From the holdings of the Department of Special Collections , Princeton University Library, Princeton, NJ

These documents are either in the public domain, or can only be used for educational and research purposes (Fair use) as per U.S. Copyright law (text below). By accessing this file, all users agree that their use falls in the public domain or within fair use as defined by the copyrightlaw. We do not charge any permission or usage fees for the publication of images of material inour collections, including those provided by Princeton University Library, via our website, catalog, or directly from staff.For more information regarding copyright, credit, and citation please review the information onthe Copyright, Credit and Citation Guidelines page of our website.
https://library.princeton.edu/special-collections/policies/copyright-credit-and-citation-guidelines. If you have any questions, including how to order higher-quality images from the collection, contact Special Collections Public Services via our Ask Us! Form. https://library.princeton.edu/special-collections/ask-us

---

Doctoral Dissertations, 2011-2026 Mathematics

2021

Reflection theorems for number rings

O'Dorney, Evan Michael

Princeton, NJ : Princeton University

---

http://arks.princeton.edu/ark:/88435/dsp01r207ts47r

U.S. Copyright law: The copyright law of the United States (Title 17, §108, United States Code) governs the making of photocopies or other reproductions of copyrighted material. Under certain conditions specified in the law, libraries and archives are authorized to furnish a photocopy or other reproduction. One of these specified conditions is that the photocopy or reproduction is not to be used for any purpose other than private study, scholarship, or research. If a user makes a request for, or later uses, a photocopy or reproduction for purposes in excess of fair use that user may be liable for copyright infringement. This institution reserves the right to refuse to accept a copying order if, in its judgment, fulfillment of the order would involve a violation of copyright law. https://www.copyright.gov/title17/title17.pdf

Reflection Theorems for Number Rings

Evan M. O'Dorney

a dissertation presented to the faculty

of princeton university in candidacy for

the degree of doctor of philosophy

recommended for acceptance by

the department of mathematics

Adviser: Manjul Bhargava

September 2021



This work is licensed under an arXiv perpetual, non-exclusive license

(https://arxiv.org/licenses/nonexclusive-distrib/1.0/license.html)

Abstract

The Ohno-Nakagawa reflection theorem is an unexpectedly simple identity relating the number of $\mathrm{GL}_2\mathbb{Z}$-classes of binary cubic forms (equivalently, cubic rings) of two different discriminants D, $-27D$; it generalizes cubic reciprocity and the Scholz reflection theorem. In this paper, we provide a framework for generalizing this theorem using a global and local step. The global step uses Fourier analysis on the adelic cohomology $H^1(\mathbb{A}_K, M)$ of a finite Galois module, modeled after the celebrated Fourier analysis on $\mathbb{A}_K$ used in Tate's thesis. The local step is combinatorial, more elementary but much more mysterious. We establish reflection theorems for binary quadratic forms over number fields of class number 1, and for cubic and quartic rings over arbitrary number fields, as well as binary quartic forms over $\mathbb{Z}$; the quartic results are conditional on some computational algebraic identities that are probabilistically true. Along the way, we find elegant new results on Igusa zeta functions of conics and the average value of a quadratic character over a box in a local field.

Contents

I Introduction **1**

1 Introduction **1**

1.1 Historical background 1

1.2 Methods 4

1.3 Results 5

1.4 Outline of the paper 6

1.5 Acknowledgements 7

2 Examples for the lay reader **7**

2.1 Reflection for quadratic equations 7

2.2 Reflection for cubic equations 11

2.3 Reflection for $2 \times n \times n$ boxes 14

2.4 Reflection for quartic equations 16

3 Notation **22**

II Galois cohomology **23**

4 Étale algebras and their Galois groups **23**

4.1 Étale algebras 23

4.2 The Galois group of an étale algebra 25

4.3 Resolvents 26

4.4 Subextensions and automorphisms 27

4.5 Torsors 28

4.6 A fresh look at Galois cohomology 31

5 Extensions of Kummer theory to explicitize Galois cohomology **37**

5.1 The Tate pairing and the Hilbert symbol 44

6 Rings over a Dedekind domain 48

6.1 Indices of lattices 48

6.2 Discriminants 50

6.3 Quadratic rings 54

6.4 Cubic rings 56

6.5 Quartic rings and their cubic resolvent rings 60

7 Cohomology of cyclic modules over a local field 71

7.1 Discriminants of Kummer and affine extensions 73

7.2 The Shafarevich basis 76

7.3 Proof of Theorem 7.1 86

7.4 The tame case 90

III Composed varieties 91

8 Composed varieties 91

8.1 Examples 94

8.2 Integral models; localization of orbit counts 96

8.3 Fourier analysis of the local and global Tate pairings 99

IV Reflection theorems: first examples 108

9 Quadratic forms by superdiscriminant 108

10 Class groups: generalizations of the Scholz and Leopoldt reflection theorems 118

10.1 Dual orders 119

10.2 Dual orders are plentiful for quadratic extensions 122

10.3 Local dual generalized orders 123

10.4 Relation to the Scholz reflection theorem 126

V Reflection theorems: cubic rings 127

11 Cubic Ohno-Nakagawa 127

11.1 A bijective proof of the tame case 133

11.2 A computational proof 138

11.3 A bijective proof of the wild case 153

12 Non-natural weightings 162

12.1 Local weightings given by splitting types 163

12.2 Discriminant reduction 165

12.3 Subring zeta functions 168

12.4 Invariant lattices at 2 174

12.5 Binary cubic forms over $\mathbb{Z}[1/N]$ 178

VI Reflection theorems: quartic rings and related objects 181

13 Reflection for 2-adic quartic orders, and applications 181

13.1 Results on binary quartic forms 187

13.2 The conductor property of the resolvent ring 194

14 Tame quartic rings with non-split resolvent, by multijection 198

14.1 Invertibility of ideals in orders 198

14.2 Self-duality of the count of quartic orders 202

VII Counting quartic rings with prescribed resolvent 207

15 Introduction 208

16 The group H^1 of quartic algebras with given resolvent 209

17 Reduced bases **211**

17.1 The extender basis of a cubic resolvent ring 217

18 Resolvent conditions **219**

18.1 Transformation, and ring volumes in the white zone 227

18.2 From ring volumes to ring counts 229

19 The conic over $\mathcal{O}_K$ **232**

19.1 Diagonal conics 238

19.2 The solution volume of the conic 242

19.3 The Brauer class 249

19.4 The squareness 250

19.5 $\mathcal{N}_{11}$ 253

20 Boxgroups **259**

20.1 Signatures 260

20.2 Boxgroups in unramified splitting type 261

20.3 Boxgroups in splitting type 1^3 269

20.4 The recentering lemma 275

20.5 Charmed cosets 277

20.6 The projectors 281

20.7 Notation 284

21 Ring volumes for ξ_1' **284**

21.1 The smearing lemma 285

21.2 The zones when $\mathcal{N}_{11}$ is strongly active (black, plum, purple, blue, green, and red) . . 287

21.3 The zones when $\mathcal{N}_{11}$ is weakly active (brown and yellow) 307

21.4 The beige zone 316

21.5 Orthogonality 319

21.6 Smeared answers 326

21.7 The average value of a quadratic character on a box 328

22 Ring volumes for ξ_2' **331**

22.1 $\mathcal{M}_{12}$ 332

22.2 $\mathcal{M}_{22}$ 334

23 Further remarks on the code **339**

VIII Unanswered questions 341

24 Doubly traced quartic rings **341**

25 Reflection for $2 \times n \times n$ boxes **345**

IX Appendices 346

A The Grothendieck-Witt ring and the proof of Lemma 19.11 **347**

B Examples of zone totals **350**

Part I

Introduction

1 Introduction

1.1 Historical background

In 1932, using the then-new machinery of class field theory, Scholz [49] proved that the class groups of the quadratic fields $\mathbb{Q}(\sqrt{D})$ and $\mathbb{Q}(\sqrt{-3D})$, whose discriminants are in the ratio -3, have 3-ranks differing by at most 1. This is a remarkable early example of a *reflection theorem.* A generalization due to Leopoldt [31] relates different components of the p-torsion of the class group of a number field containing μ_p when decomposed under the Galois group of that field. Applications of such reflection theorems are far-ranging: for instance, Ellenberg and Venkatesh [21] use reflection theorems of Scholz type to prove upper bounds on ℓ-torsion in class groups of number fields, while Mihăilescu [34] uses Leopoldt's generalization to simplify a step of his monumental proof of the Catalan conjecture that 8 and 9 are the only consecutive perfect powers. Through the years, numerous reflection principles for different generalizations of ideal class groups have come into print. A very general reflection theorem for Arakelov class groups is due by Gras [23].

A quite different direction of generalization was discovered by accident in 1997: The following relation was conjectured by Ohno [44] on the basis of numerical data and proved by Nakagawa [38], for which reason we will call it the *Ohno-Nakagawa (O-N) reflection theorem*:

Theorem 1.1 (Ohno–Nakagawa)**.** *For a nonzero integer D, let $h(D)$ be the number of $\mathrm{GL}_2(\mathbb{Z})$-orbits of* binary cubic forms

$$f(x,y) = ax^3 + bx^2y + cxy^2 + dy^3$$

of discriminant D, each orbit weighted by the reciprocal of its number of symmetries (i.e. stabilizer in $\mathrm{GL}_2(\mathbb{Z})$). Let $h_3(D)$ be the number of such orbits $f(x,y)$ such that the middle two coefficients b, c are multiples of 3, weighted in the same way.

Then for every nonzero integer D, we have the exact identity

$$h_3(-27D) = \begin{cases} 3h(D), & D > 0 \\ h(D), & D < 0. \end{cases} \tag{1}$$

By the well-known index-form parametrization (see 6.9 below), $h(D)$ also counts the cubic *rings* of discriminant D over $\mathbb{Z}$, weighted by the reciprocal of the order of the automorphism group. It turns out that $h_3(D)$ counts those rings C for which $3|\operatorname{tr}_{C/\mathbb{Z}}\xi$ for every $\xi \in C$. When D is a fundamental discriminant, the corresponding cubic extensions are closely related, via class field theory, to the 3-class group of $\mathbb{Q}(\sqrt{D})$ and we get back Scholz's reflection theorem, as Nakagawa points out ([38], Remark 0.9).

Theorem 1.1 was quite unexpected, because $\mathrm{GL}_2(\mathbb{Z})$-orbits of binary cubics have been tabulated since Eisenstein without unearthing any striking patterns. Even the exact normalizations $h(D)$, $h_3(D)$ had been in use for over two decades. They appear in the *Shintani zeta functions*

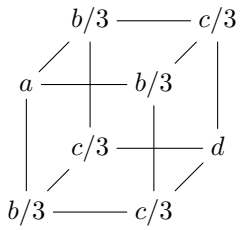
$$\zeta^{\pm}(s) = \sum_{n\geq 1} \frac{h(\pm n)}{n^s}$$
$$\hat{\zeta}^{\pm}(s) = \sum_{n\geq 1} \frac{h_3(\pm 27n)}{n^s},$$

a family of Dirichlet series which play a prominent role in understanding the distribution of cubic number fields, similar to how the famous Riemann zeta function controls the distribution of primes. As Shintani proved as early as 1972 [52], the Shintani zeta functions satisfy a matrix functional equation (see Nakagawa [38], eq. (0.1))

$$\begin{bmatrix} \zeta^+(1-s) \\ \zeta^-(1-s) \end{bmatrix} = 2^{-1}3^{3s-2}\pi^{-4s}\Gamma\left(s-\frac{1}{6}\right)\Gamma(s)^2\Gamma\left(s+\frac{1}{6}\right)\begin{bmatrix} \sin 2\pi s & \sin \pi s \\ 3\sin \pi s & \sin 2\pi s \end{bmatrix}\begin{bmatrix} \hat{\zeta}^+(s) \\ \hat{\zeta}^-(s) \end{bmatrix} \tag{2}$$

The condition that 3 divide b and c is equivalent to requiring that the cubic form f is *integer-matrix*,

that is, its corresponding symmetric trilinear form



has integer entries. This condition arose in Shintani's work by taking the dual lattice to $\mathbb{Z}^4$ under the pairing

$$\langle (a,b,c,d),(a',b',c',d')\rangle = ad' - \frac{1}{3}bc' + \frac{1}{3}cb' - da', \tag{3}$$

which plays a central role in proving the functional equation. However, as we will find, the pairing (3) does not figure in the proof of our reflection theorems, which indeed often relate lattices that are not dual under it.

Using the functional equation, Shintani proved that the $\zeta^{\pm}$ admit meromorphic continuations to the complex plane with simple poles at 1 and 5/6, inspiring him to conjecture that the number $N_{\pm}(X)$ of cubic fields of positive or negative discriminant up to X has the shape

$$N_{\pm}(X) = a_{\pm}X + b_{\pm}X^{5/6} + o(X^{5/6})$$

for suitable constants $a_{\pm}$ and $b_{\pm}$. This conjecture was proven by Bhargava, Shankar, and Tsimerman [8] and independently by Taniguchi and Thorne [54]. Neither proof needs the Ohno-Nakagawa reflection theorem (Theorem 1.1), which appears in the notation of Shintani zeta functions in the succinct form

$$\hat{\zeta}^{+}(s) = \zeta^{-}(s) \quad \text{and} \quad \hat{\zeta}^{-}(s) = 3\zeta^{+}(s). \tag{4}$$

Remark 1.2. In the earlier papers, the term "Ohno-Nakagawa identities" was used, referring to the pair (4). Our work confirms the intuition that, despite the different scalings, both identities are essentially one theorem.

1.2 Methods

Several proofs of O-N are now in print ([38, 33, 43, 22]), all of which consist of two main steps:

- A "global" step that uses global class field theory to understand cubic fields, equivalently $\mathrm{GL}_2(\mathbb{Q})$-orbits of cubic forms;
- A "local" step to count the rings in each cubic field, equivalently the $\mathrm{GL}_2(\mathbb{Z})$-orbits in each $\mathrm{GL}_2(\mathbb{Q})$-orbit, and put the result in a usable form.

In this paper, the distinction between these steps will be formalized and clarified.

For the global step, we take inspiration from Tate's celebrated thesis [55], which uses Fourier analysis on the adeles to give illuminating new proofs of the functional equations for the Riemann ζ-function and various L-functions. Taniguchi and Thorne (see [53]) used Fourier analysis on the space of binary cubic forms over $\mathbb{F}_q$ to get the functional equation for the Shintani zeta function of forms satisfying local conditions at primes. Despite the similarities, their work is essentially independent from ours. We are also inspired by a remark due to Calegari in a paper of Cohen, Rubinstein-Salzedo, and Thorne ([12], Remark 1.6), pointing out that their reflection theorem counting dihedral fields of prime order can also be derived from a theorem of Greenberg and Wiles for the sizes of Selmer groups in Galois cohomology.

We present a notion of *composed variety*, a scheme $\mathcal{V}$ over the ring of integers $\mathcal{O}_K$ of a number field admitting an action of an algebraic group $\mathcal{G}$ over $\mathcal{O}_K$. Our guiding example is the scheme $\mathcal{V}$ of binary cubic forms of discriminant D with its action of $\mathcal{V} = \mathrm{SL}_2$. The term "composed" refers to the presence of a composition law on the orbits, which relate naturally to a Galois cohomology group $H^1(K, M)$. Our (global) reflection theorems can be stated as saying that two composed varieties $\mathcal{V}^{(1)}$, $\mathcal{V}^{(2)}$ have the same number of $\mathcal{O}_K$-points, with a suitable weighting. Introducing a new technique of Fourier analysis on the adelic cohomology group $H^1(\mathbb{A}_K, M) = \prod_v' H^1(K_v, M)$, based on Poitou-Tate duality, we present a generalized reflection engine (Theorems 8.12 and 8.13) that reduces global reflection theorems to *local reflection theorems,* that is, statements involving only the $\mathcal{O}_{K_v}$-points of $\mathcal{V}^{(1)}$ and $\mathcal{V}^{(2)}$ for a single place v of K. A typical case is Theorem 11.2.

These local reflection theorems are approachable by elementary methods but can be difficult to prove. We present two kinds of proofs. The first is a bijective argument involving Bhargava's self-balanced ideals that is very clean but has only been discovered at the "tame primes" ($\mathfrak{p} \nmid 3$ in the cubic case, $\mathfrak{p} \nmid 2$ in the quartic). The second is by explicitly computing the number of orders of given resolvent in a cubic or quartic algebra. We express it as a generating function in a number of variables depending on the splitting type of the resolvent. The generating function is rational, and local reflection can be written as an equality between two rational functions; but these functions are so complicated that the best approximation to a proof of the identity that we can find is a Monte Carlo proof, namely, substituting random values for the variables in some large finite field and verifying that the equality holds. The reader is invited to recheck this verification using the source code in Sage that will be made available with the final version of this paper.

1.3 Results

We are able to prove O-N for binary cubic forms over all number fields K, verifying and extending the conjectures of Dioses [20, Conjecture 1.1]. However, we go further and ask whether every $\mathrm{SL}_2(\mathcal{O}_K)$-invariant lattice within the space $V(K)$ of binary cubic forms admits an O-N-style reflection theorem. Over $\mathbb{Z}$, this question was answered affirmatively for each of the ten invariant lattices by Ohno and Taniguchi [45]. Over $\mathcal{O}_K$, such lattices were classified by Osborne [47], and they differ from one another only at the primes dividing 2 and 3. The lattices at 3 yield an elegant reflection theorem (Theorem 11.3) in which the condition $b, c \in \mathfrak{t}$, where $\mathfrak{t}$ is an ideal dividing 3 in $\mathcal{O}_K$, reflects to $b, c \in 3\mathfrak{t}^{-1}$, the complementary divisor. At 2, the corresponding reflection theorems still exist, though they become difficult to write explicitly: see Theorem 12.14.

We also find a new reflection theorem (Theorem 9.3) counting binary *quadratic* forms, not by discriminant, but by a curious invariant: the product $a(b^2 - 4ac)$ of the discriminant and the leading coefficient. Over $\mathbb{Z}$, the reflection theorem (Theorem 9.5) has the potential to be proved simply using quadratic reciprocity, eschewing the machinery of Galois cohomology, though it seems unlikely that the theorem would have ever been discovered without it.

Nakagawa has also conjectured [36] a reflection theorem for *pairs of ternary quadratic forms,* which parametrize *quartic rings.* The natural invariant to count by is the discriminant, but it is more natural from our perspective to subdivide further and ask for a reflection theorem for rings with fixed *cubic resolvent*, which holds in the known cases [36, Theorem 1]. Here our global framework applies without change, but the local enumeration of orders in a quartic field presents formidable combinatorial difficulties, especially in the wildly ramified (2-adic) setting, which have been attacked in another work of Nakagawa [37]. Our methods have the potential to finish this work, but because we count by resolvent rather than discriminant, our answers do not directly match his.

The process of proving local quartic O-N leads us down some fruitful routes that do not at first sight have any connection to reflection theorems or to the enumeration of quartic rings. These include new cases of the Igusa zeta functions of conics (Lemmas 19.9 and 19.10) and a result on the average value of a quadratic character on a box in a local field (Theorem 21.21). If quartic O-N holds true in all cases, it implies that the cubic resolvent ring (in the sense of Bhargava) of a maximal quartic order has a second natural characterization: it is the "conductor ring" for which the Galois-naturally attached extension K_6/K_3 is a ring class field (Theorem* 13.15).

1.4 Outline of the paper

In Section 2, we state and give examples of the main global reflection theorems of the paper over $\mathbb{Z}$, in a fashion that requires a minimum of prior knowledge, for the end of further diffusing interest in, and appreciation of, the beauty of number theory.

In Part II, we lay out preliminary matter, much of which is closely related to results that have appeared in the literature but under different guises. It includes a simple characterization (Proposition 4.21) of Galois H^1 in terms of étale algebras whose Galois group is a semidirect product. It also includes a theorem (Theorem 7.1) on the structure of $H^1(K, M)$ in the case that K is local and $M \cong \mathcal{C}_p$ (with any Galois structure), which will be invaluable in what follows.

In Part III, we lay out the framework of composed varieties, on which we perform the novel technique of Fourier analysis of the local and global Tate pairings to get our main local-to-global

reflection engine (Theorems 8.12 and 8.13). The remainder of the paper will concern applications of this engine.

In Part IV, we prove two relatively simple reflection theorems: one for quadratic forms (Theorem 9.3), and a version of the Scholz reflection principle for class groups of quadratic orders (Theorem 10.3).

In Part V, we prove our extensions of Ohno-Nakagawa for cubic forms and rings.

The quartic case is dealt with in Parts VI and VII: the first part dealing with the bijective methods, and the second with the (long) work of explicitly counting orders in each quartic algebra. The case of partially ramified cubic resolvent (splitting type $1^2 1$) is still in progress, so we restrict our attention to the four tamely splitting types in the present version.

We conclude the paper with some unanswered questions engendered by this research.

1.5 Acknowledgements

For fruitful discussions, I would like to thank (in no particular order): Manjul Bhargava, Xiaoheng Jerry Wang, Fabian Gundlach, Levent Alpöge, Melanie Matchett Wood, Kiran Kedlaya, Alina Bucur, Benedict Gross, Sameera Vemulapalli, Brandon Alberts, Peter Sarnak, and Jack Thorne.

2 Examples for the lay reader

Fortunately for the non-specialist reader, the statements (though not the proofs) of the main results in this thesis can be stated in a way requiring little more than high-school algebra. We here present these statements and some examples to illustrate them.

2.1 Reflection for quadratic equations

Definition 2.1. Let $f(x) = ax^2 + bx + c$ be a quadratic polynomial, where the coefficients a, b, c are integers. The *superdiscriminant* of f is the product

$$I = a \cdot (b^2 - 4ac)$$

of the leading coefficient with the usual discriminant.

