Twisted extensions of the cubic case of Fermat's Last Theorem*, Ann. Sci. Math. Québec **35** (2011), no. 1, 1–15.
17. Laurent Berger, *Représentations p-adiques et équations différentielles*, Invent. Math. **148** (2002), no. 2, 219–284.
18. Jonas Bergström and Gerard van der Geer, *Picard modular forms and the cohomology of local systems on a Picard modular surface*, Comment. Math. Helv. **97** (2022), no. 2, 305–381.
19. Vladimir G. Berkovich, *Étale cohomology for non-Archimedean analytic spaces*, Publ. Math. Inst. Hautes Études Sci. **78** (1993), 5–161.
20. Frits Beukers and Gert Heckman, *Monodromy for the hypergeometric function ${}_nF_{n-1}$*, Invent. Math. **95** (1989), no. 2, 325–354.
21. Nicolas Billerey, Imin Chen, Lassina Dembélé, Luis Dieulefait, and Nuno Freitas, *Some extensions of the modular method and Fermat equations of signature $(13, 13, n)$*, Publ. Mat. **67** (2023), no. 2, 715–741.
22. Nicolas Billerey, Imin Chen, Luis Dieulefait, and Nuno Freitas, *A multi-Frey approach to Fermat equations of signature (r, r, p)*, Trans. Amer. Math. Soc. **371** (2019), no. 12, 8651–8677.
23. ———, *On Darmon's program for the generalized Fermat equation, I*, J. Reine Angew. Math. **822** (2025), 107–146, cited by the numbering of arXiv:2205.15861v5.
24. ———, *On Darmon's program for the generalized Fermat equation, II*, Math. Comp. **94** (2025), no. 354, 1977–2003, cited by the numbering of arXiv:2308.07062v2.
25. Christophe Breuil, Brian Conrad, Fred Diamond, and Richard Taylor, *On the modularity of elliptic curves over $\mathbf{Q}$: wild 3-adic exercises*, J. Amer. Math. Soc. **14** (2001), no. 4, 843–939.
26. Nils Bruin, *On powers as sums of two cubes*, Algorithmic number theory (Leiden, 2000), Lecture Notes in Comput. Sci., vol. 1838, Springer, Berlin, 2000, pp. 169–184.
27. Frank Calegari, Matthew Emerton, and Toby Gee, *Globally realizable components of local deformation rings*, J. Inst. Math. Jussieu **21** (2022), no. 2, 533–602, cited by the numbering of arXiv:1807.03529v3.
28. Ana Caraiani, *Monodromy and local-global compatibility for $l = p$*, Algebra Number Theory **8** (2014), no. 7, 1597–1646.
29. J. W. S. Cassels and E. V. Flynn, *Prolegomena to a middlebrow arithmetic of curves of genus 2*, London Mathematical Society Lecture Note Series, vol. 230, Cambridge University Press, Cambridge, 1996.
30. Imin Chen and Samir Siksek, *Perfect powers expressible as sums of two cubes*, J. Algebra **322** (2009), no. 3, 638–656.

31. Laurent Clozel, Michael Harris, and Richard Taylor, *Automorphy for some l-adic lifts of automorphic mod l Galois representations*, Publ. Math. Inst. Hautes Études Sci. **108** (2008), 1–181.
32. Robert F. Coleman, *Effective Chabauty*, Duke Math. J. **52** (1985), no. 3, 765–770.
33. Pierre Colmez and Jean-Marc Fontaine, *Construction des représentations p-adiques semi-stables*, Invent. Math. **140** (2000), no. 1, 1–43.
34. J. H. Conway, R. T. Curtis, S. P. Norton, R. A. Parker, and R. A. Wilson, *Atlas of finite groups*, Oxford University Press, Eynsham, 1985.
35. Sander R. Dahmen, *Classical and modular methods applied to Diophantine equations*, Ph.D. thesis, Utrecht University, 2008, http://hdl.handle.net/1874/29640.
36. Henri Darmon, *Rigid local systems, Hilbert modular forms, and Fermat's last theorem*, Duke Math. J. **102** (2000), no. 3, 413–449.
37. Henri Darmon and Andrew Granville, *On the equations* $z^m = F(x, y)$ *and* $Ax^p + By^q = Cz^r$, Bull. Lond. Math. Soc. **27** (1995), no. 6, 513–543.
38. Rachel Davis and Rachel Pries, *Cohomology groups of Fermat curves via ray class fields of cyclotomic fields*, J. Algebra **554** (2020), 78–105, cited by the numbering of arXiv:1806.08352v3.
39. A. J. de Jong, *Étale fundamental groups of non-Archimedean analytic spaces*, Compos. Math. **97** (1995), no. 1–2, 89–118.