Lemma 2.2. *If we replace x by $x+t$ in a quadratic polynomial f, where t is a fixed integer, then the superdiscriminant does not change.*

Proof. This can be verified by brute-force calculation, but the following method is more illuminating. The discriminant is classically related to the two roots of f,

$$x_1 = \frac{-b+\sqrt{b^2-4ac}}{2a} \quad \text{and} \quad x_2 = \frac{-b-\sqrt{b^2-4ac}}{2a},$$

through their *difference:*

$$\begin{aligned} x_1 - x_2 &= \frac{2\sqrt{b^2-4ac}}{2a} = \frac{\sqrt{b^2-4ac}}{a} \\ (x_1-x_2)^2 &= \frac{b^2-4ac}{a^2} \\ a^3(x_1-x_2)^2 &= a\cdot(b^2-4ac) = I. \end{aligned}$$

If we replace x by $x+t$, then a does not change, and both roots x_1, x_2 are decreased by t, so their difference $x_1 - x_2$ is unchanged. Therefore I is unchanged. ■

Definition 2.3. Call two quadratics f_1, f_2 *equivalent* if they are related by a translation $f_2(x) = f_1(x+t)$. If I is a nonzero integer, let $q(I)$ be the number of quadratics of superdiscriminant I, up to equivalence. Let $q_2(I)$, $q^+(I)$, $q_2^+(I)$ be the number of such quadratics that satisfy certain added conditions:

- For $q_2(I)$, we require that the middle coefficient b be even.
- For $q^+(I)$, we require that the roots be real, that is, that $b^2-4ac>0$.
- For $q_2^+(I)$, we impose both of the last two conditions.

We are now ready to state a *quadratic reflection theorem,* the main result of this section.

Theorem 2.4 ("Quadratic O-N"). *For every nonzero integer n,*

$$q_2^+(4n) = q(n)$$

$$q_2(4n) = 2q^+(n).$$

Proof. The proof is not easy. See Theorem 9.5. ■

It's not hard to compute all quadratics of a fixed superdiscriminant I. The leading coefficient a must be a divisor of I (possibly negative), and there are only finitely many of these. Then, by replacing x by $x+t$ where t is an integer nearest to $-b/(2a)$, we can assume that b lies in the window $-|a| < b \leq |a|$. We can try each of the integer values in this window, checking whether

$$c = \frac{ab^2 - I}{4a^2}$$

comes out to an integer.

Example 2.5. There are five quadratics of superdiscriminant 15:

$f(x)$	q	q^+	q_2	q_2^+
$-x^2 + x - 4$	✓			
$15x^2 + x$	✓	✓		
$15x^2 - x$	✓	✓		
$15x^2 + 11x + 2$	✓	✓		
$15x^2 - 11x + 2$	✓	✓		

You might think we left out $-x^2 - x - 4$, but it is equivalent to another quadratic on the list:

$$-x^2 - x - 4 = -(x+1)^2 + (x+1) - 4.$$

So we get the totals

$$q(15) = 5 \quad \text{and} \quad q^+(15) = 4.$$

There are 18 quadratics of superdiscriminant 60:

$f(x)$	q	q^+	q_2	q_2^+
$x^2 - 15$	✓	✓	✓	✓
$-x^2 - 15$	✓		✓	
$-3x^2 + 2x - 2$	✓		✓	
$-3x^2 - 2x - 2$	✓		✓	
$-4x^2 + x - 1$	✓			
$-4x^2 - x - 1$	✓			
$15x^2 + 2x$	✓	✓	✓	✓
$15x^2 - 2x$	✓	✓	✓	✓
$15x^2 + 8x + 1$	✓	✓	✓	✓
$15x^2 - 8x + 1$	✓	✓	✓	✓
$60x^2 + x$	✓	✓		
$60x^2 - x$	✓	✓		
$60x^2 + 31x + 4$	✓	✓		
$60x^2 - 31x + 4$	✓	✓		
$60x^2 + 41x + 7$	✓	✓		
$60x^2 - 41x + 7$	✓	✓		
$60x^2 + 49x + 10$	✓	✓		
$60x^2 - 49x + 10$	✓	✓		

Counting carefully, we get

$$q(60) = 18, \quad q_2(60) = 8, \quad q^+(60) = 13, \quad q_2^+(60) = 5.$$

The equalities

$$q_2^+(60) = 5 = q(15) \quad \text{and} \quad q_2(60) = 8 = 2 \cdot 4 = 2q^+(15)$$

are instances of Theorem 2.4. From the same theorem, we derive, without computation, that

$$q_2^+(240) = q(60) = 18 \quad \text{and} \quad q_2(240) = 2q^+(60) = 26.$$

This short investigation raises many questions. The superdiscriminant $I = a(b^2 - 4ac)$ does not seem to have been considered before. Is there an explicit formula for $q(I)$? Is there an elementary proof of Theorem 2.4? See Example 9.6 for a connection to Gauss's celebrated law of quadratic reciprocity.

2.2 Reflection for cubic equations

Definition 2.6. For a cubic polynomial

$$f(x) = ax^3 + bx^2 + cx + d,$$

we define the *discriminant* to be

$$\operatorname{disc} f = a^4(x_1 - x_2)^2(x_1 - x_3)^2(x_2 - x_3)^2, \tag{5}$$

where x_1, x_2, x_3 are the roots. Explicitly,

$$\operatorname{disc} f = b^2c^2 - 4ac^3 - 4b^3d - 27a^2d^2 + 18abcd. \tag{6}$$

There are many transformations of a cubic polynomial that don't change the discriminant. One is changing x to $x + t$, where t is a constant. Another is reversing the coefficients,

$$f(x) = ax^3 + bx^2 + cx + d \longmapsto x^3 f\left(\frac{1}{x}\right) = dx^3 + cx^2 + bx + a.$$

Both of these are special cases of the following construction.

Definition 2.7. Two cubic polynomials f_1, f_2 with integer coefficients are *equivalent* if there is a matrix

$$\begin{bmatrix} p & q \\ r & s \end{bmatrix}$$

whose determinant $ps - qr$ is ± 1 such that

$$f_2(x) = (rx + s)^3 \cdot f_1\left(\frac{px + q}{rx + s}\right).$$

A matrix that makes f equivalent to *itself*, that is,

$$f(x) = (rx + s)^3 \cdot f\left(\frac{px + q}{rx + s}\right),$$

is called a *symmetry* of f. The number of symmetries of f is denoted by $s(f)$.

Definition 2.8. If D is a nonzero integer, define $h(D)$ to be the number of cubic polynomials

$$f(x) = ax^3 + bx^2 + cx + d$$

of discriminant D, up to equivalence, each f counted not once but $1/s(f)$ times, where $s(f)$ is the number of symmetries. Define $h_3(D)$ to be the number of cubics of discriminant D for which the middle two coefficients, b and c, are multiples of 3, up to equivalence, each f counted $1/s(f)$ times as before.

We can now state the Ohno-Nakagawa reflection theorem that got this research project started:

Theorem 2.9 (Ohno-Nakagawa; Theorem 1.1)**.** *For every nonzero integer D,*

$$h_3(-27D) = \begin{cases} 3h(D), & D > 0 \\ h(D), & D < 0. \end{cases}$$

Proof. Several proofs are in print (see the Introduction). In this paper, we prove this theorem as a special case of Theorem 11.3. ■

Example 2.10. Take $D = 1$. There is just one cubic with integer coefficients and discriminant 1, namely

$$f(x) = x(x+1) = x^2 + x.$$

The reader may balk at considering a quadratic polynomial as a "cubic" with leading coefficient 0, but the polynomial can be replaced by any number of equivalent forms, for instance

$$(x-1)^3 \cdot f\left(\frac{x}{x-1}\right) = x(x-1)(2x-1).$$

We will suppress this detail in subsequent examples. (A program for computing all cubics of a given discriminant is found in the attached file `cubics.sage`, based on an algorithm of Cremona [15, 16]). The cubic f has six symmetries, which is related to the fact that three linear factors can be permuted in $3! = 6$ ways. In terms of $f(x) = x(x+1)$, the symmetries are

$$\begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}, \begin{bmatrix} -1 & -1 \\ 0 & 1 \end{bmatrix}, \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}, \begin{bmatrix} -1 & -1 \\ 1 & 0 \end{bmatrix}, \begin{bmatrix} 1 & 0 \\ -1 & -1 \end{bmatrix}, \begin{bmatrix} 0 & 1 \\ -1 & -1 \end{bmatrix}.$$

So $h(1) = 1/6$.

Correspondingly, we look at cubics of discriminant -27. There are two:

$$f(x) = x^2 + x + 7 \quad \text{and} \quad f(x) = x^3 + 1.$$

Each admits two symmetries: the first has

$$\begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}, \begin{bmatrix} -1 & -1 \\ 0 & 1 \end{bmatrix},$$

and the second has

$$\begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}, \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}.$$

So $h(-27) = 1/2 + 1/2 = 1$ and $h_3(-27) = 1/2$. In particular,

$$h_3(-27) = 3h_3(1),$$

in conformity with Theorem 2.9.

2.3 Reflection for $2 \times n \times n$ boxes

Bhargava [4] studied $2 \times 3 \times 3$ boxes as a visual representation for quartic rings, as cubic polynomials do for cubic rings. We think that reflection holds not only for $2 \times 3 \times 3$ boxes but for $2 \times 5 \times 5$, $2 \times 7 \times 7$, and so on. We nearly prove the $2 \times 3 \times 3$ case in this paper. We are quite far from proving it for the larger boxes.

Definition 2.11. A *box* is a pair (A, B) of $n \times n$ integer symmetric matrices. The *resolvent* of a box is the polynomial

$$f(x) = \det(Ax - B).$$

It is a polynomial in x, of degree at most n. If A is the identity matrix, the resolvent devolves into the standard *characteristic polynomial.*

Definition 2.12. Two boxes (A_1, B_1) and (A_2, B_2) are *equivalent* if there is an integer $n \times n$ matrix X, whose inverse X^{-1} also has integer entries, such that

$$A_2 = XA_1X^\top \quad \text{and} \quad B_2 = XB_1X^\top.$$

If $(A_2, B_2) = (A_1, B_1) = (A, B)$ are the same pair, then X is called a *symmetry* of (A, B). The number of symmetries of (A, B) will be denoted by $s(A, B)$.

Conjecture 2.13 ("O-N for $2 \times n \times n$ boxes"). *Let n be a positive odd integer. Let f be a*

polynomial of degree n with no multiple roots and only one real root. Denote by $h(f)$ the number of $2\times n\times n$ boxes with resolvent f, up to equivalence, each box weighted by the reciprocal of its number of symmetries. Denote by $h_2(f)$ the number of such boxes with even numbers along the main diagonals of A and B, weighted the same way. Then

$$h_2(2^{n-1}f) = 2^{\frac{n-1}{2}} \cdot h(f). \tag{7}$$

Remark 2.14. The condition that f have no multiple roots (even complex ones) is needed to ensure that there are only finitely many boxes with f as a resolvent. The condition that f have no more than one real root can be eliminated, but then we must impose conditions on the real behavior of the boxes that are difficult to state succinctly.

Example 2.15. Take as resolvent $f(x) = x^3 - x - 1$, the simplest irreducible cubic. It has one real root $\xi \approx 1.3247$ and discriminant -23. There are two boxes with resolvent f, up to equivalence:

$$\left[\begin{pmatrix} 0 & 0 & -1 \\ 0 & -1 & 0 \\ -1 & 0 & -1 \end{pmatrix}, \begin{pmatrix} 0 & -1 & 0 \\ -1 & 0 & -1 \\ 0 & -1 & -1 \end{pmatrix}\right], \left[\begin{pmatrix} 0 & -1 & 0 \\ -1 & 0 & -1 \\ 0 & -1 & -1 \end{pmatrix}, \begin{pmatrix} -1 & 0 & -1 \\ 0 & -1 & -1 \\ -1 & -1 & -1 \end{pmatrix}\right].$$

(These were computed from the balanced pairs $(\mathcal{O}_R, 1)$ and $(\mathcal{O}_R, \xi)$ in the number field $R = \mathbb{Z}[\xi]/(\xi^3 - \xi - 1)$ corresponding to f.) Neither has any symmetries besides the two trivial ones, the identity matrix and its negative, so

$$h(f) = \frac{1}{2} + \frac{1}{2} = 1.$$

There are many boxes with resolvent $2f$, but just one with even numbers all along the main diagonals of A and B, namely

$$\left[\begin{pmatrix} 0 & 0 & 1 \\ 0 & -2 & 0 \\ 1 & 0 & 2 \end{pmatrix}, \begin{pmatrix} 0 & 1 & 0 \\ 1 & 0 & 0 \\ 0 & 0 & -2 \end{pmatrix}\right].$$

(This was computed from the unique quartic ring $\mathcal{O} = \mathbb{Z} \times \mathcal{O}_R$ with resolvent $\mathcal{O}_R$.) It too has only the trivial symmetries, to $h_2(2f) = 1/2$, in accord with Conjecture 2.13.

2.4 Reflection for quartic equations

There are also reflection theorems that appear when counting *quartic* polynomials.

Definition 2.16. If

$$f(x) = ax^4 + bx^3 + cx^2 + dx + e$$

is a quartic polynomial with integer coefficients, its *resolvent* is

$$g(y) = y^3 - cy^2 + (bd - 4ae)y + 4ace - b^2e - ad^2; \tag{8}$$

equivalently, if

$$f(x) = a(x - x_1)(x - x_2)(x - x_3)(x - x_4),$$

then

$$g(y) = \big(y - a(x_1x_2 + x_3x_4)\big)\big(y - a(x_1x_3 + x_2x_4)\big)\big(y - a(x_1x_4 + x_2x_3)\big).$$

Remark 2.17. Cubic resolvents of this type have been used since the 16th century as a step in solving quartic equations. For instance, it is well known that if $f(x)$ factors as the product of two quadratics with integer coefficients, then $g(y)$ has a rational root (the converse is not true).

Analogously to Definition 2.7, we put:

Definition 2.18. Two quartic polynomials f_1, f_2 with integer coefficients are *equivalent* if there is a matrix

$$\begin{bmatrix} p & q \\ r & s \end{bmatrix}$$

whose determinant $ps - qr$ is ± 1 such that

$$f_2(x) = (rx + s)^4 \cdot f_1\left(\frac{px + q}{rx + s}\right).$$

A matrix that makes f equivalent to *itself*, that is,

$$f(x) = (rx+s)^4 \cdot f\left(\frac{px+q}{rx+s}\right),$$

is called a *symmetry* of f. The number of symmetries of f is denoted by $s(f)$.

We have:

Lemma 2.19. (*a*) *If two quartics f_1, f_2 are equivalent, then their resolvents g_1, g_2 are related by a translation*

$$g_2(x) = g_1(x+t)$$

for some integer t.

(*b*) *A quartic and its resolvent have the same discriminant*

$$\begin{aligned}\operatorname{disc} f = \operatorname{disc} g = {} & b^2c^2d^2 - 4ac^3d^2 - 4b^3d^3 + 18abcd^3 - 27a^2d^4 - 4b^2c^3e + 16ac^4e + \\ & 18b^3cde - 80abc^2de - 6ab^2d^2e + 144a^2cd^2e - 27b^4e^2 + 144ab^2ce^2 - \\ & 128a^2c^2e^2 - 192a^2bde^2 + 256a^3e^3.\end{aligned}$$

Proof. Exercise. ■

As before, our reflection theorem will relate general quartics to quartics satisfying certain divisibility relations. Here the relations are quite peculiar:

Definition 2.20. A quartic polynomial

$$f(x) = ax^4 + bx^3 + cx^2 + dx + e$$

is called *supereven* if b, c, and e are multiples of 4 and d is a multiple of 8.

Not every quartic equivalent to a super-even quartic is itself supereven. (For instance, $f_1 = x^4+4$ and $f_2 = 4x^4+1$ are equivalent under the flip $\left[\begin{smallmatrix}0&1\\1&0\end{smallmatrix}\right]$, but f_2 is not supereven.) We therefore make the following definition.

Definition 2.21. Two quartic polynomials f_1, f_2 with integer coefficients are *evenly equivalent* if there is a matrix

$$\begin{bmatrix} p & q \\ r & s \end{bmatrix}$$

whose determinant $ps - qr$ is ± 1, **and r is even,** such that

$$f_2(x) = (rx + s)^4 \cdot f_1\left(\frac{px + q}{rx + s}\right).$$

Such a matrix that makes f equivalent to *itself*, that is,

$$f(x) = (rx + s)^4 \cdot f\left(\frac{px + q}{rx + s}\right),$$

is called an *even symmetry* of f. The number of even symmetries of f is denoted by $s_2(f)$.

Theorem 2.22 ("Quartic O-N"). *Let g be an integer cubic with leading coefficient 1, no multiple roots, and odd discriminant. Denote by $h(g)$ the number of quartics whose resolvent is $g(y + t)$ for some t, up to equivalence and weighted by the reciprocal of the number of symmetries. Denote by $h_2(g)$ the number of supereven quartics whose resolvent is $g(y+t)$ for some t, up to even equivalence and weighted by the reciprocal of the number of even symmetries. Define g_2 by*

$$g_2(y) = 64g\left(\frac{y}{4}\right)$$

Then:

- *If g has one real root, then*

$$4h(g) = h_2(g_2).$$

- *If g has three real roots, then we subdivide*

$$h(g) = h^+(g) + h^-(g) + h^{\pm}(g)$$

where the respective terms count only quartic functions that are always positive, always negative, and have four real roots. We subdivide

$$h_2(g) = h_2^+(g) + h_2^-(g) + h_2^\pm(g).$$

Then:

$$2h(g) = h_2^\pm(g_2)$$
$$4\big(h^+(g) + h^\pm(g)\big) = h_2^+(g_2) + h_2^\pm(g_2)$$
$$4\big(h^-(g) + h^\pm(g)\big) = h_2^-(g_2) + h_2^\pm(g_2)$$

Also, denote by $k(g)$ the number of integral 3×3 symmetric matrices of characteristic polynomial g. Then

$$k(g) = 24\big(h^\pm(g) - h^+(g) - h^-(g)\big).$$

Proof. See Theorem 13.11. ■

Remark 2.23. We think that the hypothesis of odd discriminant is removable, but we have not yet finished the proof.

Example 2.24. Let $g(y) = y^3 - y - 1$. By techniques presented in Section 13.1, it is possible to transform the boxes found in example 2.15 into binary quartic forms. We find that there is only one quartic with resolvent g, namely

$$f(x) = x^3 - x - 1$$

(which, as before, can be transformed by an equivalence to one with nonzero leading coefficient);

and four supereven binary quartics with resolvent $g_2(y) = y^3 - 16y - 64$, namely

$$f(x) = 4x^3 + 12x^2 + 8x - 4 = 4\big((x+1)^3 - (x+1) - 1\big)$$

$$f(x) = -x^4 + 4x^3 + 12x^2 + 8x$$

$$f(x) = -x^4 + 8x - 4$$

$$f(x) = -x^4 + 4x^3 - 4.$$

All these have one pair of complex roots (as must occur for a resolvent with negative discriminant) and only the trivial symmetries $\pm\left[\begin{smallmatrix} 1 & 0 \\ 0 & 1 \end{smallmatrix}\right]$, so

$$h(g) = \frac{1}{2} \quad \text{and} \quad h_2(g_2) = 2 = 4 \cdot \frac{1}{2},$$

in accord with the first part of the theorem.

Example 2.25. Consider $g(y) = y^3 - 2y^2 - 3y + 6 = (y-2)(y+\sqrt{3})(y-\sqrt{3})$, a cubic with three real roots. The quartics with resolvent g are

$$f(x) = -x(2x-1)(3x^2-1),$$

which has four real roots, and

$$f(x) = (x^2 + x + 1)(x^2 + 1),$$

which has no real roots and is positive for all real x. Each has only the trivial symmetries, so

$$h^{\pm}(g) = \frac{1}{2}, \quad h^{+}(g) = \frac{1}{2}, \quad h^{-}(g) = 0.$$

(Note the discrepancy between h^+ and h^-.) Correspondingly, there are eight supereven binary

quartics with resolvent $g_2(y) = (y-8)(y+4\sqrt{3})(y-4\sqrt{3})$:

$$f(x) = -2x^4 - 8x^3 - 4x^2 + 8x = -2x(x+2)(x^2+2x-2)$$

$$f(x) = 4x^3 - 4x^2 - 16x - 8 = 4(x+1)(x^2-2x-2)$$

$$f(x) = 8x^4 - 16x^3 + 20x^2 - 12x + 4 = 4(x^2-x+1)(2x^2-2x+1)$$

$$f(x) = x^4 - 6x^3 + 20x^2 - 32x + 32 = (x^2-4x+8)(x^2-2x+4)$$

$$f(x) = -x^4 + 8x^2 - 12 = -(x^2-2)(x^2-6)$$

$$f(x) = -3x^4 + 8x^2 - 4 = -(x^2-2)(3x^2-2)$$

$$f(x) = x^4 + 8x^2 + 12 = (x^2+2)(x^2+6)$$

$$f(x) = 3x^4 + 8x^2 + 4 = (x^2+2)(3x^2+2).$$

Thus

$$h_2^{\pm}(g_2) = 2, \quad h_2^{+}(g_2) = 2, \quad h_2^{-}(g_2) = 0.$$

This is in accord with the theorem, from which we also learn that

$$k(g) = 48\big(h^{\pm}(g) - h^{+}(g) - h^{-}(g)\big) = 0,$$

so g is *not* the characteristic polynomial of any integer 3×3 symmetric matrix, despite having three real roots (which is a necessary, but not a sufficient, condition).

Example 2.26. Let $g(y) = y^3 - y$. Knowing that $f(x) = x^3 - x$ is the only quartic with cubic resolvent f, and it has four symmetries, the powers of $\left[\begin{smallmatrix} 0 & -1 \\ 1 & 0 \end{smallmatrix}\right]$, we get

$$k(g) = 24\left(h^{\pm}(g) - h^{+}(g) - h^{-}(g)\right) = 24\left(\frac{1}{4} - 0 - 0\right) = 6.$$

So there are six symmetric matrices with characteristic polynomial $y^3 - y$. Indeed, they are the diagonal matrices with 1, 0, and -1 along the diagonal in any of the $3! = 6$ possible orders.

3 Notation

The following conventions will be observed in the remainder of the paper.

We denote by $\mathbb{N}$ and $\mathbb{N}^+$, respectively, the sets of nonnegative and of positive integers.

If P is a statement, then

$$\mathbf{1}_P = \begin{cases} 1 & P \text{ is true} \\ 0 & P \text{ is false.} \end{cases}$$

If S is a set, then $\mathbf{1}_S$ denotes the characteristic function $\mathbf{1}_S(x) = \mathbf{1}_{x \in S}$.