40. Pierre Deligne, *La conjecture de Weil. I*, Publ. Math. Inst. Hautes Études Sci. **43** (1974), 273–307.
41. ———, *La conjecture de Weil. II*, Publ. Math. Inst. Hautes Études Sci. **52** (1980), 137–252.
42. ———, *Un théorème de finitude pour la monodromie*, Discrete groups in geometry and analysis (New Haven, Conn., 1984), Progr. Math., vol. 67, Birkhäuser Boston, 1987, pp. 1–19.
43. ———, *Le groupe fondamental de la droite projective moins trois points*, Galois groups over **Q** (Berkeley, CA, 1987), Math. Sci. Res. Inst. Publ., vol. 16, Springer, 1989, pp. 79–297.
44. Pierre Deligne and Nicholas Katz, *Groupes de monodromie en géométrie algébrique (SGA 7 II)*, Lecture Notes in Math., vol. 340, Springer, 1973.
45. Michael Dettweiler and Claude Sabbah, *Hodge theory of the middle convolution*, Publ. Res. Inst. Math. Sci. **49** (2013), no. 4, 761–800.
46. Fred Diamond and Jerry Shurman, *A first course in modular forms*, Graduate Texts in Mathematics, vol. 228, Springer-Verlag, New York, 2005.
47. Leonard Eugene Dickson, *Linear groups, with an exposition of the Galois field theory*, B. G. Teubner, Leipzig, 1901.
48. Luis Dieulefait and Franco Golfieri Madriaga, *On Fermat's Last Theorem over the* $\mathbb{Z}_3$*-extension of* $\mathbb{Q}$ *and other fields*, 2025, preprint, arXiv:2507.16883v1.
49. Luis V. Dieulefait, *Existence of families of Galois representations and new cases of the Fontaine–Mazur conjecture*, J. Reine Angew. Math. **577** (2004), 147–151.
50. Bas Edixhoven, *Néron models and tame ramification*, Compos. Math. **81** (1992), no. 3, 291–306.
51. Xander Faber, *Finite p-irregular subgroups of* $\mathrm{PGL}_2(k)$, La Matematica **2** (2023), 479–522.
52. Roman Fedorov, *Variations of Hodge structures for hypergeometric differential operators and parabolic Higgs bundles*, Int. Math. Res. Not. IMRN (2018), no. 18, 5583–5608.
53. Jean-Marc Fontaine, *Il n'y a pas de variété abélienne sur* **Z**, Invent. Math. **81** (1985), no. 3, 515–538.
54. ———, *Schémas propres et lisses sur* **Z**, Proceedings of the Indo-French Conference on Geometry (Bombay, 1989), Hindustan Book Agency, Delhi, 1993, pp. 43–56.
55. ———, *Représentations ℓ-adiques potentiellement semi-stables*, Périodes p-adiques (Bures-sur-Yvette, 1988), Astérisque, vol. 223, Soc. Math. France, 1994, pp. 321–347.
56. ———, *Représentations p-adiques semi-stables*, Périodes p-adiques (Bures-sur-Yvette, 1988), Astérisque, vol. 223, Soc. Math. France, 1994, pp. 113–184.
57. Jean-Marc Fontaine and Guy Laffaille, *Construction de représentations p-adiques*, Ann. Sci. Éc. Norm. Supér. (4) **15** (1982), no. 4, 547–608.
58. Nuno Freitas, *On the Fermat-type equation* $x^3 + y^3 = z^p$, Comment. Math. Helv. **91** (2016), no. 2, 295–304.
59. Nuno Freitas and Alain Kraus, *On the symplectic type of isomorphisms of the p-torsion of elliptic curves*, Mem. Amer. Math. Soc. **277** (2022), no. 1361.
60. Nuno Freitas, Alain Kraus, and Samir Siksek, *Class field theory, Diophantine analysis and the asymptotic Fermat's Last Theorem*, Adv. Math. **363** (2020), 106964.
61. ———, *On asymptotic Fermat over the* $\mathbb{Z}_2$*-extension of* $\mathbb{Q}$, Ann. Math. Blaise Pascal **28** (2021), no. 1, 1–6.

62. Nuno Freitas and Diana Mocanu, *Local points on twists of $X(p)$ with applications*, 2025, preprint, arXiv:2509.04294v4.
63. Nuno Freitas and Ignasi Sánchez-Rodríguez, *Comparing Galois representations in the residually reducible case*, Math. Comp. (2026), to appear; cited by the numbering of arXiv:2510.12956v1.
64. Alexandru Ghitza and Takuya Yamauchi, *The non-existence of some Galois representations of moderate dimension in small characteristic*, 2025, preprint, arXiv:2509.00635v2.