An *algebra* will always be commutative and of finite rank over a field, while a *ring* or *order* will be a finite-dimensional, torsion-free ring over a Dedekind domain, containing 1. An order need not be a domain.

If $a, b \in L$ are elements of a local or global field, a separable closure thereof, or a finite product of the preceding, we write $a|b$ to mean that $b = ca$ for some c in the appropriate ring of integers $\mathcal{O}_L$. If $a|b$ and $b|a$, we say that a and b are *associates* and write $a \sim b$. Note that a and b may be zero-divisors.

If S is a finite set, we let $\mathrm{Sym}(S)$ denote the set of permutations of S; thus $S_n = \mathrm{Sym}(\{1, \ldots, n\})$. If $|S| = |T|$, and if $g \in \mathrm{Sym}(S)$, $h \in \mathrm{Sym}(T)$ are elements, we say that g and h are *conjugate* if there is a bijection between S and T under which they correspond. Likewise when we say that two subgroups $G \subseteq \mathrm{Sym}(S)$, $H \subseteq \mathrm{Sym}(T)$ are conjugate.

We will use the semicolon to separate the coordinates of an element of a product of rings. For instance, in $\mathbb{Z} \times \mathbb{Z}$, the nontrivial idempotents are $(1;0)$ and $(0;1)$.

If n is a positive integer, then ζ_n denotes a primitive nth root of unity in $\bar{\mathbb{Q}}$, while $\bar{\zeta}_n$ denotes the nth root of unity

$$\bar{\zeta}_n = \left(1; \zeta_n; \zeta_n^2; \ldots; \zeta_n^{n-1}\right) \in \bar{\mathbb{Q}}^n.$$

Throughout the proofs of the local reflection theorems, we will fix a local field K, its valuation $v = v_K$, its residue field k_K of order q, and a uniformizer $\pi = \pi_K$. The letter e will denote the absolute ramification index ($e = v_K(2)$ in the quadratic and quartic cases, $v_K(3)$ in the cubic). We

let $\mathfrak{m}_K$ denote the maximal ideal, and likewise $\mathfrak{m}_{\bar{K}}$ be the maximal ideal of the ring $\mathcal{O}_{\bar{K}}$ of algebraic integers over K; note that $\mathfrak{m}_{\bar{K}}$ is not finitely generated. We also allow $v = v_K$ to be applied to elements of $\bar{K}$, the valuation being scaled so that its restriction to K has value group $\mathbb{Z}$. We use the absolute value bars $|\bullet|$ for the corresponding metric, whose normalization will be left undetermined.

If K is a local field, an *m-pixel* is a subset of an affine or projective space over $\mathcal{O}_K$ defined by requiring the coordinates to lie in specified congruence classes modulo π^n. For instance, in $\mathbb{P}^2(\mathcal{O}_K)$, a 0-pixel is the whole space, which is subdivided into $(q^2+q+1)q^{2n-2}$-many n-pixels for each $n \geq 1$.

If R/K is a finite-dimensional, locally free algebra over a ring, we denote by $R^{N=1}$ the subgroup of units of norm 1. The group operation is implicitly multiplication, so $R^{N=1}[n]$, for instance, denotes the nth roots of unity of norm 1.

Part II

Galois cohomology

4 Étale algebras and their Galois groups

4.1 Étale algebras

If K is a field, an *étale algebra* over K is a finite-dimensional separable commutative algebra over K, or equivalently, a finite product of finite separable extension fields of K. A treatment of étale algebras is found in Milne ([35], chapter 8): here we summarize this theory and prove a few auxiliary results that will be of use.

An étale algebra L of rank n admits exactly n maps $\iota_1, \ldots, \iota_n$ (of K-algebras) to a fixed separable closure $\bar{K}$ of K. We call these the *coordinates* of L; the set of them will be called $\mathrm{Coord}(L/K)$ or simply $\mathrm{Coord}(L)$. Together, the coordinates define an embedding of L into $\bar{K}^n$, which we call the *Minkowski embedding* because it subsumes as a special case the embedding of a degree-n number field into $\mathbb{C}^n$, which plays a major role in algebraic number theory, as in Delone-Faddeev [19].

For any element γ of the absolute Galois group G_K, the composition $\gamma \circ \iota_i$ with any coordinate is also a coordinate ι_j, so we get a homomorphism $\phi = \phi_L : G_K \to \mathrm{Sym}(\mathrm{Coord}(L)))$ such that

$$\gamma(\iota(x)) = (\phi_\gamma \iota)(x)$$

for all $x \in L, \iota \in \mathrm{Coord}(L)$. This gives a functor from étale K-algebras to G_K-sets (sets with a G_K-action), which is denoted $\mathcal{F}$ in Milne's terminology. A functor going the other way, which Milne calls $\mathcal{A}$, takes $\phi : G_K \to S_n$ to

$$L = \{(x_1, \ldots, x_n) \in \bar{K}^n \mid \gamma(x_i) = x_{\phi_\gamma(i)} \, \forall \gamma \in G_K, \forall i\} \tag{9}$$

Proposition 4.1 ([35], Theorem 7.29)**.** *The functors $\mathcal{F}$ and $\mathcal{A}$ establish a bijection between*

- *étale extensions L/K of degree n, up to isomorphism, and*
- *G_K-sets of size n up to isomorphism; that is to say, homomorphisms $\phi : G_K \to S_n$, up to conjugation in S_n.*

Moreover, the bijection respects base change, in the following way:

Proposition 4.2. *Let K_1/K be a field extension, not necessarily algebraic, and let L/K be an étale extension of degree n. Then $L_1 = L \otimes_K K_1$ is étale over K_1, and the associated Galois representations $\phi_{L/K}$, ϕ_{L_1/K_1} are related by the commutative diagram*

$$\begin{array}{ccc} G_{K_1} & \xrightarrow{\bullet|_{\bar{K}}} & G_K \\ \downarrow{\scriptstyle \phi_{L_1/K_1}} & & \downarrow{\scriptstyle \phi_{L/K}} \\ \mathrm{Sym}(\mathrm{Coord}_{K_1}(L_1)) & \xrightarrow{\sim} & \mathrm{Sym}(\mathrm{Coord}_K(L)) \end{array} \tag{10}$$

Proof. That L_1/K_1 is étale is standard (see Milne [35], Prop. 8.10). For the second claim, consider the natural restriction map $r : \mathrm{Coord}_{K_1}(L_1) \to \mathrm{Coord}_K(L)$. It is injective, since a K_1 linear map out of L_1 is determined by its values on L; and since both sets have the same size, r is surjective and is hence an isomorphism of G_{K_1}-sets (the G_{K_1}-structure on $\mathrm{Coord}_K(L)$ arising by restriction from

the G_K-structure). ■

We will use this proposition most frequently in the case that K is a global field and $K_1 = K_v$ one of its completions. The resulting L_1 is then the product $L_v \cong \prod_{w|v} L_w$ of the completions of L at the places dividing v. Note the departure from the classical habit of studying the completion L_w at each place individually. The preservation of degrees, $[L_1 : K_1] = [L : K]$ will be important for our applications.

4.2 The Galois group of an étale algebra

Define the *Galois group* $G(L/K)$ of an étale algebra to be the image of its associated Galois representation $\phi : G_K \to \mathrm{Sym}(\mathrm{Coord}(L))$. It transitively permutes the coordinates corresponding to each field factor. For example, if L is a quartic field, then $G(L/K)$ is one of the five (up to conjugacy) transitive subgroups of $\mathcal{S}_4$, which (to use the traditional names) are $\mathcal{S}_4$, $\mathcal{A}_4$, $\mathcal{D}_4$, $\mathcal{V}_4$, and $\mathcal{C}_4$. Galois groups in this sense are used in the tables of cubic and quartic fields in Delone-Faddeev [19] and the Number Field Database [28]. Note that the Galois group $G(L/K)$ is defined whether or not L is a Galois extension. If it is, then the Galois group is *simply* transitive and coincides with the Galois group in the sense of Galois theory.

Important for us will be two notions pertaining to the Galois group.

Definition 4.3. Let $G \subseteq \mathcal{S}_n$ be a subgroup. A *G-extension* of K is a degree-n étale algebra L with a choice of subgroup $G' \subseteq \mathrm{Sym}(\mathrm{Coord}(L))$ that is conjugate to G and contains $G(L/K)$, plus a conjugacy class of isomorphisms $G' \cong G$: the conjugacy being in G, not in $\mathcal{S}_n$. The added data is called a *G-structure* on L.

Proposition 4.4. *G-extensions L/K up to isomorphism are in bijection with homomorphisms $\phi : G_K \to G$, up to conjugation in G.*

Proof. Immediate from Proposition 4.1. ■

Example 4.5. $L = \mathbb{Q}(\zeta_5)$ is a $\mathcal{C}_4$-extension (taking $\mathcal{C}_4 = \langle (1234) \rangle \subseteq \mathcal{S}_4$), indeed its Galois group is isomorphic to $\mathcal{C}_4$; and L admits two distinct $\mathcal{C}_4$-structures, as there are two ways to identify $\mathcal{C}_4$ with

its image in $\mathcal{S}_4$, which are conjugate in $\mathcal{S}_4$ but not in $\mathcal{C}_4$. Likewise, $L = \mathbb{Q} \times \mathbb{Q} \times \mathbb{Q} \times \mathbb{Q}$ admits six $\mathcal{C}_4$-structures, one for each embedding of $\mathcal{C}_4$ into $\mathcal{S}_4$, as its Galois group is trivial.

4.3 Resolvents

This will be an important notion.

Definition 4.6. Let $G \subseteq \mathcal{S}_n$, $H \subseteq \mathcal{S}_m$ be subgroups and $\rho : G \to H$ be a homomorphism. Then for every G-extension L/K, the corresponding $\phi_L : G_K \to G$ may be composed with ρ to yield a map $\phi_R : G_K \to H$, which defines an étale extension R/K of degree m. This R is called the *resolvent* of L under the map ρ.

Example 4.7. Since there is a surjective map $\rho_{4,3} : \mathcal{S}_4 \to \mathcal{S}_3$, every quartic étale algebra L/K has a cubic resolvent R. This resolvent appears in Bhargava [4], but it is much older than that. It is generated by a formal root of the *resolvent cubic* that appears when a general quartic equation is to be solved by radicals.

Example 4.8. Likewise, the sign map can be viewed as a homomorphism $\operatorname{sgn} : \mathcal{S}_n \to \mathcal{S}_2$, attaching to every étale algebra L a quadratic resolvent T. If $L = K[\theta]/f(\theta)$ is generated by a polynomial f, and if $\operatorname{char} K \neq 2$, then it is not hard to see that $T = K[\sqrt{\operatorname{disc} f}]$ where $\operatorname{disc} f$ is the polynomial discriminant. Note that T still exists even if $\operatorname{char} K = 2$. We have that $T \cong K \times K$ is split if and only if the Galois group $G(L/K)$ is contained in the alternating group $\mathcal{A}_n$.

Example 4.9. The dihedral group $\mathcal{D}_4$ has an outer automorphism, because rotating a square in the plane by $45°$ does not preserve the square but does preserve every symmetry of the square. This map $\rho : \mathcal{D}_4 \to \mathcal{D}_4$ associates to each $\mathcal{D}_4$-algebra L a new $\mathcal{D}_4$-algebra L', not in general isomorphic. This is the classical phenomenon of the *mirror field*. For instance, if $L = \mathbb{Q}[\sqrt{1+\sqrt{2}}]$, then

$$L' = \mathbb{Q}\left[\sqrt{1+\sqrt{2}} + \sqrt{1-\sqrt{2}}\right] = \mathbb{Q}\left[\sqrt{2+2\sqrt{-1}}\right].$$

Both L and L' have the same Galois closure, a $\mathcal{D}_4$-octic extension of $\mathbb{Q}$. Likewise, the outer automorphism of $\mathcal{S}_6$ permits the association to each sextic étale algebra L/K a mirror sextic étale

algebra L'.

Example 4.10. The *Cayley embedding* is an embedding of any group G into $\mathrm{Sym}(G)$, acting by left multiplication. The Cayley embedding $\rho : \mathcal{S}_n \hookrightarrow \mathcal{S}_{n!}$ attaches to every étale algebra L of degree n an algebra $\tilde{L}$ of degree $n!$ with an $\mathcal{S}_n$-torsor structure. This is none other than the $\mathcal{S}_n$-*closure* of L, constructed by Bhargava in a quite different way in [4, Section 2].

More generally, for any $G \subseteq S_n$, the Cayley embedding $G \hookrightarrow \mathrm{Sym}(G)$ allows one to associate to each G-extension L a G-torsor T, which we may call the G-*closure* of L. The name "closure" is justified by the following observation: if $G \subseteq S_n$ is a transitive subgroup, then, since any transitive G-set is a quotient of the simply transitive one, we can embed L into T by Proposition 4.11 below. More generally, G-closures of ring extensions, not necessarily étale or even reduced, have been constructed and studied by Biesel [10, 11].

If $\rho : G \to H$ is invertible, as in many of the above examples, then the map from G-extensions to H-extensions is also invertible: we say that the two extensions are *mutual resolvents*.

4.4 Subextensions and automorphisms

The Galois group holds the answers to various natural questions about an étale algebra. The next two propositions are given without proof, since they follow immediately from the functorial character of the correspondence in Proposition 4.1

Proposition 4.11. *The subextensions $L' \subseteq L$ of an étale extension L/K, correspond to the equivalence relations $\sim$ on* $\mathrm{Coord}(L)$ *stable under permutation by $G(L/K)$, under the bijection*

$$\sim \mapsto L' = \{x \in L : \iota(x) = \iota'(x) \text{ whenever } \iota \sim \iota'\}.$$

Remark 4.12. Note that if L is a Galois field extension, the image of ϕ_L is a simply transitive subgroup $-$, and identifying $\mathrm{Coord}(L)$ with $-$, the stable equivalence relations are just right congruences modulo subgroups of $-$: so we recover the Galois correspondence between subgroups and subfields.

The Galois group is *not* a group of automorphisms of L. However, the automorphisms of L as a K-algebra can be described in terms of the Galois group readily.

Proposition 4.13. *Let L be Minkowski-embedded by its coordinates $\iota_1, \ldots, \iota_n$. Then the automorphism group* $\mathrm{Aut}(L/K)$ *is given by permutations of coordinates,*

$$\tau_\pi(x_1; \ldots; x_n) = x_{\pi^{-1}(1)}; \ldots; x_{\pi^{-1}(n)},$$

for π in the centralizer $C(S_n, G(L/K))$ of the Galois group.

(For $H \subseteq G$ groups, the *centralizer* $C(G, H)$ of H in G is the subgroup of elements of G that commute with every element of H.)

This provides a characterization, in terms of the Galois group, of rings having various kinds of automorphisms.

- Since S_2 is abelian, any étale algebra L of rank 2 has a unique non-identity automorphism, the conjugation $\bar{x} = \operatorname{tr} x - x$.
- If L has rank 4, automorphisms τ of L of order 2 whose fixed algebra is of rank 2 are in bijection with D_4-structures on L. Indeed, the conditions force τ to correspond to the permutation $\pi = (12)(34)$ or one of its conjugates, and the centralizer of this permutation is D_4.
- Particularly relevant is the case that L has a complete set of automorphisms that permute the coordinates simply transitively: this is a generalization of a Galois field extension called a *torsor*. This case is sufficiently important to merit its own subsection.

4.5 Torsors

Definition 4.14. Let G be a finite group. A *G-torsor* over K is an étale algebra L over K equipped with an action of G by automorphisms $\{\tau_g\}_{g \in G}$ that permute the coordinates simply transitively,

that is, such that $L \otimes_K \bar{K}$ is isomorphic to

$$\bigoplus_{g \in G} \bar{K}$$

with G acting by right multiplication on the indices.

Proposition 4.15. *Let G be a group of order n. An étale algebra L is a G-torsor if and only if it is a G-extension, where G is embedded into S_n by the Cayley embedding (G acting on itself by left multiplication). Moreover, there is a bijection between*

- *G-torsor structures on L, up to conjugation in G, and*
- *G-structures on L.*

The bijection is given in the following way: there is a labeling $\{\iota_g\}$ of the coordinates of L with the elements of G such that the Galois action is by left multiplication

$$g(\iota_h(x)) = \iota_{\phi_g h}(x) \tag{11}$$

while the torsor action is by right multiplication

$$\iota_g(\tau_h(x)) = \iota_{gh^{-1}}(x). \tag{12}$$

Proof. We first claim that the only elements of $\mathrm{Sym}(G)$ commuting with all right multiplications are left multiplications, and vice versa. If $\pi : G \to G$ is a permutation commuting with left multiplications, then

$$\pi(g) = \pi(g \cdot \mathrm{id}_G) = g \cdot \pi(\mathrm{id}_G),$$

so π is a right multiplication. So the embedded images of G in $\mathrm{Sym}(G)$ given by left and right multiplication (which are conjugate under the inversion permutation $\bullet^{-1} \in \mathrm{Sym}(G)$) are centralizers of one another. It is then clear that conjugates G' of G in $\mathrm{Sym}(\mathrm{Coord}(L))$ that *contain* $G(L/K)$ are in bijection with conjugates G'' that *commute* with $G(L/K)$. This establishes the first assertion.

For the bijection of structures, if an embedding $G \cong G' \subseteq \mathrm{Sym}(\mathrm{Coord}(L))$ is given, then we can label the coordinates with elements of G so that G acts on them by multiplication; then G'' gets identified with G by the corresponding right action. The only ambiguity is in which embedding is labeled with the identity element; if this is changed, one computes that the resulting identification of G'' with G is merely conjugated, so the map is well defined. The reverse map is constructed in exactly the same way. ■

Here is another perspective on torsors.

Proposition 4.16. *G-torsors over a field K, up to isomorphism, are determined by their field factor, a Galois extension L_1/K equipped with an embedding $\mathrm{Gal}(L/K) \hookrightarrow G$ up to conjugation in G.*

Proof. If T is a G-torsor, then since G permutes the coordinates simply transitively, all the coordinates have the same image; that is, the field factors of G are all isomorphic to a Galois extension L/K. The torsor operations fixing one field factor L_i of T realize the Galois group $\mathrm{Gal}(L/K)$ as a subgroup of G; changing the field factor L_i and/or the identification $L_i \cong L$ corresponds to conjugating the map $\mathrm{Gal}(L/K) \hookrightarrow G$ by an element of G.

Conversely, suppose L and an embedding

$$\mathrm{Gal}(L/K) \xrightarrow{\sim} H \subseteq G$$

are given. Let $1 = g_1, \ldots, g_r$ be coset representatives for G/H. Then $g_2, \ldots, g_r$ must map any field factor $L_1 \cong L$ isomorphically onto the remaining field factors $L_2, \ldots, L_r$, each L_i occurring once. To finish specifying the G-action on $T \cong L_1 \times \cdots \times L_r$, it suffices to determine $g|_{L_i}$ for each $g \in G$. Factor $gg_i = g_j h$ for some $j \in \{1, \ldots, r\}$, $h \in H$. Then for each $x \in L_1$, $g(g_i(x)) = g_j(h(x))$, and the value of this is known because the H-action on L_1 is known. It is easy to see that we get one and only one consistent G-torsor action in this way. ■

Because all field factors of a torsor are isomorphic, we will sometimes speak of "the" field factor of a torsor.

4.5.1 Torsors over étale algebras

On occasion, we will speak of a G-torsor over L, where L is itself a product $K_1 \times \cdots \times K_r$ of fields. By this we simply mean a product $T_1 \times \cdots \times T_r$ where each T_i is a G-torsor over K_i. This case is without conceptual difficulty, and some theorems on torsors will be found to extend readily to it, such as the following variant of the fundamental theorem of Galois theory:

Theorem 4.17. *Let T be a G-torsor over an étale algebra L. For each subgroup $H \subseteq G$,*

(a) The fixed algebra T^H is uniformly of degree $[G : H]$ over L (that is, of this same degree over each field factor of L);

(b) T is an H-torsor over T^H, under the same action;

(c) If H is normal, then T^H is also a G/H-torsor over L, under the natural action.

Proof. Adapt the relevant results from Galois theory. ■

4.6 A fresh look at Galois cohomology

Galois cohomology is one of the basic tools in the development of class field theory. It is usually presented in a highly abstract fashion, but certain Galois cohomology groups, specifically $H^1(K, M)$ for finite M, have explicit meaning in terms of field extensions of M. It seems that this interpretation is well known but has not yet been written down fully, a gap that we fill in here. We begin by describing Galois modules.

Proposition 4.18 (a description of Galois modules). *Let M be a finite abelian group, and let K be a field. Let M^- denote the subset of elements of M of maximal order m, the exponent of M. The following objects are in bijection:*

(a) Galois module structures on M over K, that is, continuous homomorphisms $\phi : G_K \to \operatorname{Aut} M$;

(b) $(\operatorname{Aut} M)$-torsors T/K;

(c) $(\operatorname{Aut} M)$-extensions L_0/K, where $\operatorname{Aut} M \hookrightarrow \operatorname{Sym} M$ in the natural way;

(*d*) (Aut M)*-extensions* L^-/K*, where* $\operatorname{Aut} M \hookrightarrow \operatorname{Sym} M^-$ *in the natural way.*

Proof. For item (d) to make sense, we need that M^- generates M; this follows easily from the classification of finite abelian groups.

The bijections are immediate from Propositions 4.4 and 4.15. ■

We will denote M with its Galois-module structure coming from these bijections by M_ϕ, M_T, or M_{L_0}. Note that T, L_0, and L^- are mutual resolvents.

Example 4.19. For example (and we will return to this case frequently), if we let $M = \mathcal{C}_3$ be the smallest group with nontrivial automorphism group: $\operatorname{Aut} M \cong \mathcal{C}_2$. Then the Galois module structures on M are in natural bijection with $\mathcal{C}_2$-torsors over K, that is, quadratic étale extensions T/K. If $\operatorname{char} K \neq 2$, these can be parametrized by Kummer theory as $T = K[\sqrt{D}]$, $D \in K^\times/(K^\times)^2$. The value $D = 1$ corresponds to the split algebra $T = K \times K$ and to the module M with trivial action. We have an isomorphism

$$M_T \cong \{0, \sqrt{D}, -\sqrt{D}\}$$

of G_K-sets, and of Galois modules if the right-hand side is given the appropriate group structure with 0 as identity.