65. Franco Golfieri Madriaga and Ariel Pacetti, *Hypergeometric motives and the generalized Fermat equation*, 2025, preprint, arXiv:2412.08804v2.
66. Franco Golfieri Madriaga, Ariel Pacetti, and Fernando Rodriguez-Villegas, *On rank 2 hypergeometric motives*, 2026, preprint, arXiv:2603.17978v1.
67. Ralph Greenberg, *Galois representations with open image*, Ann. Math. Québec **40** (2016), no. 1, 83–119.
68. Alexander Grothendieck, *Revêtements étales et groupe fondamental (SGA 1)*, Lecture Notes in Math., vol. 224, Springer, 1971.
69. Shin Hattori, *Integral p-adic Hodge theory and ramification of crystalline representations*, An excursion into p-adic Hodge theory: from foundations to recent trends, Panor. Synthèses, vol. 54, Soc. Math. France, Paris, 2019, pp. 159–203.
70. Hervé Jacquet and Joseph A. Shalika, *On Euler products and the classification of automorphic forms. II*, Amer. J. Math. **103** (1981), no. 4, 777–815.
71. Manvir Jaswal, *Programs and data for "The generalized Fermat equation $x^3 + y^3 = z^n$"*, 2026, programs, outputs and commands for Appendix A, Remark 4.18 and the Supplement; Zenodo, https://doi.org/10.5281/zenodo.23197806.
72. Fredrik Johansson, *Arb: efficient arbitrary-precision midpoint-radius interval arithmetic*, IEEE Trans. Comput. **66** (2017), no. 8, 1281–1292.
73. Nicholas M. Katz, *Galois properties of torsion points on abelian varieties*, Invent. Math. **62** (1981), no. 3, 481–502.
74. ———, *Exponential sums and differential equations*, Annals of Mathematics Studies, vol. 124, Princeton University Press, 1990.
75. M. A. Kenku, *On the number of $\mathbf{Q}$-isomorphism classes of elliptic curves in each $\mathbf{Q}$-isogeny class*, J. Number Theory **15** (1982), no. 2, 199–202.
76. Chandrashekhar Khare and Jean-Pierre Wintenberger, *On Serre's conjecture for 2-dimensional mod p representations of* $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$, Ann. of Math. (2) **169** (2009), no. 1, 229–253.
77. ———, *Serre's modularity conjecture. I, II*, Invent. Math. **178** (2009), no. 3, 485–504 and 505–586.
78. Mark Kisin, *Potentially semi-stable deformation rings*, J. Amer. Math. Soc. **21** (2008), no. 2, 513–546.
79. Helmut Koch, *Galois theory of p-extensions*, Springer Monographs in Mathematics, Springer-Verlag, Berlin, 2002.
80. Alain Kraus, *Sur l'équation $a^3 + b^3 = c^p$*, Experiment. Math. **7** (1998), no. 1, 1–13.
81. Alain Kraus and Joseph Oesterlé, *Sur une question de B. Mazur*, Math. Ann. **293** (1992), 259–275.
82. Shanta Laishram and Tarlok N. Shorey, *Baker's explicit abc-conjecture and applications*, Acta Arith. **155** (2012), no. 4, 419–429.
83. Richard Massy, *Construction de p-extensions galoisiennes d'un corps de caractéristique différente de p*, J. Algebra **109** (1987), no. 2, 508–535.
84. Barry Mazur, *Rational isogenies of prime degree (with an appendix by D. Goldfeld)*, Invent. Math. **44** (1978), no. 2, 129–162.
85. William McCallum and Bjorn Poonen, *The method of Chabauty and Coleman*, Explicit methods in number theory, Panor. Synthèses, vol. 36, Soc. Math. France, Paris, 2012, pp. 99–117.
86. Ján Mináč and Nguyễn Duy Tân, *Construction of unipotent Galois extensions and Massey products*, Adv. Math. **304** (2017), 1021–1054, cited by the numbering of arXiv:1501.01346v4.
87. Abdellah Mokrane, *La suite spectrale des poids en cohomologie de Hyodo–Kato*, Duke Math. J. **72** (1993), no. 2, 301–337.
88. Hyunsuk Moon, *Finiteness results on certain mod p Galois representations*, J. Number Theory **84** (2000), no. 1, 156–165.
89. Hyunsuk Moon and Yuichiro Taguchi, *Refinement of Tate's discriminant bound and non-existence theorems for mod p Galois representations*, Doc. Math. **Extra Vol.** (2003), 641–654.
90. Yukiyoshi Nakkajima, *p-adic weight spectral sequences of log varieties*, J. Math. Sci. Univ. Tokyo **12** (2005), no. 4, 513–661.