In particular, the Galois-module structures on $\mathcal{C}_3$ form a group $\operatorname{Hom}(G_K, \mathcal{C}_2) \cong K^\times/(K^\times)^2$: the group operation can also be viewed as *tensor product* of one-dimensional $\mathbb{F}_3$-vector spaces with Galois action.

4.6.1 Galois cohomology

Note that the zeroth cohomology group $H^0(K, M)$ has a ready parametrization:

Proposition 4.20. *Let* $M = M_{L_0}$ *be a Galois module. The elements of* $H^0(K, M)$ *are in bijection with the degree-*1 *field factors of* L_0*.*

Proof. Proposition 4.18 establishes an isomorphism of G_K-sets between the coordinates of L_0 and the points of M. A degree-1 field factor corresponds to an orbit of G_K on $\operatorname{Coord}(L_0)$ of size 1, which corresponds exactly to a fixed point of G_K on M. ■

Deeper and more useful is a description of H^1. For an abelian group M, let $\mathcal{GA}(M) = M \rtimes \operatorname{Aut} M$ be the semidirect product under the natural action of $\operatorname{Aut} M$ on M. We can describe $\mathcal{GA}(M)$ more explicitly as the group of *affine-linear transformations* of M; that is, maps

$$a_{g,t}(x) = gx + t, \quad g \in \operatorname{Aut} M, t \in M$$

composed of an automorphism and a translation, the group operation being composition. In particular, we have an embedding

$$\mathcal{GA}(M) \hookrightarrow \operatorname{Sym}(M).$$

Proposition 4.21 (a description of H^1). *Let $M = M_\phi = M_{L_0}$ be a Galois module.*

(*a*) *$Z^1(K, M)$ is in natural bijection with the set of continuous homomorphisms $\psi : G_K \to \mathcal{GA}(M)$ such that the following triangle commutes:*

$$\begin{array}{ccc} G_K & \xrightarrow{\psi} & \mathcal{GA}(M) \\ & \searrow^{\phi} & \downarrow \\ & & \operatorname{Aut} M \end{array} \tag{13}$$

(*b*) *$H^1(K, M)$ is in natural bijection with the set of such $\psi : G_K \to \mathcal{GA}(M)$ up to conjugation by $M \subseteq \mathcal{GA}(M)$.*

(*c*) *$H^1(K, M)$ is also in natural bijection with the set of $\mathcal{GA}(M)$-extensions L/K (with respect to the embedding $\mathcal{GA}(M) \hookrightarrow \operatorname{Sym}(M)$) equipped with an isomorphism from their resolvent $(\operatorname{Aut} M)$-torsor to T.*

Proof. By the standard construction of group cohomology, Z^1 is the group of continuous crossed homomorphisms

$$Z^1(K, M) = \{\sigma : G_K \to M \mid \sigma(\gamma\delta) = \sigma(\gamma) + \phi(\gamma)\sigma(\delta)\}.$$

Send each σ to the map

$$\psi : G_K \to \mathcal{GA}(M)$$

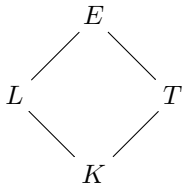
$$\gamma \mapsto a_{\phi(\gamma),\sigma(\gamma)}.$$

It is easy to see that the conditions for ψ to be a homomorphism are exactly those for σ to be a crossed homomorphism, establishing (a). For (b), we observe that adding a coboundary $\sigma_a(\gamma) = \gamma(a) - a$ to a crossed homomorphism σ is equivalent to post-conjugating the associated map $\psi : G_K \to \mathcal{GA}(M)$ by a. As to (c), a $\mathcal{GA}(M)$-extension carries the same information as a map ψ up to conjugation by *the whole of* $\mathcal{GA}(M)$. Specifying the isomorphism from the resolvent $(\operatorname{Aut} M)$-torsor to T means that the map $\pi \circ \psi = \phi : G_K \to \operatorname{Aut}(M)$ is known exactly, not just up to conjugation. Hence ψ is known up to conjugation by M. ■

Remark 4.22. The zero cohomology class corresponds to the extension L_0, with its structure given by the embedding $\operatorname{Aut} M \hookrightarrow \mathcal{GA}(M)$. This can be seen to be the unique cohomology class whose corresponding $\mathcal{GA}(X)$-extension has a field factor of degree 1.

If K is a local field, a cohomology class $\alpha \in H^1(K, M)$ is called *unramified* if it is represented by a cocycle $\alpha : \operatorname{Gal}(\bar{K}/K) \to M$ that factors through the unramified Galois group $\operatorname{Gal}(K^{\mathrm{ur}}/K)$. The subgroup of unramified coclasses is denoted by $H^1_{\mathrm{ur}}(K, M)$. If M itself is unramified (and we will never have to think about unramified cohomology in any other case), this is equivalent to the associated étale algebra L being unramified.

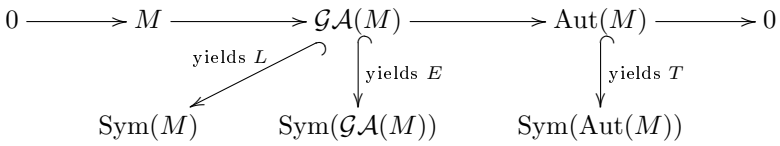
If $X = M_T$ is a Galois module and $\sigma \in Z^1(K, M)$ is the Galois module corresponding to a $\mathcal{GA}(X)$-extension L/K, we can also take the $\mathcal{GA}(X)$-closure of L, a $\mathcal{GA}(X)$-torsor E which fits into the following diagram:



(14)

Because of the semidirect product structure of $\mathcal{GA}(X)$, we have $E \cong L \otimes_K T$. It is also worth

tabulating the permutation representations of finite groups that yield each of the étale algebras discussed here:



(15)

4.6.2 The Tate dual

If M is a Galois module and the exponent m of M is not divisible by $\operatorname{char} K$, then

$$M' = \operatorname{Hom}(M, \mu_m)$$

is also a Galois module, called the *Tate dual* of M. The modules M and M' have the same order and are isomorphic as abstract groups, though not canonically; as Galois modules, they are frequently not isomorphic at all.

Example 4.23. If $M = M_{K[\sqrt{D}]}$ is one of the order-3 modules studied in Example 4.19, then the relevant μ_m is

$$\mu_3 \cong M_{K[\sqrt{-3}]}.$$

Examining the Galois actions (here it helps to use the theory of G_K-sets of size 2 presented in Knus and Tignol [30]), we see that

$$M' = M_{K[\sqrt{-3D}]}.$$

This explains the $D \mapsto -3D$ pattern in the Scholz reflection theorem and its generalizations, including cubic Ohno-Nakagawa.

Example 4.24. A module M of underlying group $\mathcal{C}_2 \times \mathcal{C}_2$ is always self-dual, regardless of what Galois-module structure is placed on it. This can be proved by noting that M has a unique alter-

nating bilinear form

$$B : M \times M \to \mu_2$$
$$(x, y) \mapsto \begin{cases} 1, & x = 0, y = 0, \text{ or } x = y \\ -1, & \text{otherwise.} \end{cases}$$

Being unique, it is Galois-stable and induces an isomorphism $M' \cong M$.

Particularly notable for us are the cases when $\mathcal{GA}(M)$ is the full symmetric group $\mathrm{Sym}(M)$, for then *every* étale algebra L/K of degree $|M|$ has a (unique) $\mathcal{GA}(M)$-affine structure. It is easy to see that there are only four such cases:

- $M = \{1\}$, $\mathcal{GA}(M) \cong \mathcal{S}_1$
- $M = \mathbb{Z}/2\mathbb{Z}$, $\mathcal{GA}(M) \cong \mathcal{S}_2$
- $M = \mathbb{Z}/3\mathbb{Z}$, $\mathcal{GA}(M) \cong \mathcal{C}_3 \rtimes \mathcal{C}_2 \cong \mathcal{S}_3$
- $M = \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$, $\mathcal{GA}(M) \cong (\mathcal{C}_2 \times \mathcal{C}_2) \rtimes \mathcal{S}_3 \cong \mathcal{S}_4$.

For degree exceeding 4, not every étale algebra arises from Galois cohomology, a restriction that plays out in the existing literature on reflection theorems. For instance, Cohen, Rubinstein-Salzedo, and Thorne [12] prove a reflection theorem in which one side counts $\mathcal{D}_p$-dihedral fields of prime degree $p \geq 3$. From our perspective, these correspond to cohomology classes of an $M = \mathcal{C}_p$ whose Galois action is by ± 1. The Tate dual of such an M can have Galois action by the full $(\mathbb{Z}/p\mathbb{Z})^\times$, and indeed they count extensions of Galois group $\mathcal{GA}(\mathcal{C}_p)$ on the other side of the reflection theorem. This will appear inevitable in light of the motivations elucidated in Part III.

5 Extensions of Kummer theory to explicitize Galois cohomology

Now that Galois cohomology groups $H^1(K, M)$ have been parametrized by étale algebras, can invoke parametrizations of étale algebras by even more explicit objects. The most familiar instance of this is *Kummer theory,* an isomorphism

$$H^1(K, \mu_m) \cong K^\times/(K^\times)^m$$

coming from the long exact sequence associated to the *Kummer sequence*

$$0 \longrightarrow \mu_m \longrightarrow \bar{K}^\times \xrightarrow{\bullet^m} \bar{K}^\times \longrightarrow 0.$$

In favorable cases, the cohomology $H^1(K, M)$ of other Galois modules M can be embedded into $R^\times/(R^\times)^m$ for some finite extension R of K.

We first state the hypothesis we need:

Definition 5.1. Let M be a finite Galois module of exponent m over a field K, and let X be a Galois-stable generating set of M. We say that M equipped with X is a *good* module if the natural map of Galois modules

$$\begin{aligned} \mathfrak{x} = \bigoplus_{x \in X} (\mathbb{Z}/m\mathbb{Z}) &\to M \\ e_x &\mapsto x \end{aligned}$$

is split, that is, its kernel admits a Galois-stable complementary direct summand $\tilde{M}$. Such a direct summand is known as a *good structure* on M.

Proposition 5.2. *The following examples of a Galois module M with generating set X are good:*

(*a*) *$M \cong \mathcal{C}_p$, with any action, and $X = M \setminus \{0\}$.*

(*b*) $M \cong \mathcal{C}_m^n$, *with any action preserving a basis* X.

(*c*) $M \cong \mathcal{C}_m^{n-1}$, $n \geq 2$ *with* $\gcd(m,n)$, *with an action that preserves a* hyperbasis X, *that is, a generating set of* n *elements with sum* 0.

Proof. (a) Here the Galois modules are representations of $\mathbb{F}_p^\times \cong \mathcal{C}_{p-1}$ over $\mathbb{F}_p$. Since the group and field are of coprime order, complete reducibility holds: any subrepresentation is a direct summand. In fact, $\mathfrak{X}$ is the regular representation, M is the tautological representation in which each $\lambda \in \mathbb{F}_p^\times$ acts by multiplication by λ, and $\tilde{M}$ can be taken (uniquely in general) to be the product of all the other isotypical components of $\mathfrak{X}$.

(b) Here the natural map $\mathfrak{X} \to M$ is an isomorphism, so $\tilde{M} = \mathfrak{X}$.

(c) Here the natural map $\mathfrak{X} \to M$ is the quotient by the one-dimensional space

$$\left\langle \sum_{x \in X} e_x \right\rangle.$$

This space has a Galois-stable direct complement, namely the kernel $\tilde{M}$ of the linear functional

$$\mathfrak{X} \to \mathbb{F}_2$$
$$e_x \to 1.$$

■

Proposition 5.3. *Let* M *be a Galois module with a good structure* $(X, \tilde{M})$, *and let* R *be the resolvent algebra corresponding to the* G_K*-set* X. *For any Galois module* A *with underlying group* $\mathbb{Z}/m\mathbb{Z}$, *there is a natural injection*

$$H^1(K, M \otimes A) \to H^1(R, A)$$

as a direct summand. The cokernel is naturally isomorphic to

$$H^1(K, (\mathfrak{X}/\tilde{M}) \otimes A).$$

Proof. We use the good structure

$$M \cong \tilde{M} \hookrightarrow \mathfrak{X}$$

to embed

$$H^1(K, \tilde{M} \otimes A) \hookrightarrow H^1(\mathfrak{X} \otimes A).$$

Since $\tilde{M}$ is a direct summand, this is an injection with cokernel naturally isomorphic to $H^1(K, (\mathfrak{X}/\tilde{M}) \otimes A)$. It remains to construct an isomorphism

$$H^1(\mathfrak{X} \otimes A) \xrightarrow{\sim} H^1(R, A).$$

If R decomposes as a product

$$R \cong R_1 \times \cdots \times R_s$$

of field factors corresponding to the orbits $X = \bigsqcup_i X_i$ of G_K on X, then $\mathfrak{X}$ has a corresponding decomposition

$$\mathfrak{X} = \bigoplus_{i=1}^{s} \mathfrak{X}_i$$

where $\mathfrak{X}_i = \langle e_x : x \in X_i \rangle$ is none other than the induced module $\operatorname{Ind}_K^{R_i} \mathbb{Z}/m\mathbb{Z}$. Its cohomology is computed by Shapiro's lemma:

$$H^1(K, \mathfrak{X} \otimes A) \cong \bigoplus_{i=1}^{s} H^1(K, \mathfrak{X}_i \otimes A) = \bigoplus_{i=1}^{s} H^1(K, \operatorname{Ind}_K^{R_i} A) \cong \bigoplus_{i=1}^{s} H^1(R_i, A) = H^1(R, A).$$

This is the desired isomorphism. ∎

We can harness Kummer theory to parametrize cohomology of other modules as follows.

Theorem 5.4 (an extension of Kummer theory). *Let M be a finite Galois module, and assume that $m = \exp M$ is not divisible by $\operatorname{char} K$. Let G_K act on the set M'^{-} of surjective characters $\chi : M \twoheadrightarrow \mu_m$ through its actions on M and μ_m, and let F be the étale algebra corresponding to this G_K-set.*

(*a*) *There is a natural group homomorphism*

$$\mathrm{Kum} : H^1(K, M) \to F^\times/(F^\times)^m.$$

(*b*) *If* $M \cong \mathcal{C}_p$ *is cyclic of prime order, then* Kum *is injective,* F *is naturally a* $(\mathbb{Z}/p\mathbb{Z})^\times$*-torsor, and*

$$\mathrm{im}(\mathrm{Kum}) = \left\{\alpha \in F^\times/(F^\times)^p : \tau_c(\alpha) = \alpha^c \,\forall c \in (\mathbb{Z}/p\mathbb{Z})^\times\right\}.$$

If $p = 3$*, then the image simplifies to*

$$\mathrm{im}(\mathrm{Kum}) = \left\{\alpha \in F^\times/(F^\times)^3 : N_{F/K}(\alpha) = 1\right\},$$

and the $\mathcal{GA}(\mathcal{C}_3) \cong S_3$*-extension* L *corresponding to a given* $\alpha \in F^\times/(F^\times)^3$ *of norm* 1 *can be described as follows: Define a* K*-linear map*

$$\begin{aligned} \kappa : K &\to \bar{K}^3 \\ \xi &\mapsto \left(\mathrm{tr}_{\bar{K}^2/K}\, \xi\omega \sqrt[3]{\delta}\right)_\omega, \end{aligned}$$

where $\sqrt[3]{\delta} \in \bar{K}^2$ *is chosen to have norm* 1*, and* ω *ranges through the set*

$$\{(1;1), (\zeta_3;\zeta_3^2); (\zeta_3^2;\zeta_3)\}$$

of cube roots of 1 *in* $\bar{K}^2$ *of norm* 1*. Then*

$$L = K + \kappa(F).$$

(*c*) *If* $M \cong \mathcal{C}_2 \times \mathcal{C}_2$*, then* Kum *is injective and*

$$\mathrm{im}(\mathrm{Kum}) = \left\{\alpha \in F^\times/(F^\times)^2 : N_{F/K}(\alpha) = 1\right\}.$$

Moreover, the $\mathcal{GA}(M) \cong S_4$-extension corresponding to a given $\alpha \in F^\times/(F^\times)^2$ of norm 1 can be described as follows: Define a K-linear map

$$\begin{aligned} \kappa : K &\to \bar{K}^4 \\ \xi &\mapsto \left(\mathrm{tr}_{\bar{K}^3/K}\, \xi\omega\sqrt{\delta}\right)_\omega, \end{aligned}$$

where $\sqrt{\delta} \in \bar{K}^3$ is chosen to have norm 1, and ω ranges through the set

$$\{(1;1;1),(1;-1;-1);(-1;1;-1);(-1;-1;1)\}$$

of square roots of 1 in $\bar{K}^3$ of norm 1. Then

$$L = K + \kappa(F).$$

Proof. If $\chi : M \twoheadrightarrow \mu_m$ is a surjective character, let F_χ be the fixed field of the stabilizer of χ; thus F_χ is the field factor of F corresponding to the G_K-orbit of χ. If $\chi_1, \ldots, \chi_\ell$ are orbit representatives, we can map

$$H^1(K,M) \xrightarrow{\prod \mathrm{res}} \prod_i H^1(F_{\chi_i}, M) \xrightarrow{\prod \chi_{i*}} \prod_i H^1(F_{\chi_i}, \mu_m) \cong \prod_i F_{\chi_i}^\times/(F_{\chi_i}^\times)^m \cong F^\times/(F^\times)^m.$$

This yields our map Kum. Alternatively, note that by Shapiro's lemma,

$$\prod_i H^1(F_{\chi_i}, \mu_m) \cong \prod_i H^1(K, \mathrm{Ind}_{F_{\chi_i}}^K \mu_m) \cong H^1(K, I),$$

where

$$I_M = \mathrm{Ind}_F^K \mu_m = \bigoplus_{\chi : M \twoheadrightarrow \mu_m} \mu_m,$$

a Galois module under the action

$$g\big((a_\chi)_i\big) = \big(g(c_{g^{-1}(\chi)})_\chi\big) = \big(g(c_{\chi(g\bullet)})_\chi\big).$$

Under this identification, it is not hard to check that Kum $= j_*$, where j is the inclusion $M \hookrightarrow I_M$ given by

$$a \mapsto (\chi(a))_\chi.$$

Although j is injective (because the characters of maximal order m generate the group of all characters), it is not obvious whether j induces an injection on cohomology, nor what the image is. What makes the modules M in parts (b) and (c) tractable is that, in these cases, $M\backslash\{0\}$ is a *good* generating set for M, so M is a direct summand of I_M. In part (b), we can identify

$$I_M \cong \mathrm{Ind}_{\{1\}}^{(\mathbb{Z}/p\mathbb{Z})^\times} \mathbb{F}_p \otimes_{\mathbb{F}_p} \mu_m$$

as a twist of the regular representation of $(\mathbb{Z}/p\mathbb{Z})^\times$ over $\mathbb{F}_p$. Since $\mathbb{F}_p$ has a complete set of $(p-1)$st roots of unity, this representation splits completely into one-dimensional subrepresentations. The image of j is the eigenspace generated by $(c)_{c\in\mathbb{Z}/p\mathbb{Z}^\times}$, so Kum is injective and its image is the subspace of $F^\times/(F^\times)^p$ cut out by the same relations $\tau_c(x) = cx$ (where τ_c is the torsor operation on F, resp. the automorphism of I_M, indexed by c) that cut out $j(M)$ in I_M.

As to part (c), since $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ has three surjective characters whose product is 1, we have $I_M/M \cong \mu_2$ with the map $\eta : I_M \to \mu_2$ given by multiplying the coordinates. Since μ_2 also injects diagonally into I_M, we easily get a direct sum decomposition, which shows that Kum is injective. As to the image, it is not hard to show that the diagram

$$\begin{array}{ccccc} F^\times/(F^\times)^2 & \xrightarrow{\sim} & H^1(F,\mathcal{C}_2) & \xrightarrow{\sim} & H^1(K,I) \\ \downarrow{\scriptstyle N} & & \downarrow{\scriptstyle \mathrm{cor}} & \swarrow{\scriptstyle \eta_*} & \\ K^\times/(K^\times)^2 & \xrightarrow{\sim} & H^1(K,C_2) & & \end{array}$$

commutes, establishing the desired norm characterization of im(Kum).

The formulas by radicals for the cubic and quartic algebras corresponding to a Kummer element follow easily by chasing through the Galois actions on the appropriate étale algebras. The quartic case is also considered by Knus and Tignol, where a closely related description of L is given ([30], Proposition 5.13). ■

Remark 5.5. For general M, the map $H^1(K, M) \to F^\times/(F^\times)^m$ may be made by the construction in Theorem 5.4, but its image is hard to characterize, and it may not even be injective: for instance, when $M \cong \mathcal{C}_4$, coclasses correspond to $\mathcal{D}_4$-extensions, and Kum conflates each extension with its mirror extension (compare Example 4.9).

Though it will not be used in the sequel, it is worth noting that Artin-Schreyer theory is amenable to the same treatment.

Theorem 5.6. *Let Let M be a finite Galois module with underlying abelian group A of exponent $m = p = \operatorname{char} K$.*

(*a*) *There is a natural map*

$$\mathrm{AS} : H^1(K, M) \to F/\wp(F).$$

(*b*) *If $A \cong \mathcal{C}_p$, then* AS *is injective, F is naturally a $(\mathbb{Z}/p\mathbb{Z})^\times$-torsor, and*

$$\operatorname{im}(\mathrm{AS}) = \left\{\alpha \in F/\wp(F) : \tau_c(\alpha) = c\alpha \ \forall c \in (\mathbb{Z}/p\mathbb{Z})^\times\right\}.$$

(*c*) *If $p = 2$ and $A \cong \mathcal{C}_2 \times \mathcal{C}_2$, then* AS *is injective and*

$$\operatorname{im}(\mathrm{AS}) = \left\{\alpha \in F/\wp(F) : \operatorname{tr}_{F/K}(\alpha) = 0\right\}.$$

5.1 The Tate pairing and the Hilbert symbol

Assume now that K is a local field. Our next step will be to understand the (local) Tate pairing, which is given by a cup product

$$\langle\ ,\ \rangle_T : H^1(K, M) \times H^1(K, M') \to H^2(K, \mu_m) \cong \mu_m.$$

As we were able to parametrize the cohomology groups $H^1(K, M)$ in favorable cases, it should not come as a surprise that we can often describe the Tate pairing with similar explicitness.