91. A. M. Odlyzko, *Bounds for discriminants and related estimates for class numbers, regulators and zeros of zeta functions: a survey of recent results*, Sém. Théor. Nombres Bordeaux (2) **2** (1990), no. 1, 119–141.
92. Stefan Patrikis and Richard Taylor, *Automorphy and irreducibility of some l-adic representations*, Compos. Math. **151** (2015), no. 2, 207–229.
93. Georges Poitou, *Sur les petits discriminants*, Séminaire Delange–Pisot–Poitou. Théorie des nombres **18** (1976–1977), no. 1, Exposé 6, 18 pp.
94. Kenneth A. Ribet, *On modular representations of* $\mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q})$ *arising from modular forms*, Invent. Math. **100** (1990), 431–476.
95. ———, *Report on mod l representations of* $\mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q})$, Motives (Seattle, WA, 1991), Proc. Sympos. Pure Math., vol. 55, Part 2, Amer. Math. Soc., Providence, RI, 1994, pp. 639–676.
96. Takeshi Saito, *Modular forms and p-adic Hodge theory*, Invent. Math. **129** (1997), no. 3, 607–620.
97. ———, *Hilbert modular forms and p-adic Hodge theory*, Compos. Math. **145** (2009), no. 5, 1081–1113.
98. Edward F. Schaefer, *2-descent on the Jacobians of hyperelliptic curves*, J. Number Theory **51** (1995), no. 2, 219–232.
99. Mehmet Haluk Şengün, *The nonexistence of certain representations of the absolute Galois group of quadratic fields*, Proc. Amer. Math. Soc. **137** (2009), no. 1, 27–35.
100. Jean-Pierre Serre, *Abelian l-adic representations and elliptic curves*, W. A. Benjamin, New York–Amsterdam, 1968.
101. ———, *Corps locaux*, second ed., Hermann, Paris, 1968.
102. ———, *Propriétés galoisiennes des points d'ordre fini des courbes elliptiques*, Invent. Math. **15** (1972), no. 4, 259–331.
103. Igor R. Shafarevich, *Extensions with prescribed ramification points*, Publ. Math. Inst. Hautes Études Sci. **18** (1963), 71–92, in Russian.
104. Romyar T. Sharifi, *Twisted Heisenberg representations and local conductors*, Ph.D. thesis, University of Chicago, 1999.
105. Joseph H. Silverman, *Advanced topics in the arithmetic of elliptic curves*, Graduate Texts in Mathematics, vol. 151, Springer-Verlag, New York, 1994.
106. ———, *The arithmetic of elliptic curves*, second ed., Graduate Texts in Mathematics, vol. 106, Springer, Dordrecht, 2009.
107. Joseph H. Silverman and John T. Tate, *Rational points on elliptic curves*, second ed., Undergraduate Texts in Mathematics, Springer, Cham, 2015.
108. Michael Stoll, *Implementing 2-descent for Jacobians of hyperelliptic curves*, Acta Arith. **98** (2001), no. 3, 245–277.
109. John Tate, *The non-existence of certain Galois extensions of* $\mathbf{Q}$ *unramified outside* 2, Arithmetic geometry (Tempe, AZ, 1993), Contemp. Math., vol. 174, Amer. Math. Soc., Providence, RI, 1994, pp. 153–156.
110. The GAP Group, *GAP – Groups, Algorithms, and Programming, version 4.15.1*, 2025, https://www.gap-system.org.
111. The PARI Group, *PARI/GP version 2.17.3*, 2025, https://pari.math.u-bordeaux.fr/.
112. Takeshi Tsuji, *p-adic étale cohomology and crystalline cohomology in the semi-stable reduction case*, Invent. Math. **137** (1999), no. 2, 233–411.
113. ———, *Semi-stable conjecture of Fontaine–Jannsen: a survey*, Cohomologies p-adiques et applications arithmétiques, II, Astérisque, vol. 279, Soc. Math. France, 2002, pp. 323–370.
114. Ashleigh Wilcox, *A systematic approach to Diophantine equations: two thousand solved examples*, 2024, preprint, arXiv:2404.08719v2.
115. Jean-Pierre Wintenberger, *Sur les représentations p-adiques géométriques de conducteur* 1 *et de dimension* 2 *de* $G_{\mathbb{Q}}$, 2004, preprint, arXiv:math/0406576v2.
116. Zhong-Peng Zhou, *The inter-universal Teichmüller theory and new Diophantine results over the rational numbers. I*, 2025, preprint, arXiv:2503.14510v1.

Toronto, Canada
Email address: manvirjaswal@icloud.com