Recall the definitions of the Artin and Hilbert symbols. If $M \cong \mathbb{Z}/m\mathbb{Z}$ has *trivial* G_K-action, then $M' \cong \mu_m$, and we have a Tate pairing

$$\langle\ ,\ \rangle_T : H^1(K, \mathbb{Z}/m\mathbb{Z}) \times H^1(K, \mu_m) \to \mu_m$$

Now $H^1(K, \mathbb{Z}/m\mathbb{Z}) \cong \mathrm{Hom}(K, \mathbb{Z}/m\mathbb{Z})$ parametrizes $\mathbb{Z}/m\mathbb{Z}$-torsors, while by Kummer theory, $H^1(K, \mu_m) \cong K^\times/(K^\times)^m$. The Tate pairing in this case is none other than the *Artin symbol* (or *norm-residue symbol*) $\phi_L(x)$ which attaches to a cyclic extension L, of degree dividing m, a mapping $\phi_L : K^\times \to \mathrm{Gal}(L/K) \to \mu_m$ whose kernel is the norm group $N_{L/K}(L^\times)$ (see Neukirch [40], Prop. 7.2.13). If, in addition, $\mu_m \subseteq K$, then $H^1(K, \mathbb{Z}/m\mathbb{Z})$ is also isomorphic to $K^\times/\left(K^\times\right)^m$, and the Tate pairing is an alternating pairing

$$\langle\ ,\ \rangle : K^\times/\left(K^\times\right)^m \times K^\times/\left(K^\times\right)^m \to \mu_m$$

classically called the *Hilbert symbol* (or *Hilbert pairing*). It is defined in terms of the Artin symbol by

$$\langle a, b\rangle = \phi_{K[\sqrt[m]{b}]}(a). \tag{16}$$

In particular, $\langle a, b\rangle = 1$ if and only if a is the norm of an element of $K[\sqrt[m]{b}]$. This can also be described in terms of the splitting of an appropriate Severi-Brauer variety; for instance, if $m = 2$,

we have $\langle a, b\rangle = 1$ exactly when the conic

$$ax^2 + by^2 = z^2$$

has a K-rational point. See also Serre ([51], §§XIV.1–2). (All identifications between pairings here are up to sign; the signs are not consistent in the literature and are totally irrelevant for this paper.) Pleasantly, for the types of M featured in Theorem 5.4, the Tate pairing can be expressed simply in terms of the Hilbert pairing.

We extend the Hilbert pairing to étale algebras in the obvious way: if $L = K_1 \times \cdots \times K_s$, then

$$\langle (a_1; \ldots; a_s), (b_1; \ldots; b_s)\rangle_L := \langle a_1, b_1\rangle_{K_1} \cdot \cdots \cdot \langle a_s, b_s\rangle_{K_s}.$$

Note that if a is a norm from $L[\sqrt[m]{b}]$ to L, then $\langle a, b\rangle_L = 1$, but the converse no longer holds. We then have the following:

Theorem 5.7 (a formula for the local Tate pairing). *Let K be a local field. For M, F as in Theorem 5.4, let M' be the Tate dual of M, and let F' be the corresponding étale algebra, corresponding to the G_K-set M^- of elements of maximal order in M, just as F corresponds to M'^-. The Tate pairing*

$$\langle \bullet, \bullet\rangle : H^1(K, M) \times H^1(K, M') \to H^2(K, \mu_m) \cong \mathcal{C}_m$$

can be described in terms of the Hilbert pairing in the following cases:

(a) If $A \cong \mathcal{C}_p$, then both F and F' embed naturally into $F'' := F[\mu_p]$, and the Tate pairing is the restriction of the Hilbert pairing on F''.

(b) If $A \cong (\mathbb{Z}/2\mathbb{Z})^2$, then we have natural isomorphisms $M \cong M'$, $F \cong F'$, and the Tate pairing is the restriction of the Hilbert pairing on F.

Proof. In case (b), set $F'' = F = F[\mu_2]$. We will do the two cases largely in parallel.

Let $\mathrm{Surj}(A, B) \subseteq \mathrm{Hom}(A, B)$ denote the set of surjections between two groups A, B. Note that if A, B are Galois modules, then $\mathrm{Surj}(A, B)$ is a G_K-set. Note that F'' is the étale algebra

corresponding to the G_K-set

$$Z = \mathrm{Surj}(M, \mu_p) \times \mathrm{Surj}(\mu_p, \mathbb{Z}/m\mathbb{Z}).$$

There is an obvious map $Z \to \mathrm{Surj}(M, \mu_p)$ given by projection to the first factor, which allows us to recover the identification $F'' = F[\mu_m]$. There is also a map of G_K-sets

$$\Psi : Z \to \mathrm{Surj}(M', \mu_p)$$

which sends a pair (χ, u) (where $\chi : M \twoheadrightarrow \mu_m$, $u : \mu_m$) to the unique surjective $\psi : M' \to \mu_p$ satisfying

$$\begin{cases} \psi(\chi) = u^{-1}(1), & A \cong \mathcal{C}_p \\ \psi(\chi) = 1, & A \cong \mathcal{C}_2 \times \mathcal{C}_2. \end{cases}$$

This allows us to embed F' into F''. It is worth noting that when $A \cong \mathcal{C}_2 \times \mathcal{C}_2$, u carries no information and $F \cong F' \cong F''$.

Let $F''_1, \ldots, F''_\ell$ be the field factors of F''; each F''_i corresponds to an orbit $G_K(\chi_i, u_i)$ on Z. Let $\psi_i = \Psi(\chi_i, u_i)$. Then for $\sigma \in H^1(K, M)$, $\tau \in H^1(K, M')$,

$$\begin{aligned} \langle \sigma, \tau \rangle_{\mathrm{Hilb}} &= \langle \mathrm{Kum}(\sigma), \mathrm{Kum}(\tau) \rangle_{\mathrm{Hilb};\ F''} \\ &= \prod_{F''_i} \mathrm{inv}_{F''_i} \left(\chi_{i*} \operatorname{res}^K_{F''_i} \sigma \cup \psi_{i*} \operatorname{res}^K_{F''_i} \tau \right). \end{aligned}$$

Since $\mathrm{inv}_{F''_i} = \mathrm{inv}_K \circ \operatorname{cor}^K_{F''_i}$ (a standard fact), we have

$$\begin{aligned} \langle \sigma, \tau \rangle_{\mathrm{Hilb}} &= \mathrm{inv}_K \sum_{F''_i} \operatorname{cor}^K_{F''_i} \left(\chi_{i*} \operatorname{res}^K_{F''_i} \sigma \cup \psi_{i*} \operatorname{res}^K_{F''_i} \tau \right) \\ &= \mathrm{inv}_K \sum_{F''_i} \operatorname{cor}^K_{F''_i} \left(\mathrm{ev} \circ (\chi_i \otimes \psi_i) \right)_* \operatorname{res}^K_{F''_i} (\sigma \cup \tau) \end{aligned}$$

where $\mathrm{ev} : M \otimes M' \to \mu_m$ is the evaluation map. We now apply the following lemma, which slightly

generalizes results seen in the literature.

Lemma 5.8. *Let $H \subseteq G$ be a subgroup of finite index. Let X and Y be G-modules, and let $f : X \to Y$ be a map that is H-linear (but not necessarily G-linear). Denote by $\tilde{f}$ the G-linear map*

$$\tilde{f}(x) = \sum_{gH \in G/H} gfg^{-1}(x).$$

Let $\sigma \in H^n(H, Y)$. Then

$$\operatorname{cor}_H^G(f_* \operatorname{res}_H^G \sigma) = \tilde{f}_* \sigma.$$

Proof. Since we are concerned with the equality of a pair of δ-functors, we can apply dimension shifting to assume that $n = 0$. The proof is now straightforward. ∎

Applying with $G = G_K$, $H = G_{F_i''}$, and $f = \operatorname{ev} \circ (\chi_i \otimes \psi_i) : M \otimes M' \to \mu_m$, we get

$$\begin{aligned}\langle \sigma, \tau \rangle_{\text{Hilb}} &= \operatorname{inv}_K \sum_{F_i''} \Big(\sum_{g \in G_K / G_{F_i''}} g \circ \operatorname{ev} \circ (\chi_i \circ g^{-1} \otimes \psi_i \circ g^{-1}) \Big) \\ &= \operatorname{inv}_K \sum_{F_i''} \Big(\sum_{g \in G_K / G_{F_i''}} \big(\operatorname{ev} \circ (\chi_{i,g} \otimes \psi_{i,g}) \big) \Big)_* (\sigma \cup \tau),\end{aligned}$$

where $\chi_{i,g} = g(\chi_i)$ and $\psi_{i,g} = g(\psi_i)$ are given by the natural action. Now the outer sum runs over all G_K-orbits of Z while the inner sum runs over the elements of each orbit, so we simply get

$$\langle \sigma, \tau \rangle_{\text{Hilb}} = \operatorname{inv}_K \Big(\sum_{(\chi, u) \in Z} \operatorname{ev} \circ (\chi \otimes \Psi(\chi, u)) \Big)_* (\sigma \cup \tau).$$

Since the Tate pairing is given by

$$\langle \sigma, \tau \rangle_{\text{Tate}} = \operatorname{inv}_K \operatorname{ev}_* (\sigma \cup \tau),$$

it remains to check that

$$\sum_{(\chi,u)\in Z} \mathrm{ev} \circ (\chi \otimes \Psi(\chi, u)) = \mathrm{ev}$$

as maps from $M \otimes M'$ to μ_m. In the case $M \cong \mathcal{C}_p$, each term is actually equal to ev, and there are $(p-1)^2 \equiv 1 \bmod p$ terms. In the case $M \cong \mathcal{C}_2 \times \mathcal{C}_2$, a direct verification on a basis of $M \otimes M'$ is not difficult. ■

6 Rings over a Dedekind domain

Thus far, we have been considering étale algebras L over a field K. We now suppose that K is the fraction field of a Dedekind domain $\mathcal{O}_K$ (not of characteristic 2), which for us will usually be a number field or a completion thereof, although there is no need to be so restrictive. Our topic of study will be the subrings of L that are lattices of full rank over $\mathcal{O}_K$—the *orders,* to use the standard but unfortunately overloaded word.

There is always a unique *maximal order* $\mathcal{O}_L$, the integral closure of $\mathcal{O}_K$ in L. If $L = L_1 \times \cdots \times L_r$ is a product of field factors, we have $\mathcal{O}_L = \mathcal{O}_{L_1} \times \cdots \times \mathcal{O}_{L_r}$.

6.1 Indices of lattices

There is one piece of notation that we explain here to avoid confusion. If V is an n-dimensional vector space over K and $A, B \subseteq V$ are two full-rank lattices, we denote by the *index* $[A : B]$ the unique fractional ideal $\mathfrak{c}$ such that

$$\Lambda^n A = \mathfrak{c} \Lambda^n B$$

as $\mathcal{O}_K$-submodules of the top exterior power $\Lambda^n V$. Alternatively, if $A \supseteq B$, then the classification theorem for finitely generated modules over $\mathcal{O}_K$ lets us write

$$A/B \cong \mathcal{O}_K/\mathfrak{c}_1 \oplus \cdots \oplus \mathcal{O}_K/\mathfrak{c}_r,$$

and the index equals

$$\mathfrak{c}_1\mathfrak{c}_2\cdots\mathfrak{c}_r.$$

The index satisfies the following basic properties:

- $[A:B][B:C]=[A:C]$;
- If V is a vector space over both K and a finite extension L, and A and B are two $\mathcal{O}_L$-sublattices, then $[A:B]_K = N_{L/K}[A:B]_L$;
- If $V=L$ is a K-algebra and $\alpha\in L^\times$, then $[A:\alpha A]=N_{L/K}(\alpha)$.

Despite the apparent abstractness of its definition, the index $[A:B]$ is *not* hard to compute in particular cases: localizing at a prime ideal, we can assume $\mathcal{O}_K$ is a PID, and then it is the determinant of the matrix expressing any basis of B in terms of a basis of A.

If L is a K-algebra, $\mathcal{O}\subseteq L$ is an order, and $\mathfrak{a}\subseteq L$ is a fractional ideal, the index $[\mathcal{O}:\mathfrak{a}]$ is called the *norm* of $\mathfrak{a}$ and will be denoted by $N_{\mathcal{O}}(\mathfrak{a})$ or, when the context is clear, by $N(\mathfrak{a})$. Note the following basic properties:

- If $\mathfrak{a}=\alpha\mathcal{O}$ is principal, then $N_{\mathcal{O}}(\mathfrak{a})=N_{L/K}(\alpha)$.
- If $\mathfrak{a}$ and $\mathfrak{b}$ are two $\mathcal{O}$-ideals and $\mathfrak{a}$ is invertible, then $N(\mathfrak{ab})=N(\mathfrak{a})N(\mathfrak{b})$. This is easily derived from the theorem that an invertible ideal is locally principal (Lemma 14.2). It is false for two arbitrary $\mathcal{O}$-ideals.
- If $\mathcal{O}_K=\mathbb{Z}$ or $\mathbb{Z}_p$, then for any L and $\mathcal{O}$, the norm $N_{\mathcal{O}}(\mathfrak{a})$ of an integral ideal is the ideal generated by the absolute norm $|\mathcal{O}/\mathfrak{a}|$.

6.2 Discriminants

As is standard, we define the *discriminant ideal* of an order $\mathcal{O}$ in an étale algebra L to be the ideal $\mathfrak{d}$ generated by the trace pairing

$$\begin{aligned} \tau : \mathcal{O}^{2n} &\to \mathcal{O}_K \\ (\xi_1, \xi_2, \ldots, \xi_n, \eta_1, \eta_2, \ldots, \eta_n) &\mapsto \det[\operatorname{tr} \xi_i \eta_j]_{i,j=1}^n. \end{aligned} \tag{17}$$

The trace pairing is nondegenerate, that is, $\mathfrak{d} \neq 0$ (this is one equivalent definition of étale). The primes dividing $\mathfrak{d}$ are those at which L is ramified and/or $\mathcal{O}$ is nonmaximal. This notion is standard and widely used. However, it does not quite extend the (also standard) notion of the discriminant of a $\mathbb{Z}$-algebra over $\mathbb{Z}$, which has a distinction between positive and negative discriminants. The Ohno-Nakagawa theorem involves this distinction prominently; Dioses [20] and Cohen–Rubinstein-Salzedo–Thorne [12] each frame their extensions of O-N in terms of an ad-hoc notion of discriminant that incorporates the splitting data of an order at the infinite primes. Here we explain the variant that we will use.

Since the trace pairing τ is alternating in the ξ's and also in the η's, it can be viewed as a bilinear form on the rank-1 lattice $\Lambda^n \mathcal{O}$. Identifying $\Lambda^n \mathcal{O}$ with a (fractional) ideal $\mathfrak{c}$ of $\mathcal{O}_K$ (whose class is often called the *Steinitz class* of $\mathcal{O}$), we can write

$$\tau(\xi) = D\xi^2$$

for some nonzero $D \in \mathfrak{c}^{-2}$. Had we rescaled the identification $\Lambda^n \mathcal{O} \to \mathfrak{c}$ by $\lambda \in K^\times$, D would be multiplied by λ^2. We call the pair $(\mathfrak{c}, D)$, up to the equivalence $(\mathfrak{c}, D) \sim (\lambda\mathfrak{c}, \lambda^{-2} D)$, the *discriminant* of $\mathcal{O}$ and denote it by $\operatorname{Disc} \mathcal{O}$.

There is another perspective on the discriminant $\operatorname{Disc} \mathcal{O}$. Let $\tilde{L}$ be the S_n-torsor corresponding to L, which comes with n embeddings $\kappa_1, \ldots, \kappa_n : L \to \tilde{L}$ freely permuted by the S_n-action (not to

be confused with the n coordinates of L). Noting that, for any $\alpha \in L$,

$$\mathrm{tr}(\alpha) = \sum_i \kappa_i(\alpha),$$

we can factor the trace pairing matrix:

$$[\mathrm{tr}\, \xi_i \eta_j]_{i,j} = [\kappa_h(\xi_i)]_{i,h} \cdot [\kappa_h(\eta_j)]_{h,j}.$$

Define

$$\tau_0(\xi_1, \ldots, \xi_n) = \det[\kappa_h(\xi_i)]_{i,h},$$

so that

$$\tau(\xi_1, \ldots, \xi_n, \eta_1, \ldots, \eta_n) = \tau_0(\xi_1, \ldots, \xi_n) \cdot \tau_0(\eta_1, \ldots, \eta_n).$$

Now look more carefully at the map τ_0. First, τ_0 is alternating under permutations of the ξ_i's, so it defines a linear map

$$\tau_0 : \mathfrak{c} \to \tilde{L}.$$

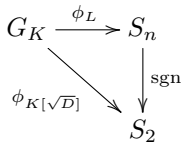
Moreover, τ_0 is alternating under postcomposition by the torsor action of S_n on $\tilde{L}$, which permutes the κ_h freely. Thus the image of τ_0 lies in the C_2-torsor $T_2 = \tilde{L}^{A_n}$, which we call the *discriminant torsor* of L, and even more specifically in the (-1)-eigenspace of the nontrivial element of C_2. By (the simplest case of) Kummer theory, we may write $T_2 = K[\sqrt{D'}]$. If $(\xi_1, \ldots, \xi_n)$ is any K-basis of $\mathcal{O}_L$, so that $\xi_1 \wedge \cdots \wedge \xi_n$ corresponds to some nonzero element $c \in \mathfrak{c}$, then

$$Dc^2 = \tau(c, c) = \tau_0(c)^2 = \left(a\sqrt{D'}\right)^2 = D'a^2.$$

Thus $T_2 = K[\sqrt{D}]$. We summarize this result in a proposition.

Proposition 6.1. *If L is an étale algebra over K of discriminant $(\mathfrak{c}, D)$, then $K[\sqrt{D}]$ is the dis-*

criminant torsor of L; that is, the diagram of Galois structure maps



commutes.

There is notable integral structure on D as well.

Lemma 6.2 (**Stickelberger's theorem over Dedekind domains**). *If $(\mathfrak{c}, D)$ is the discriminant of an order $\mathcal{O}$, then $D \equiv t^2 \bmod 4\mathfrak{c}^{-2}$ for some $t \in \mathfrak{c}^{-1}$.*

Remark 6.3. When $\mathcal{O}_K = \mathbb{Z}$, Lemma 6.2 states that the discriminant of an order is congruent to 0 or 1 mod 4: a nontrivial and classical theorem due to Stickelberger. Our proof is a generalization of the most familiar one for Stickelberger's theorem, due to Schur [50].

Proof. Since $D \in \mathfrak{c}^{-2}$, the conclusion can be checked locally at each prime dividing 2 in $\mathcal{O}_K$. We can thus assume that $\mathcal{O}_K$ is a DVR and in particular that $\mathfrak{c} = (1)$. Now there is a simple tensor $\xi_1 \wedge \cdots \wedge \xi_n$ that corresponds to the element $1 \in \mathfrak{c}$. By definition,

$$\sqrt{D} = \tau_0(\xi_1, \ldots, \xi_n) = \det[\kappa_h(\xi_i)]_{i,h} = \sum_{\pi \in S_n} \left(\operatorname{sgn}(\sigma) \prod_i \kappa_{\pi(i)}(\xi_i) \right) = \rho - \bar{\rho}, \tag{18}$$

where

$$\rho = \sum_{\pi \in A_n} \prod_i \kappa_{\pi(i)}(\xi_i)$$

lies in T_2 by symmetry and $\bar{\rho}$ is its conjugate. By construction, ρ is integral over $\mathcal{O}_K$, that is to say, $\rho + \bar{\rho}$ and $\rho\bar{\rho}$ lie in $\mathcal{O}_K$. Now

$$D = (\rho - \bar{\rho})^2 = (\rho + \bar{\rho})^2 - 4\rho\bar{\rho}$$

is the sum of a square and a multiple of 4 in $\mathcal{O}_K$. ■

Remark 6.4. One can write (18) in the suggestive form

$$\det[\kappa_h(\xi_i)]_{i,h} = \det \begin{bmatrix} \theta_1(1) & \theta_2(1) \\ \theta_1(\rho) & \theta_2(\rho) \end{bmatrix}$$

where θ_1, θ_2 are the two automorphisms of T_2. This equates discriminants of orders in L with those of orders in T_2. Equalities of determinants of this sort reappear in Bhargava's parametrizations of quartic and quintic rings and appear to be a common feature of many types of resolvent fields.

We can now state the notion of discriminant as we would like to use it.

Definition 6.5. A *discriminant* over $\mathcal{O}_K$ is an equivalence class of pairs $(\mathfrak{c}, D)$, with $D \in \mathfrak{c}^{-2}$ and $D \equiv t^2 \bmod 4\mathfrak{c}^2$ for some $t \in \mathfrak{c}^{-1}$, up to the equivalence relation

$$(\mathfrak{c}, D) \sim (\lambda\mathfrak{c}, \lambda^{-2}D).$$

If $\mathcal{O}$ is an étale order, the *discriminant* $\operatorname{Disc}\mathcal{O}$ is defined as follows: Pick any representation $\phi : \Lambda^n\mathcal{O} \to \mathfrak{c}$ of the Steinitz class as an ideal class; then $\operatorname{Disc}\mathcal{O}$ is the unique pair $(\mathfrak{c}, D)$ such that

$$\det[\operatorname{tr}\xi_i\eta_j]_{i,j=1}^n = D \cdot \phi(\xi_1 \wedge \cdots \wedge \xi_n) \cdot \phi(\eta_1 \wedge \cdots \wedge \eta_n).$$

Note the following points.

- The discriminant recovers the discriminant ideal via $\mathfrak{d} = D\mathfrak{c}^2$.
- If L has degree 3, the discriminant also contains the splitting information of L at the infinite primes. Namely, for each real place ι of K, if $\iota(D) > 0$ then $L_v \cong \mathbb{R} \times \mathbb{R} \times \mathbb{R}$, while if $\iota(D) < 0$ then $L_v \cong \mathbb{R} \times \mathbb{C}$.
- By a usual abuse of language, if L is an étale algebra over a number field K, its *discriminant* is the discriminant of the ring of integers $\mathcal{O}_L$ over $\mathcal{O}_K$.

- The discriminants over $\mathcal{O}_K$ form a cancellative semigroup under the multiplication law

$$(\mathfrak{c}_1, D_1)(\mathfrak{c}_2, D_2) = (\mathfrak{c}_1\mathfrak{c}_2, D_1 D_2).$$

- If $\mathcal{O}_K$ is a PID, then we can take $\mathfrak{c} = \mathcal{O}_K$, and then the discriminants are simply nonzero elements $D \in \mathcal{O}_K$ congruent to a square mod 4, up to multiplication by squares of units.

- We will often denote a discriminant by a single letter, such as $\mathcal{D}$. When elements or ideals of $\mathcal{O}_K$ appear in discriminants, they are to be understood as follows:

$$D \quad (D \in \mathcal{O}_K) \quad \text{means} \quad ((1), D) \tag{19}$$

$$\mathfrak{c}^2 \quad (\mathfrak{c} \subseteq K) \quad \text{means} \quad (\mathfrak{c}, 1). \tag{20}$$

  The seemingly counterintuitive convention (20) is motivated by the fact that, if $\mathfrak{c} = (c)$ is principal, then $(\mathfrak{c}, 1)$ is the same discriminant as $((1), c^2)$.

With these remarks in place, the reader should not have difficulty reading and proving the following relation:

Proposition 6.6. *If $\mathcal{O} \supseteq \mathcal{O}'$ are two orders in an étale algebra L, then*

$$\operatorname{Disc} \mathcal{O}' = [\mathcal{O} : \mathcal{O}']^2 \cdot \operatorname{Disc} \mathcal{O}.$$

6.3 Quadratic rings

We will spend a lot of time investigating the number of rings over $\mathcal{O}_K$ of given degree n and discriminant $\mathcal{D} = (\mathfrak{c}, D)$. For *quadratic* rings, the problem has a complete answer:

Proposition 6.7 (the parametrization of quadratic rings). *Let $\mathcal{O}_K$ be a Dedekind domain of characteristic not 2. For every discriminant $\mathcal{D}$, there is a unique quadratic étale order $\mathcal{O}_\mathcal{D}$ having discriminant $\mathcal{D}$.*

Proof. Note first that the theorem is true when $\mathcal{O}_K = K$ is a field: by Kummer theory, quadratic étale algebras over K are parametrized by $K^\times/(K^\times)^2$, as are discriminants; and it is a simple matter to check that $\operatorname{Disc} K[\sqrt{D}] = D$. We proceed to the general case.

For existence, let $\mathcal{D} = (\mathfrak{c}, D)$ be given. By definition, D is congruent to a square t^2 mod $4\mathfrak{c}^2$, $t \in \mathfrak{c}^{-1}$. Consider the lattice

$$\mathcal{O} = \mathcal{O}_K \oplus \mathfrak{c}\xi, \quad \xi = \frac{t + \sqrt{D}}{2} \in L = K[\sqrt{D}].$$

To prove that $\mathcal{O}$ is an order in L, it is enough to verify that $(c\xi)(d\xi) \in \mathcal{O}$ for any $c, d \in \mathfrak{c}$, and this follows from the computation

$$\xi^2 = \xi(t - \bar{\xi}) = t\xi - \left(\frac{t^2 - D}{4}\right)$$

and the conditions $t \in \mathfrak{c}^{-1}, t^2 - D \in 4\mathfrak{c}^{-2}$.

Now suppose that $\mathcal{O}_1$ and $\mathcal{O}_2$ are two orders with the same discriminant $\mathcal{D} = (\mathfrak{c}, D)$. Their enclosing K-algebras L_1, L_2 have the same discriminant D over K, and hence we can identify $L_1 = L_2 = L$. Now project each $\mathcal{O}_i$ along $\pi : L \to L/K$ is an $\mathcal{O}_K$-lattice $\mathfrak{c}_i$ in L/K, which is a one-dimensional K-vector space: indeed, we naturally have $L/K \cong \Lambda^2 L$, and upon computation, we find that $\operatorname{Disc} \mathcal{O}_i = (\mathfrak{c}_i, D)$. Consequently $\mathfrak{c}_1 = \mathfrak{c}_2 = \mathfrak{c}$. Now, for each $\beta \in \mathfrak{c}$, the fiber $\pi^{-1}(\mathfrak{c}) \cap \mathcal{O}_i$ is of the form $\beta_i + \mathcal{O}_K$ for some β_i. The element $\beta_1 - \beta_2$ is integral over $\mathcal{O}_K$ and lies in K, hence in $\mathcal{O}_K$. Thus $\mathcal{O}_1 = \mathcal{O}_2$. ∎

If $\mathcal{O}$ is any order in an étale algebra L/K ($\operatorname{char} K \neq 2$), the quadratic order $B = \mathcal{O}_{\operatorname{Disc} \mathcal{O}}$ having the same discriminant as $\mathcal{O}$ is called the *quadratic resolvent ring* of $\mathcal{O}$. It embeds into the discriminant torsor T_2, in two conjugate ways. Indeed, it is not hard to show that B is generated by the elements

$$\rho(\xi_1, \ldots, \xi_n) = \sum_{\pi \in A_n} \prod_i \kappa_{\pi(i)}(\xi_i) \in T_2$$

appearing in the proof of Lemma 6.2.

Remark 6.8. The notion of a quadratic resolvent ring extends to characteristic 2, being always an

order in the quadratic resolvent algebra constructed in Example 4.8. We omit the details.

6.4 Cubic rings

Cubic and quartic rings have parametrizations, known as *higher composition laws,* linking them to certain forms over $\mathcal{O}_K$ and also to ideals in resolvent rings. The study of higher composition laws was inaugurated by Bhargava in his celebrated series of papers ([2, 3, 4, 5]), although the gist of the parametrization of cubic rings goes back to work of F.W. Levi [32]. Later work by Deligne and by Wood [58, 60] has extended much of Bhargava's work from $\mathbb{Z}$ to an arbitrary base scheme. In a previous paper [42], the author explained how a representative sample of these higher composition laws extend to the case when the base ring A is a Dedekind domain. In the present work, we will need a few more; fortunately, there are no added difficulties, and we will briefly run through the statements and the methods of proof.

Theorem 6.9 (**the parametrization of cubic rings**). *Let A be a Dedekind domain with field of fractions K,* $\operatorname{char} A \neq 3$.

(*a*) *Cubic rings $\mathcal{O}$ over A, up to isomorphism, are in bijection with cubic maps*

$$\Phi : M \to \Lambda^2 M$$

between a two-dimensional A-lattice M and its own Steinitz class, up to isomorphism, in the obvious sense of a commutative square

$$\begin{array}{ccc} M_1 & \xrightarrow[i]{\sim} & M_2 \\ \downarrow{\scriptstyle \Phi_1} & & \downarrow{\scriptstyle \Phi_2} \\ \Lambda^2 M_1 & \xrightarrow[\det i]{\sim} & \Lambda^2 M_2. \end{array}$$

The bijection sends a ring $\mathcal{O}$ to the index form $\Phi : \mathcal{O}/A \to \Lambda^2(\mathcal{O}/A)$ given by

$$x \mapsto x \wedge x^2.$$

(*b*) *If $\mathcal{O}$ is nondegenerate, that is, the corresponding cubic K-algebra $L = K \otimes_A \mathcal{O}$ is étale, then the map Φ is the restriction, under the Minkowski embedding, of the index form of $\bar{K}^3$, which is*

$$\begin{aligned} \Phi : \bar{K}^3/\bar{K} &\to \bar{K}^2/\bar{K} \\ (x;y;z) &\mapsto \big((x-y)(y-z)(z-x), 0\big). \end{aligned} \tag{21}$$

(*c*) *Conversely, let L be a cubic étale algebra over K. If $\bar{\mathcal{O}} \subseteq L/K$ is a lattice such that Φ sends $\bar{\mathcal{O}}$ into $\Lambda^2\bar{\mathcal{O}}$, then there is a unique cubic ring $\mathcal{O} \subseteq L$ such that, under the natural identifications, $\mathcal{O}/A = \bar{\mathcal{O}}$.*

Proof. (a) The proof is quite elementary, involving merely solving for the coefficients of the unknown multiplication table of $\mathcal{O}$. The case where A is a PID is due to Gross ([24], Section 2): the cubic ring having index form

$$f(x\xi + y\eta) = ax^3 + bx^2y + cxy^2 + dy^3$$

has multiplication table

$$\xi\eta = -ad, \xi^2 = -ac + b\xi - a\eta, \eta^2 = -bd + d\xi - c\eta. \tag{22}$$

For the general Dedekind case, see my [42], Theorem 7.1. It is also subsumed by Deligne's work over an arbitrary base scheme; see Wood [58] and the references therein.

(b) This follows from the fact that the index form respects base change. The index form of $\bar{K}^3/\bar{K}$ is a Vandermonde determinant that can easily be written in the stated form.

(c) We have an integral cubic map $\Phi\big|_{\bar{\mathcal{O}}} : \bar{\mathcal{O}} \to \Lambda^2\bar{\mathcal{O}}$, which is the index form $\Phi_{\mathcal{O}}$ of a unique cubic ring $\mathcal{O}$ over $\mathcal{O}_K$. But over K, $\Phi_{\mathcal{O}}$ is isomorphic to the index form of L. Since L (as a cubic ring over K) is determined by its index form, we obtain an identification $\mathcal{O} \otimes_{\mathcal{O}_K} K \cong L$ for which $\mathcal{O}/A$, the projection of $\mathcal{O}$ onto L/K, coincides with $\bar{\mathcal{O}}$. The uniqueness of $\mathcal{O}$ is obvious, as $\mathcal{O}$ must lie in the integral closure $\mathcal{O}_L$ of K in L.

■

In this paper we only deal with nondegenerate rings, that is, those of nonzero discriminant, or equivalently, those that lie in an étale K-algebra. Consequently, all index forms Φ that we will see are restrictions of (21). When cubic algebras are parametrized Kummer-theoretically, the resolvent map becomes very explicit and simple:

Proposition 6.10 (**explicit Kummer theory for cubic algebras**). *Let R be a quadratic étale algebra over K (*$\operatorname{char} K \neq 3$*), and let*

$$L = K + \kappa(R)$$

be the cubic algebra of resolvent $R' = R \odot K[\mu_3]$ (the Tate dual of R) corresponding to an element $\delta \in K^\times$ of norm 1 in Theorem 5.4(b), where

$$\kappa(\xi) = \left(\operatorname{tr}_{\bar{K}^2/K} \xi\omega\sqrt[3]{\delta}\right)_{\omega\in\left(\bar{K}^2\right)^{N=1}[3]} \in \bar{K}^3$$

so κ maps R bijectively onto the traceless plane in L. Then the index form of L is given explicitly by

$$\begin{aligned} \Phi : L/K &\to \Lambda^2(L/K) \\ \kappa(\xi) &\mapsto 3\sqrt{-3}\delta\xi^3 \wedge 1, \end{aligned} \tag{23}$$

where we identify

$$\Lambda^2 L/K \cong \Lambda^3 L \cong \Lambda^2 R' \cong R'/K \cong \sqrt{-3}\cdot R/K$$

using the fact that R' is the discriminant resolvent of L.

Proof. Direct calculation, after reducing to the case $K = \bar{K}$. ■

Theorem 6.11 (**self-balanced ideals in the cubic case**). *Let $\mathcal{O}_K$ be a Dedekind domain,* $\operatorname{char} K \neq 3$*, and let R be a quadratic étale extension. A* self-balanced triple *in R is a triple (B, I, δ) consisting of a quadratic order $B \subseteq R$, a fractional ideal I of B, and a scalar $\delta \in (KB)^\times$ satisfying the conditions*

$$\delta I^3 \subseteq B, \quad N(I) = (t) \text{ is principal}, \quad \text{and} \quad N(\delta)t^3 = 1, \tag{24}$$

(*a*) *Fix B and $\delta \in R^\times$ with $N(\delta)$ a cube t^{-3}. Then the mapping*

$$I \mapsto \mathcal{O} = \mathcal{O}_K + \kappa(I) \tag{25}$$

defines a bijection between

- *self-balanced triples of the form (B, I, δ), and*
- *subrings $\mathcal{O} \subseteq L$ of the cubic algebra $L = K + \kappa(R)$ corresponding to the Kummer element δ, such that $\mathcal{O}$ is* 3-traced, *that is,* $\mathrm{tr}(\xi) \in 3\mathcal{O}_K$ *for every $\xi \in L$.*

(*b*) *Under this bijection, we have the discriminant relation*

$$\operatorname{disc} C = -27 \operatorname{disc} B. \tag{26}$$

Proof. The mapping κ defines a bijection between lattices $I \subseteq R$ and $\kappa(I) \subseteq L/K$. The difficult part is showing that I fits into a self-balanced triple (B, I, δ) if and only if $\kappa(I)$ is the projection of a 3-traced order $\mathcal{O}$. Note that if (B, I, δ) exists, it is unique, as the requirement $[B : I] = (t)$ pins down B.

Rather than establish this equivalence directly, we will show that both conditions are equivalent to the symmetric trilinear form

$$\beta : I \times I \times I \to \Lambda^2 R$$

$$(\alpha_1, \alpha_2, \alpha_3) \to \delta \alpha_1 \alpha_2 \alpha_3$$

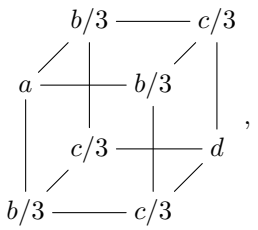
taking values in $t^{-1} \cdot \Lambda^2 I$.

In the case of self-balanced ideals, this was done over $\mathbb{Z}$ by Bhargava [2, Theorem 3]. Over a Dedekind domain, it follows from the parametrization of *balanced* triples of ideals over B [42, Theorem 5.3], after specializing to the case that all three ideals are identified with one ideal I. It also follows from the corresponding results over an arbitrary base in Wood [60, Theorem 1.4].

In the case of rings, we compute by Proposition 6.10 that β is the trilinear form attached to the index form of $\kappa(I)$. By Theorem 6.9(c), the diagonal restriction $\beta(\alpha,\alpha,\alpha)$ takes values in $t^{-1}\Lambda^2(I)$ if and only if $\kappa(I)$ lifts to a ring $\mathcal{O}$. We wish to prove that β itself takes values in $t^{-1}\Lambda^2(I)$ if and only if $\mathcal{O}$ is 3-traced. Note that both conditions are local at the primes dividing 2 and 3, so we may assume that $\mathcal{O}_K$ is a DVR. With respect to a basis (ξ,η) of I and a generator of $t^{-1}\Lambda^2(I)$, the index form of $\mathcal{O}$ has the form

$$f(x,y) = ax^3 + bx^2y + cxy^2 + dy^3, \quad a,\ldots,d \in \mathcal{O}_K.$$

If this is the diagonal restriction of β, then β itself can be represented as a 3-dimensional matrix



,

which is integral exactly when $b,c \in 3\mathcal{O}_K$. Since the trace ideal of $\mathcal{O}$ is generated by

$$\mathrm{tr}(1) = 3, \quad \mathrm{tr}(\xi) = -b, \quad \mathrm{tr}(\eta) = c$$

(by reference to the multiplication table (22)), this is also the condition for $\mathcal{O}$ to be 3-traced, establishing the equivalence.

The discriminant relation (26) follows easily from the definition of κ. ■

6.5 Quartic rings and their cubic resolvent rings

The basic method for parametrizing quartic orders is by means of *cubic resolvent rings,* introduced by Bhargava in [4] and developed by Wood in [58] and the author in [42].

Definition 6.12 ([42], Definition 8.1; also a special case of [58], p. 1069)**.** Let A be a Dedekind domain, and let $\mathcal{O}$ be a quartic algebra over A. A *resolvent* for $\mathcal{O}$ ("numerical resolvent" in [42])

consists of a rank-2 A-lattice Y, an A-module isomorphism $\Theta : \Lambda^2 Y \to \Lambda^3(\mathcal{O}/A)$, and a quadratic map $\Phi : \mathcal{O}/A \to Y$ such that there is an identity of biquadratic maps

$$x \wedge y \wedge xy = \Theta(\Phi(x) \wedge \Phi(y)) \tag{27}$$

from $\mathcal{O} \times \mathcal{O}$ to $\Lambda^3(\mathcal{O}/A)$.

We collect some basic facts about these resolvents.

Theorem 6.13 (**the parametrization of quartic rings**). *The notion of resolvent for quartic rings has the following properties.*

(*a*) *If X is a rank-3 A-lattice and $\Theta : \Lambda^2 Y \to \Lambda^3 X$, $\Phi : X \to Y$ satisfy* (27)*, then there is a unique (up to isomorphism) quartic ring $\mathcal{O}$ equipped with an identification $\mathcal{O}/A \cong X$ making $(\mathcal{O}, Y, \Theta, \Phi)$ a resolvent.*

(*b*) *There is a canonical (in particular, base-change-respecting) way to associate to a resolvent $(\mathcal{O}, Y, \Theta, \Phi)$ a cubic ring C and an identification $C/A \cong X$ with the following property: For any element $x \in \mathcal{O}$ and any lift $y \in C$ of the element $\Phi(x) \in C/A$, we have the equality*

$$x \wedge x^2 \wedge x^3 = \Theta(y \wedge y^2).$$

It satisfies

$$\operatorname{Disc} C = \operatorname{Disc} \mathcal{O}.$$

(Here the discriminants are to be seen as quadratic resolvent rings, as in [42]; this implies the corresponding identity of discriminant ideals.) If $\mathcal{O}$ is nondegenerate, then C is unique.

(*c*) *Any quartic ring $\mathcal{O}$ has at least one resolvent.*

(*d*) *If $\mathcal{O}$ is maximal, the resolvent is unique (but need not be maximal).*

(*e*) *The number of resolvents of $\mathcal{O}$ is the sum of the absolute norms of the divisors of the* content *of $\mathcal{O}$, the smallest ideal $\mathfrak{c}$ such that $\mathcal{O} = \mathcal{O}_K + \mathfrak{c}\mathcal{O}'$ for some order $\mathcal{O}'$.*

(*f*) *Let* (Y, Θ, Φ) *be a resolvent of* $\mathcal{O}$ *with associated cubic ring* C*, and let* $K = \operatorname{Frac} A$*. If the corresponding quartic* K*-algebra* $L = K \otimes_A \mathcal{O}$ *is étale, then the cubic* K*-algebra* $R = C \otimes_A \mathcal{O}$ *is none other than the cubic resolvent of* L*, as defined in Example 4.7. The maps* Θ *and* Φ *are the restrictions, under the Minkowski embedding, of the unique resolvent of* $\bar{K}^4$*, which is* $\bar{K}^3$ *with the maps*

$$\begin{aligned} \Theta : \Lambda^2(\bar{K}^3/\bar{K}) &\to \Lambda^3(\bar{K}^4/\bar{K}) \\ (0;1;0) \wedge (0;0;1) &\mapsto (0;1;0;0) \wedge (0;0;1;0) \wedge (0;0;0;1) \end{aligned} \tag{28}$$

and

$$\begin{aligned} \Phi : \bar{K}^4/\bar{K} &\to \bar{K}^3/\bar{K} \\ (x;y;z;w) &\mapsto (xy + zw; xz + yw; xw + yz). \end{aligned} \tag{29}$$

(*g*) *Conversely, let* L *be a quartic étale algebra over* K *and* R *its cubic resolvent. Let*

$$\Theta_K : \Lambda^2 R/K \to \Lambda^3 L/K, \quad \Phi_K : L/K \to R/K$$

be the resolvent data of L *as a (maximal) quartic ring over* K*. Suppose* $\bar{\mathcal{O}} \subseteq L/K$*,* $\bar{C} \subseteq R/K$ *are lattices such that*

- Φ_K *sends* $\bar{\mathcal{O}}$ *into* $\bar{C}$*,*
- Θ_K *maps* $\Lambda^3\bar{\mathcal{O}}$ *isomorphically onto* $\Lambda^2\bar{C}$*.*

Then there are unique quartic rings $\mathcal{O} \subseteq L$*,* $C \subseteq R$ *such that, under the natural identifications,* $\mathcal{O}/A = \bar{\mathcal{O}}$*,* $C/A = \bar{C}$*, and* $\bar{C}$ *is a resolvent with the restrictions of* Θ_K *and* Φ_K*.*

Proof. (a) See [42], Theorem 8.3.

(b) See [42], Theorems 8.7 and 8.8.

(c) See [42], Corollary 8.6.

(d) This is a special case of the following part.

(e) See [42], Corollary 8.5.

(f) By base-changing to K, we see that $Y \otimes_A K = R/K$ is a resolvent for L. Since the resolvent is unique, it suffices to show that the cubic resolvent R' from Example 4.7 is a resolvent for L also. The maps Θ and Φ defined in the theorem statement are seen, by symmetry, to restrict to maps of the appropriate K-modules. The verification of (27) and of the fact that the multiplicative structure on R' is the right one can be checked at the level of $\bar{K}$-algebras.

(g) Letting $X = \bar{\mathcal{O}}$, $Y = \bar{C}$ in part (a), we construct the desired $\mathcal{O}$ and C. By comparison to the situation under base-change to K, we see that $\mathcal{O}$, C naturally inject into L, R respectively. Uniqueness is obvious, as $\mathcal{O}$ must lie in the integral closure $\mathcal{O}_L$.

■

In this paper we only deal with nondegenerate rings, that is, those of nonzero discriminant, or equivalently, those that lie in an étale K-algebra. Consequently, all resolvent maps Θ, Φ that we will see are restrictions of (28) and (29). When quartic algebras are parametrized Kummer-theoretically, the resolvent map becomes very explicit and simple:

Proposition 6.14 (**explicit Kummer theory for quartic algebras**). *Let R be a cubic étale algebra over K ($\operatorname{char} K \neq 2$), and let*

$$L = K + \kappa(R)$$

be the quartic algebra of resolvent R corresponding to an element $\delta \in K^\times$ of norm 1 in Theorem 5.4(c), where

$$\kappa(\xi) = \left(\operatorname{tr}_{\bar{K}^3/K} \xi\omega\sqrt{\delta}\right)_{\omega \in \left(\bar{K}^3\right)^{N=1}[2]} \in \bar{K}^4$$

so κ maps R bijectively onto the traceless hyperplane in L. Then the resolvent of L is given explicitly by

$$\begin{aligned} \Theta : \Lambda^3(R) &\to \Lambda^3(L/K) \\ \alpha \wedge \beta \wedge \gamma &\mapsto \frac{1}{16\sqrt{N(\delta)}} \cdot \kappa(\alpha) \wedge \kappa(\beta) \wedge \kappa(\gamma) \end{aligned} \tag{30}$$

$$\begin{aligned} \Phi : L/K &\to R/K \\ \kappa(\xi) &\mapsto 4\delta\xi^2 \end{aligned} \tag{31}$$

Proof. Since the resolvent is unique (over a field, any étale extension has content 1), it suffices to prove that (30) and (31) define a resolvent. This can be done after extension to $\bar{K}$, and then it is enough to prove that (30) and (31) agree with the standard resolvent on $\bar{K}^4$, given in Theorem 6.13(f).

As to (30), since both sides are alternating in α, β, and γ, it suffices to prove it in the case that

$$\alpha = (1;0;0), \quad \beta = (0;1;0) \quad \gamma = (0;0;1)$$

form the standard basis of $R = \bar{K}^3$. Let $\delta = (\delta^{(1)}, \delta^{(2)}, \delta^{(3)})$. Then

$$\begin{aligned}
\kappa(\alpha) &= \left(\sqrt{\delta^{(1)}}, \sqrt{\delta^{(1)}}, -\sqrt{\delta^{(1)}}, -\sqrt{\delta^{(1)}}\right) \\
\kappa(\beta) &= \left(\sqrt{\delta^{(2)}}, -\sqrt{\delta^{(2)}}, \sqrt{\delta^{(2)}}, -\sqrt{\delta^{(2)}}\right) \\
\kappa(\gamma) &= \left(\sqrt{\delta^{(3)}}, -\sqrt{\delta^{(3)}}, -\sqrt{\delta^{(3)}}, \sqrt{\delta^{(3)}}\right)
\end{aligned}$$

and hence the wedge product of these differs from the standard generator of $\Lambda^3(L/K)$ by a factor of

$$\begin{aligned}
&\begin{vmatrix}
1 & 1 & 1 & 1 \\
\sqrt{\delta^{(1)}} & \sqrt{\delta^{(1)}} & -\sqrt{\delta^{(1)}} & -\sqrt{\delta^{(1)}} \\
\sqrt{\delta^{(2)}} & -\sqrt{\delta^{(2)}} & \sqrt{\delta^{(2)}} & -\sqrt{\delta^{(2)}} \\
\sqrt{\delta^{(3)}} & -\sqrt{\delta^{(3)}} & -\sqrt{\delta^{(3)}} & \sqrt{\delta^{(3)}}
\end{vmatrix} \\
&= \sqrt{N(\delta)} \begin{vmatrix}
1 & 1 & 1 & 1 \\
1 & 1 & -1 & -1 \\
1 & -1 & 1 & -1 \\
1 & -1 & -1 & 1
\end{vmatrix} \\
&= 16 \cdot \sqrt{N(\delta)}.
\end{aligned}$$

The calculation for (31) is even more routine. ∎

Remark 6.15. The datum Θ of a resolvent carries no information, in the following sense. It is unique up to scaling by $c \in A^\times$, and the resolvent data (X, Y, Θ, Φ) and $(X, Y, c\Theta, \Phi)$ are isomorphic under multiplication by c^{-1} on X and by c^{-2} on Y. If A is a PID, indeed, neither X nor Y carries any information, and the entire data of the resolvent is encapsulated in Φ, a pair of 3×3 symmetric matrices over A (with formal factors of $1/2$ off the diagonal) defined up to the natural action of $\mathrm{GL}_3 A \times \mathrm{GL}_2 A$. This establishes the close kinship with Bhargava's parametrization of quartic rings in [4]. However, it is useful to keep Θ around.

6.5.1 Traced resolvents

Just as we found it natural to study not just binary cubic 1111-forms, but also 1331-forms and their analogue for each divisor of the ideal (3), so too we study not just quartic rings in general but those satisfying a natural condition at the primes dividing 2.

Definition 6.16. Let A be a Dedekind domain, $\mathrm{char}\, A \neq 2$, and let $\mathfrak{t}$ be an ideal dividing (2) in A. A resolvent $(\mathcal{O}, Y, \Theta, \Phi)$ over A is called $\mathfrak{t}$-*traced* if, for all x and y in A, the associated bilinear form

$$\Phi(x, y) = \frac{\Phi(x + y) - \Phi(x) - \Phi(y)}{2}$$

whose diagonal restriction is $\Phi(x, x) = \Phi(x)$ takes values in $2^{-1}\mathfrak{t}Y$. If A is a PID, this is equivalent to saying that the off-diagonal entries in the matrix representation of Φ, which a priori live in $\frac{1}{2}A$, actually belong to $\frac{\mathfrak{t}}{2}A$. We say that A is $\mathfrak{t}$-*traced* if it admits a $\mathfrak{t}$-traced resolvent.

Here are some facts about traced resolvents:

Proposition 6.17. *Let $\mathcal{O}$ be a quartic ring over a Dedekind domain $\mathcal{O}_K$.*

(*a*) *$\mathcal{O}$ is $\mathfrak{t}$-traced if and only if*

  (*i*) $\mathfrak{t}^2 | \operatorname{tr} x$ *for all* $x \in \mathcal{O}$;

  (*ii*) $x^2 \in A + \mathfrak{t}\mathcal{O}$ *for all* $x \in \mathcal{O}$.

(*b*) *If $\mathcal{O}$ is not an order in the* trivial algebra $K[\varepsilon_1, \varepsilon_2, \varepsilon_3]/(\varepsilon_i \varepsilon_j)_{i,j=1}^3$, *the number of $\mathfrak{t}$-traced*

resolvents of $\mathcal{O}$ is the sum of the absolute norms of the divisors of its $\mathfrak{t}$-traced content, *which is the smallest ideal* $\mathfrak{c}$ *such that* $\mathcal{O} = A + \mathfrak{c}\mathcal{O}'$ *and* $\mathcal{O}'$ *is also* $\mathfrak{t}$*-traced.*

(*c*) *If* $(\mathcal{O}, Y, \Theta, \Phi)$ *is a* $\mathfrak{t}$*-traced resolvent with associated cubic ring* C*, then* $\mathfrak{t}^2 | \operatorname{ct}(C)$*, that is,* $C = A + \mathfrak{t}^2 C'$ *for some cubic ring* C'*. We call* C' *a "reduced resolvent" of the* $\mathfrak{t}$*-traced ring* A*. Also,* $\mathfrak{t}^8 | \operatorname{disc} A$.

Proof. (*a*) Since both statements are local at the primes dividing 2, we can assume that $\mathcal{O}_K$ is a DVR, and thus that $\mathfrak{t} = (t)$ is principal. With respect to bases $(1 = \xi_0, \xi_1, \xi_2, \xi_3)$ for $\mathcal{O}$ and $(1 = \eta_0, \eta_1, \eta_2)$ for a resolvent C, the structure constants c_{ij}^k of the ring $\mathcal{O}$, defined by

$$\xi_i \xi_j = \sum_k c_{ij}^k \xi_k,$$

are determined by the entries of the resolvent

$$\Phi = ([a_{ij}], [b_{ij}])$$

via the determinants

$$\lambda_{k\ell}^{ij} = 2^{\mathbf{1}_{i \neq j} + \mathbf{1}_{k \neq \ell}} \begin{vmatrix} a_{ij} & a_{k\ell} \\ b_{ij} & b_{k\ell} \end{vmatrix}$$

and a set of formulas appearing in Bhargava [4, equation (21)] and over a Dedekind domain by the author [42, equation (12)]:

$$\begin{aligned} c_{ii}^j &= -\varepsilon \lambda_{ik}^{ii} \\ c_{ij}^k &= \varepsilon \lambda_{ii}^{jj} \\ c_{ij}^j - c_{ik}^k &= \varepsilon \lambda_{ii}^{jk} \\ c_{ii}^i - c_{ij}^j - c_{ik}^k &= \varepsilon \lambda_{ik}^{ij}, \end{aligned} \tag{32}$$

where (i, j, k) denotes any permutation of $(1, 2, 3)$ and $\varepsilon = \pm 1$ its sign. (Here the nonappearance of some of the individual c_{ij}^k on the left-hand side of (32) stems from the ambiguity of

translating each ξ_i by $\mathcal{O}_K$, which does not change the matrix of Φ.)

Assume first that $\Phi : \mathcal{O}/\mathcal{O}_K \to C/\mathcal{O}_K$ is $\mathfrak{t}$-traced. Then

$$\lambda_{k\ell}^{ij} \in \mathfrak{t}^{\mathbf{1}_{i\neq j}+\mathbf{1}_{k\neq \ell}}. \tag{33}$$

We then prove that the conditions (i) and (ii) must hold:

(i) The trace

$$\begin{aligned} \operatorname{tr}(\xi_1) &= c_{11}^1 + c_{12}^2 + c_{13}^3 \\ &= \lambda_{13}^{12} + 2\lambda_{11}^{23} + 4c_{13}^3 \\ &\equiv 0 \mod \mathfrak{t}^2, \end{aligned}$$

and likewise $\operatorname{tr}(\xi_2), \operatorname{tr}(\xi_3) \in \mathfrak{t}^2$.

(ii) The coefficients c_{11}^i of ${\xi_1}^2$ satisfy:

$$c_{11}^2 = \lambda_{13}^{11} \in \mathfrak{t}$$

and likewise for c_{11}^3; and then $c_{11}^1 \in \mathfrak{t}$ also, since the trace $c_{11}^1 + c_{12}^2 + c_{13}^3 = \operatorname{tr}(\xi_1) \in \mathfrak{t}^2 \subseteq \mathfrak{t}$. So the desired relation $\xi^2 \in \mathcal{O}_K + \mathfrak{t}\mathcal{O}$ holds when $\xi = \xi_1$, indeed $\xi = a_1\xi_1$ for any $a_1 \in \mathcal{O}_K$. The same proof works for $\xi = a_2\xi_2$ or $\xi = a_3\xi_3$. Since the case $\xi = a_0 \in \mathcal{O}_K$ is trivial and squaring is a $\mathbb{Z}$-linear operation modulo 2, we get the result for all $\xi \in \mathcal{O}$.

Conversely, suppose that (i) and (ii) hold. We first establish (33). We have

- $\lambda_{13}^{11} = c_{11}^2 \in \mathfrak{t}$
- $\lambda_{11}^{23} = c_{12}^2 - c_{13}^3 = \operatorname{tr}\xi_1 - c_{11}^1 - 2c_{13}^3 \in \mathfrak{t}$
- $\lambda_{13}^{12} = c_{11}^1 - c_{12}^2 - c_{13}^3 = \operatorname{tr}\xi_1 - 2\lambda_{11}^{23} + 4c_{13}^3 \in \mathfrak{t}^2$.

Permuting the indices as needed, this accounts for all the $\lambda_{k\ell}^{ij}$ about which (33) makes a nontrivial assertion.

Now we work from the $\lambda_{k\ell}^{ij}$ back to the resolvent $(\mathcal{A}, \mathcal{B})$. We may assume that C is nontrivial (the trivial rings, one for each Steinitz class, are plainly 2-traced with $(\mathcal{A}, \mathcal{B}) = (0, 0)$.) Then, in the proof of [42], Theorem 8.4, the author established that there are vectors μ_{ij} in a two-dimensional vector space V over K, unique up to $\mathrm{GL}_2(V)$, such that

$$\mu_{ij} \wedge \mu_{k\ell} = \lambda_{k\ell}^{ij} \cdot \omega$$

for some fixed generator $\omega \in \Lambda^2 V$. (The proof uses the *Plücker relations*, which are a consequence of the associative law on $\mathcal{O}$.) This V is none other than R/K, the resolvent module of the quartic algebra $L = \mathcal{O} \otimes_{\mathcal{O}_K} K$, which admits the unique resolvent

$$\begin{aligned} \Phi(a_1\xi_1 + a_2\xi_2 + a_3\xi_3) &= \sum_{i<j} a_i a_j \mu_{ij} \\ \Theta(\xi_1 \wedge \xi_2 \wedge \xi_3) &= \omega. \end{aligned} \tag{34}$$

The resolvents of $\mathcal{O}$ were found to be exactly the lattices M containing the span M_0 of the six μ_{ij}, with the correct index

$$[M : M_0] = \mathfrak{c} = \left(\lambda_{k\ell}^{ij}\right)_{i,j,k,\ell} = \left(c_{ii}^j, c_{ij}^k, c_{ij}^j - c_{ik}^k, c_{ii}^i - c_{ij}^j - c_{ik}^k : i \neq j \neq k \neq i\right),$$

the content ideal of $\mathcal{O}$. By inspection of (34) that M is $\mathfrak{t}$-traced if and only if it actually contains the span $\tilde{M}_0$ of the six vectors

$$\tilde{\mu}_{ij} = t^{-\mathbf{1}_{i \neq j}} \mu_{ij}.$$

Condition (33) is interpreted as saying that the $\tilde{\mu}_{ij} \wedge \tilde{\mu}_{k\ell}$ are still integer multiples of ω. Then the $\mathfrak{t}$-traced resolvents are the lattices $M \supseteq \tilde{M}_0$. The needed index

$$\tilde{\mathfrak{c}} = [M : \tilde{M}_0] = \left(\tilde{\lambda}_{k\ell}^{ij}\right)_{i,j,k,\ell}$$

is an integral ideal, so such M exists, finishing the proof of (a).

(b) It suffices to prove that $\tilde{\mathfrak{c}}$ is the $\mathfrak{t}$-traced content of $\mathcal{O}$. To see this, note that if $\mathcal{O} = \mathcal{O}_K + a\mathcal{O}'$ has content divisible by a, then the structure coefficients c_{ij}^k of $\mathcal{O}'$ are obtained from those of $\mathcal{O}$ by dividing by a. This means that the $\lambda_{k\ell}^{ij}$ and $\tilde{\lambda}_{k\ell}^{ij}$ are divided by a, and so remain integral (indicating that $\mathcal{O}'$ is also $\mathfrak{t}$-traced) exactly when $a \mid \tilde{\mathfrak{c}}$.

(c) We can again reduce to the case that $\mathcal{O}_K$ is a DVR so $\mathcal{O}$ has an $\mathcal{O}_K$-basis. Recall that the index form of the resolvent C is given by

$$f(x, y) = 4 \det(\mathcal{A}x + \mathcal{B}y)$$

([4], Proposition 11; [42], Theorem 8.7). If $\mathcal{A}$ and $\mathcal{B}$ have off-diagonal entries in $2^{-1}\mathfrak{t}$, it immediately follows that f is divisible by t^2, so $t^2 \mid \operatorname{ct}(C)$. Consequently $\operatorname{disc} \mathcal{O} = \operatorname{disc} C$, being quartic in the coefficients of f, is divisible by t^8. ■

Similar to Theorem 6.11, we have the following relation between 2-traced quartic rings and self-balanced ideals:

Theorem 6.18 (**self-balanced ideals in the quartic setting**). *Let $\mathcal{O}_K$ be a Dedekind domain,* $\operatorname{char} K \neq 2$*, and let R be a cubic étale extension. A* self-balanced triple *in R is a triple (C, I, δ) consisting of a cubic order $C \subseteq R$, a fractional ideal I of C, and a scalar $\delta \in (KC)^\times$ satisfying the conditions*

$$\delta I^2 \subseteq C, \quad N(I) = (t) \text{ is principal}, \quad \text{and} \quad N(\delta)t^2 = 1, \tag{35}$$

Fix an order $C \subseteq R$ and a scalar $\delta \in R^\times$ with $N(\delta)$ a square t^{-2}. Then the mapping

$$I \mapsto \mathcal{O} = \mathcal{O}_K + \kappa(I) \tag{36}$$

defines a bijection between

- *self-balanced triples of the form (C, I, δ), and*

- *subrings $\mathcal{O} \subseteq L$ of the quartic algebra $L = K + \kappa(R)$ corresponding to the Kummer element δ, such that $\mathcal{O}$ is 2-traced with reduced resolvent C.*

Proof. The proof is very similar to that of 6.11, so we simply summarize the main points. The linear isomorphism κ establishes a bijection between lattices $I \subseteq R$ and $\kappa(I) \subseteq L/K$. We wish to prove that (C, I, δ) is balanced if and only if $\kappa(I)$ is the projection of a 2-traced order with reduced resolvent C.

First note that either of these conditions uniquely specifies

$$[C : I] = (t),$$

the former by the balancing condition $N(I) = (t)$, and the latter by the Θ-condition that $\mathcal{O}$ have discriminant $256 \operatorname{disc} C$.

Once again, it is difficult to proceed directly, and we instead prove that both conditions are equivalent to the bilinear map

$$\Phi : I \times I \to R/K$$

$$(\alpha_1, \alpha_2) \to 4\delta\alpha_1\alpha_2$$

taking values in $4C/K$. ■

On the self-balanced ideals side, this follows from the parametrization of *balanced* pairs of ideals by $2 \times 3 \times 3$ boxes performed over $\mathbb{Z}$ by Bhargava [3, Theorem 2] and over a general base by Wood [60, Theorem 1.4].

On the quartic rings side, the diagonal restriction of Φ is precisely the resolvent of $\kappa(I)$, by Proposition 6.14. That $\Phi(\alpha, \alpha) \in 4C/K$ for each $\alpha \in I$ expresses the one condition remaining for $\kappa(I)$ to lift (by Theorem 6.13(g)) to a quartic ring $\mathcal{O}$ with resolvent $\mathcal{O}_K + 4C$. Then, by definition, this resolvent is 2-traced exactly when Φ itself has image in $4C/K$.

7 Cohomology of cyclic modules over a local field

Let M be a Galois module with underlying group $\mathcal{C}_p$ over a local field $K \supseteq \mathbb{Q}_p$ (that is, a *wild* local field of characteristic 0). Denote by T and T', respectively, the $(\mathbb{Z}/p\mathbb{Z})^\times$-torsors corresponding to the action of G_K on $M\backslash\{0\}$ and on

$$\mathrm{Surj}(M, \mu_p) = M' \setminus \{0\},$$

and denote by $\tau_c : T' \to T'$ the torsor operation corresponding to $c \in (\mathbb{Z}/p\mathbb{Z})^\times \cong \mathrm{Aut}\, M$. By Theorem 5.4, Kummer theory gives an isomorphism

$$H^1(K, M) \cong \left\{\alpha \in T'^\times/(T'^\times)^p : \tau_c(\alpha) = \alpha^c \,\forall c \in (\mathbb{Z}/p\mathbb{Z})^\times\right\}. \tag{37}$$

Our objective in this section is to understand the group on the right: that is, to describe a basis of it (a generalization of the well-known Shafarevich basis for $T'^\times$) and understand how the Tate pairing respects it. Much of our work parallels that of Del Corso and Dvornicich [13] and Nguyen-Quang-Do [41].

If $\sigma \in H^1(K, M)$, we let $L = L_\sigma$ be the $\mathcal{GA}(\mathcal{C}_p)$-extension of degree p coming from the affine action of G_K on M, while we let $E = E_\sigma$ be the associated $\mathcal{GA}(\mathcal{C}_p)$-torsor. Owing to the semidirect product structure of $\mathcal{GA}(\mathcal{C}_p)$, we get a natural decomposition

$$E \cong L \otimes_K T.$$

Using the division algorithm in $\mathbb{Z}$, we let $\ell = \ell(L) = \ell(\sigma)$ and $\theta = \theta(L) = \theta(\sigma)$ the integers such that

$$v_K(\mathrm{disc}\, L) = p(e - \ell) + \theta, \quad -1 \le \theta \le p - 2.$$

We call ℓ the *level*, and θ the *offset*, of the $\mathcal{GA}(\mathcal{C}_p)$-extension L or of the coclass σ. Although these definitions appear strange, they allow us to state concisely the following theorem, which will be the

main theorem of this section.

Theorem 7.1 (**levels and offsets**). *Let M be a Galois module with underlying group $\mathcal{C}_p$ over a local field K with* $\operatorname{char} K \neq p$.

(*a*) *The level ℓ of a coclass determines its offset θ uniquely in the following way:*

(*i*) *If $\ell = e$, then $\theta = v_K(\operatorname{disc} T)$.*

(*ii*) *If $0 \leq \ell < e$, then $\theta \geq 0$ and*

$$\theta \equiv \ell - v_K(\beta) \mod p - 1,$$

where β is the Kummer element corresponding to the resolvent μ_{p-1}-torsor of M.

(*iii*) *If $\ell = -1$, then $\theta = -1$.*

(*b*) *For all $i \geq 0$, the* level space

$$\mathcal{L}_i = \mathcal{L}_i(M) = \{\sigma \in H^1(K, M) : \ell(\sigma) \geq i\}$$

consisting of coclasses of level at least i is a subgroup of $H^1(K, M)$.

(*c*) $\mathcal{L}_e = H^1_{\mathrm{ur}}(K, M)$.

(*d*) *For $0 \leq i \leq e$,*

$$|\mathcal{L}_i| = q^{e-i}|H^0(K, M)|.$$

(*e*) *$\mathcal{L}_{-1}$ is the whole of $H^1(K, M)$, and*

$$|H^1(K, M)| = q^e|H^0(K, M)| \cdot |H^0(K, M')|.$$

(*f*) *For $d \leq 1$, a neighborhood*

$$\big\{[\alpha] \in H^1(K, M) : \alpha \in T'^{\times}, |\alpha - 1| \leq d\big\}$$

is a level space $\mathcal{L}_i$ whose index i is given by

$$i = \begin{cases} \left\lceil \dfrac{v_K(\beta)}{p} + \dfrac{p-1}{p}\left\lceil \dfrac{\log d}{\log|\pi_K|} - 1 - \dfrac{v_K(\beta)}{p-1}\right\rceil\right\rceil, & d \geq d_{\min} \\ e+1, & d < d_{\min}, \end{cases}$$

where

$$d_{\min} = |p|^{p/(p-1)}.$$

(g) *For $0 \leq i \leq e$, with respect to the Tate pairing between $H^1(K,M)$ and $H^1(K,M')$,*

$$\mathcal{L}_i(M)^\perp = \mathcal{L}_{e-i}(M').$$

One corollary is sufficiently important that we state it before starting the proof:

Corollary 7.2. *For $0 \leq i \leq e$, the characteristic function L_i of the level space $\mathcal{L}_i$ has Fourier transform given by*

$$\widehat{L_i} = q^{e-i} L_{e-i}. \tag{38}$$

where $q = |k_K|$.

Proof. Immediate from Theorem 7.1, parts (d) and (g). ■

7.1 Discriminants of Kummer and affine extensions

The starting point for our investigation of discriminants is as follows:

Theorem 7.3. *Let K be a local field with $\mu_p \subseteq K$, and let $u \in K^\times$ be a minimal representative of a class in $K^\times/(K^\times)^p$. The discriminant ideal of the associated Kummer extension $L = K[\sqrt[p]{u}]$ is given by*

$$\mathrm{Disc}(L/K) = \begin{cases} \dfrac{p^p \cdot {\pi_K}^{p-1}}{(u-1)^{p-1}}\mathcal{O}_K & v_K(u-1) < \dfrac{pe_K}{p-1} \\ (1) & v_K(u-1) \geq \dfrac{pe_K}{p-1}. \end{cases}$$

Proof. One can find an explicit basis for $\mathcal{O}_L$ and compute the discriminant. For details, see Del Corso and Dvornicich [13, Lemmas 5, 6, and 7]. ■

In this section, we will prove the following generalization:

Theorem 7.4. *Let K be a local field, and let M be a G_K-module with underlying group $\mathcal{C}_p$. Let T' be the $(\mathbb{Z}/p\mathbb{Z})^\times$-torsor corresponding to the G_K-set $\mathrm{Surj}(M, \mu_m)$, and let T_1' be the field factor of T'. Let $u \in T_1'^\times$ be a minimal representative for a class in $(T_1'^\times)_\omega$ parametrizing, via Theorem 5.4 a coclass $\sigma \in H^1(K, M)$, and let L be the corresponding $\mathcal{GA}(\mathcal{C}_p)$-extension. Then*

$$\mathrm{Disc}(L/K)\mathcal{O}_{T_1'} = \begin{cases} \dfrac{p^p \cdot {\pi_K}^{p-1}}{(u-1)^{p-1}}\mathcal{O}_{T_1'} & v_{T_1'}(u-1) < \dfrac{pe_{T_1'}}{p-1} \\ \mathrm{Disc}(T/K) \cdot \mathcal{O}_{T_1'} & v_{T_1'}(u-1) \geq \dfrac{pe_{T_1'}}{p-1}, \end{cases} \tag{39}$$

where T is the $(\mathbb{Z}/p\mathbb{Z})^\times$-torsor corresponding to M.

Remark 7.5. Note that $(u-1)^{p-1}\mathcal{O}_{T_1'}$ is the extension of an ideal of K, since $e_{T_1'/K}$ divides $p-1$.

Proof. If L is *not* a field, then the image of G_K in $\mathcal{GA}(\mathcal{C}_p)$ lies in a nontransitive subgroup (viewing $\mathcal{GA}(\mathcal{C}_p)$ as embedded in $\mathrm{Sym}(\mathcal{C}_p)$). It is not hard to show that every nontransitive subgroup of $\mathcal{GA}(\mathcal{C}_p)$ has a fixed point. Moving this fixed point to 0, we get that $\sigma = 0$, $u = 1$, and $L \cong K \times T$, in accord with the second case of the formula.

We may now assume that L is a field. Although the extension L/K need not be Galois, we have

$$T[\mu_p] \otimes_K L \cong T[\mu_p, \sqrt[p]{u}],$$

a Kummer extension of $T[\mu_p]$. Let E be a field factor of $T[\mu_p]$ containing T_1'. Then

$$E \otimes_K L \cong E[\sqrt[p]{u}]$$

as extensions of E. Note that $[E:K] | (p-1)^2$; in particular, $[E:K]$ is prime to p. So u remains a minimal representative in $E^\times$, and since E and L must be linearly disjoint, $E \otimes_K L = EL$ is a field

unless $u = 1$. So

$$\mathrm{Disc}(EL/E) = \begin{cases} \dfrac{p^p \cdot {\pi_E}^{p-1}}{(u-1)^{p-1}}\mathcal{O}_E & v_K(u-1) < \dfrac{pe_K}{p-1} \\ (1) & v_K(u-1) \geq \dfrac{pe_K}{p-1}. \end{cases}$$

We must now relate $\mathrm{Disc}(EL/E)$ to $\mathrm{Disc}(L/K)$. If $v_K(u-1) \geq pe_K/(p-1)$, then EL/E is unramified, so $p \nmid e_{EL/K}$ and L/K is unramified as well. In particular, L/K is Galois, so M is trivial, T is totally split, and the formula again holds.

We are left with the case that $v_K(u-1) < \dfrac{pe_K}{p-1}$. Here EL/E, and hence L/K, are totally ramified. We relate their discriminants by the following trick, which also appears in Del Corso and Dvornicich [13]. An $\mathcal{O}_K$-basis for $\mathcal{O}_L$ is given by

$$1, \pi_L, \ldots, \pi_L^{p-1}. \tag{40}$$

The same elements form an $\mathcal{O}_E$-basis for an order $\mathcal{O} \subseteq \mathcal{O}_{EL}$, but their EL-valuations are $0, e', \ldots, (p-1)e'$, where $e' = e_{E/K}$. Divide each basis element by π_E as many times as possible so that it remains integral. We get a new system of elements

$$1, \frac{\pi_L}{\pi_E^{a_1}}, \ldots, \frac{\pi_L^{p-1}}{\pi_E^{a_{p-1}}}. \tag{41}$$

Since e' is coprime to p, these elements have EL-valuations $0, 1, \ldots, e'-1$ in some order and thus form an $\mathcal{O}_E$-basis for $\mathcal{O}_{EL}$. We have

$$\begin{aligned} v_E([\mathcal{O}_{EL} : \mathcal{O}]) &= a_1 + \cdots + a_{p-1} \\ &= \frac{[e' + \cdots + (p-1)e'] - [1 + \cdots + (p-1)]}{p} \\ &= \frac{(p-1)(e'-1)}{2}, \end{aligned}$$

and hence

$$\begin{aligned}\mathrm{Disc}(L/K) &= \mathrm{Disc}(\mathcal{O}/\mathcal{O}_E) \\ &= \mathrm{Disc}(\mathcal{O}_{EL}/\mathcal{O}_E)\cdot[\mathcal{O}_{EL}:\mathcal{O}]^2 \\ &= \frac{p^p\cdot {\pi_E}^{p-1}}{(u-1)^{p-1}}\cdot \pi_E^{(p-1)(e'-1)}\cdot\mathcal{O}_E \\ &= \frac{p^p\cdot {\pi_E}^{e'(p-1)}}{(u-1)^{p-1}}\cdot\mathcal{O}_E \\ &= \frac{p^p\cdot {\pi_K}^{(p-1)}}{(u-1)^{p-1}}\cdot\mathcal{O}_E. \end{aligned}$$

■

Remark 7.6. Along the lines of the preceding argument, we can prove the following more general result on discriminants in extensions of coprime degree:

Proposition 7.7. *Let L and M be two extensions of a local field K with* $\gcd([L:K],[M:K])=1$. *Then*

$$\mathrm{Disc}(L/K) = \mathrm{Disc}(LM/M)\cdot\left(\frac{\pi_M}{\pi_K}\right)^{f_{L/K}\left(e_{L/K}-1\right)}.$$

7.2 The Shafarevich basis

We start with the following exposition of the Shafarevich basis theorem. Although this theorem has appeared many times in the literature (see Del Corso and Dvornicich, [13], Proposition 6), we include a proof here by a method that will establish some important corollaries for us.

Filter $U = K^\times$ by the subgroups

$$U_i = \{x\in\mathcal{O}_K^\times : x\equiv 1 \mod \pi^i\},$$

and let $\bar{U}_i$ be the projection of U_i onto $\bar{U} := K^\times/(K^\times)^p$. Note that $\bar{U}_i = 0$ for $i > pe_K/(p-1)$, as the Taylor series for $\sqrt[p]{x}$ about 1 converges for $x\equiv 1 \bmod \pi^{\lfloor pe_K/(p-1)\rfloor+1}$. So

$$\bar{U}\cong \bar{U}/\bar{U}_0 \oplus \bigoplus_{0\le i\le \frac{pe_{T_1'}}{p-1}} \bar{U}_i/\bar{U}_{i+1} \tag{42}$$

as $\mathbb{F}_p$-vector spaces, and we can produce a basis for $\bar{U}$ by lifting a basis for each of the composition factors on the right-hand side.

Proposition 7.8 (the Shafarevich basis theorem). *Let $K \supseteq \mathbb{Q}_p$ be a local field, and let $i \geq 0$. The structure of $\bar{U}_i/\bar{U}_{i+1}$ is as follows:*

- *If*

$$0 < i < \frac{p}{p-1} e_K, \quad p \nmid i,$$

then $\bar{U}_i/\bar{U}_{i+1} \cong U_i/U_{i+1}$ has a basis of f_K units of the form $1 + x_j \pi^i$, where x_j ranges over an $\mathbb{F}_p$-basis of k_K. We call these generic units.

- *if $i = \frac{p}{p-1} e_K$ and $\mu_p \subseteq K$, then $\bar{U}_i/\bar{U}_{i+1}$ has dimension 1 and is generated by*

$$u = 1 + p(\zeta_p - 1)a,$$

for any $a \in \mathcal{O}_K$ with $p \nmid \mathrm{tr}_{\mathcal{O}_K/\mathbb{Q}_p}(a)$. We call such a generator an intimate unit, *and we let*

$$d_{\min} = |p(\zeta_p - 1)| = |p|^{p/(p-1)},$$

the distance of an intimate unit to 1.

- *For all other i, we have $\bar{U}_i/\bar{U}_{i+1} = 0$.*

Proof. Note that $\bar{U}_0/\bar{U}_1 = 0$ because $U_0/U_1 \cong k_K^\times$ has order prime to p. To compute $\bar{U}_i/\bar{U}_{i+1}$, where $i \geq 1$, we must see how many of the congruence classes $1 + x\pi^i \bmod \pi^{i+1}$ (where $x \in k_K$) contain a pth power.

Consider a general pth power u^p, $1 \neq u \in \mathcal{O}_K^\times$. Write $u = 1 + y\pi^j$, $\pi \nmid y$. By the binomial theorem,

$$u^p \equiv 1 + py\pi^j + y^p \pi^{pj} \mod \pi^{2j + e_K},$$

so

$$v(u^p-1)\begin{cases} = pj, & j < \frac{e_K}{p-1}, \\ \geq \frac{pe_K}{p-1}, & j = \frac{e_K}{p-1}, \\ = j + e_K, & j > \frac{e_K}{p-1}. \end{cases}$$

We now perform the needed analysis in each case:

- If $0 < i < pe_K/(p-1)$ and $p \nmid i$, then $v(u^p - 1)$ can never attain the value i, so the map $U_i/U_{i+1} \to \bar{U}_i/\bar{U}_{i+1}$ is an isomorphism, and we must include an entire basis of f elements in our basis for $\bar{U}$.

- If $0 < i < pe_K/(p-1)$ and $p|i$, then the pth powers

$$(1 + y\pi^{i/p})^p \equiv 1 + y^p\pi^i \mod \pi^{i+1}$$

  cover all the desired congruence classes, as the map $y \mapsto y^p$ on k_K is surjective; so $\bar{U}_i/\bar{U}_{i+1} = 0$.

- If $i > pe_K/(p-1)$, then the pth powers of elements of the form $1 + x\pi^{i-e_K}$ surject onto the congruence classes, repeating what we knew from the Taylor series.

- Finally, if $i = pe_K/(p-1)$, then we can only use powers $u^p = (1+\pi^j)^p$ where $j = e_K/(p-1)$. We have

$$(1 + y\pi^j) \equiv 1 + py\pi^j + y^p\pi^{pj} \equiv 1 + (y^p - cy)\pi^i \mod \pi^{i+1},$$

  where

$$c = \frac{-p}{\pi^{(p-1)j}} \in \mathcal{O}_K^\times.$$

  So we must analyze the (clearly linear) map $\wp_c : k_K \to k_K$ given by $\wp_c(y) = y^p - cy$.

  If c is *not* a $(p-1)$st power in k_K (or in $\mathcal{O}_K$, which amounts to the same thing by Hensel's lemma), then $\wp_c$ is injective and hence surjective, so $\bar{U}_i/\bar{U}_{i+1} = 0$. Also, K has no nontrivial pth roots of unity, as $u = \zeta_p$ would yield a nontrivial element of $\ker \wp_c$ (since $v_p(\zeta_p) = e_K/(p-1)$).

  If $c = b^{p-1}$ is a $(p-1)$st power in $\mathcal{O}_K$, then $y = b$ is an element of $\ker \wp_c$. Note that $u = 1 + b\pi^j$

lifts to a nontrivial pth root of unity ζ_p, since $u^p \equiv 1 \bmod \pi^{i+1}$ has (by the Taylor series again) a pth root that is 1 mod π^{j+1}. Note that $\ker \wp_c$ has dimension only 1, since b is unique up to $\mu_{p-1} = \mathbb{F}_p^\times$. Consequently $\operatorname{coker} \wp_c \cong \bar{U}_i/\bar{U}_{i+1}$ has dimension exactly 1.

This does not tell us how to find a generator for $\bar{U}_i/\bar{U}_{i+1}$. For this, put $y = by'$ so

$$(1 + by'\pi^j) \equiv 1 + b^p(y^p - y)\pi^i \equiv 1 + b^p \wp(y) \mod \pi^{i+1},$$

where $\wp(y) = y^p - y$ is the usual Artin-Schreyer map. Since y^p and y are Galois conjugates over $\mathbb{F}_p$, we have $\operatorname{tr}_{k_K/\mathbb{F}_p}(y^p - y) = 0$, so if $a \in k_K$ is an element with nonzero trace to $\mathbb{F}_p$, then $\bar{U}_i/\bar{U}_{i+1}$ is generated by

$$1 + ab^p\pi^i \equiv 1 + abc\pi^i \equiv 1 + ap(\zeta_p - 1) \mod \pi^{i+1}. \qquad \blacksquare$$

We draw two corollaries of the above method.

Corollary 7.9. *$\bar{U}$ has dimension*

$$[K : \mathbb{Q}_p] + 1 + \mathbf{1}_{\mu_p \subseteq K}$$

with a basis consisting of π_K and (arbitrary lifts of) the elements in the bases of $\bar{U}_i/\bar{U}_{i+1}$ in Proposition 7.8.

We call this basis the *Shafarevich basis* for U.

Remark 7.10. The dimension of $\bar{U}$ follows also from the Euler-characteristic computation

$$\frac{|H^0(K, \mu_p)||H^2(K, \mu_p)|}{|H^1(K, \mu_p)|} = p^{-[K:\mathbb{Q}_p]}$$

Proof. Clearly $\bar{U}/\bar{U}_0 \cong \mathcal{C}_p$ is generated by π_K. The result follows from the composition series (42). $\blacksquare$

Corollary 7.11. *An element $x \in \bar{U}$ belongs to $\bar{U}_i$ if and only if, in the expansion of x in the Shafarevich basis, only the basis elements in U_i appear (to nonzero exponents).*

Proof. Filtering $\bar{U}_i$ by the $\bar{U}_j$, for $j \geq i$, we see that a basis for $\bar{U}_i$ is given by the portion of the Shafarevich basis coming from $\bar{U}_j/\bar{U}_{j+1}$ for $j \geq i$. This is just the basis elements that lie in U_i. ■

The following simple result is one I have not seen in the literature before:

Corollary 7.12. *The cyclotomic extension $\mathbb{Q}_p[\mu_p]$ is isomorphic to $\mathbb{Q}_p[\sqrt[p-1]{-p}]$ and has Kummer element $-p$ as a μ_{p-1}-torsor.*

Proof. Let $K = \mathbb{Q}_p[\sqrt[p-1]{-p}]$, with uniformizer $\pi_K = \sqrt[p-1]{-p}$. In the notation of the intimate unit case of Proposition 7.8, we have $i = p$, $j = 1$,

$$c = \frac{-p}{\pi_K^{p-1}} = 1,$$

and we can take $b = \sqrt[p-1]{c} = 1$. Accordingly, $1 + \pi_K$ is congruent mod π_K^2 to a unique pth root of unity ζ_p. Note that $\zeta_p^i \equiv 1 + i\pi_K \bmod \pi_K^2$. Since μ_{p-1} acts on π_K by multiplication, it must act on the powers of ζ_p by ω. Hence $K \cong \mathbb{Q}_p[\mu_p]$ as μ_{p-1}-torsors. ■

In the rest of this section we will study how $\bar{U} = \bar{U}(K)$ behaves under field extension. We use the following notational conventions:

Elements $u \in K^\times/(K^\times)^p$ are classified by their *distance,* by which we mean the closest distance of a representative from 1:

$$d(u) = d_K(u) = \min_{y \in K^\times} |uy^p - 1|.$$

Here the absolute value is the local one on K. (We could choose a normalization of this absolute value, but we prefer to express $d(u)$ in terms of an undetermined $|\pi_K|$ and $|p| = |\pi_K|^{e_K}$.) Note that $d(u) \leq 1$, since u can always be taken to have nonnegative valuation. Also, it is easy to see that $d(uv) \leq \max\{d(u), d(v)\}$, so d defines a norm on $K^\times/(K^\times)^p$.

For ease in stating theorems involving distances, we note that an ideal (or even a fractional ideal) $\mathfrak{a}$ of a local field K is uniquely determined by the largest absolute value of its elements, which we denote by $|\mathfrak{a}|$. We have

$$\mathfrak{a} = \{x \in K : |x| \leq |\mathfrak{a}|\}.$$

For any real $d > 0$, let $B_{\leq d}$ denote the closed ball of radius d about 1 in $K^\times/(K^\times)^p$:

$$B_{\leq d} = \{u \in K^\times/(K^\times)^p : d(u) \leq d\}$$

and likewise for $B_{<d}$. It is easy to prove that these are subgroups. If $\mathfrak{f} \subsetneq \mathcal{O}_K$ is an ideal, then $B_{\leq |\mathfrak{f}|}$ is the projection of $\mathcal{U}_\mathfrak{f}$; but this fails for $\mathfrak{f} = (1)$.

Note the following:

Lemma 7.13. *If L/K is an extension of local fields whose degree n is prime to p, then the canonical map from $K^\times/(K^\times)^p$ to $L^\times/(L^\times)^p$ is injective and preserves distance: that is, for every $u \in K^\times/(K^\times)^p$,*

$$d_K(u) = d_L(u).$$

Proof. The injectivity follows from the fact that if $u \in K$, then $N_{L/K} = u^n$ and n is prime to p.

It is obvious that $d_L(u) \leq d_K(u)$, so it suffices to prove the opposite inequality. It's easy to see that if $x \in \mathcal{O}_L$, then

$$|N_{L/K}(x) - 1| \leq |x - 1|.$$

Let $y \in L^\times$ achieve $|uy^p - 1| = d_L(u)$. Then

$$d_L(u) = |uy^p - 1| \geq |N_{L/K}(uy^p) - 1| = |u^{[L:K]}N_{L/K}(y)^p - 1| \geq d_K\left(u^{[L:K]}\right).$$

But u is a power of $u^{[L:K]}$ up to pth powers, so $d_K(u) \leq d_K\left(u^{[L:K]}\right)$, completing the proof. ■

Assume $K \supseteq \mathbb{Q}_p$. We first parametrize M itself. By (classical) Kummer theory, we have canonical isomorphisms

$$\mathrm{Hom}(G_K, \mathrm{Aut}(\mathcal{C}_p)) \cong H^1(G_K, (\mathbb{Z}/p\mathbb{Z})^\times) \cong H^1(G_K, \mu_{p-1}) \cong K^\times/(K^\times)^{p-1}$$

where the isomorphism $(\mathbb{Z}/p\mathbb{Z})^\times \cong \mu_{p-1}$ is given by Teichmüller lift. (Note that we do not need to pick a generator of $(\mathbb{Z}/p\mathbb{Z})^\times$ to do this.) We have the following:

Lemma 7.14. *If M is the Galois module with underlying group $\mathcal{C}_p$ corresponding to the Kummer element $\beta \in K^\times/(K^\times)^{p-1}$, then the Tate dual M' has Kummer element $\beta' = -p/\beta$.*

Proof. When M is trivial, the result was proved as Corollary 7.12. The lemma then follows by noting that if M_1, M_2 are cyclic Galois modules of order p with Kummer elements β_1, β_2, respectively, then $\mathrm{Hom}(M_1, M_2)$ is also cyclic of order p and has Kummer element β_2/β_1. ■

If T' has r field factors (all necessarily isomorphic to one T_1'), then, by Corollary 7.9,

$$\dim_{\mathbb{F}_p} T'^\times/(T'^\times)^p = \begin{cases} n+2r, & \mu_p \subseteq T_1' \\ n+r & \text{otherwise.} \end{cases}$$

The group $T'^\times/(T'^\times)^p$ is a representation of $(\mathbb{Z}/p\mathbb{Z})^\times$ over the field $\mathbb{F}_p$. Since $\mathbb{F}_p$ has the $(p-1)$st roots of unity, such a representation splits as a direct sum of 1-dimensional representations; there are $p-1$ of these, and they are the powers of the standard representation

$$\omega : (\mathbb{Z}/p\mathbb{Z})^\times \to \mathrm{GL}_1(\mathbb{F}_p)$$

given by the obvious isomorphism. By Theorem 5.4, $H^1(K, M)$ is parametrized by the ω-isotypical component of $T'^\times/(T'^\times)^p$, which we denote by $T_\omega'^\times$ for brevity.

We can reduce the problem from T' to T_1' in the following way:

Lemma 7.15. *Let T' be a μ_t-torsor, $t|p-1$. Let T_1' be the field factor of T', and let $r = [T_1' : K]$. Then:*

(a) *The subgroup fixing T_1' (as a set) is $\mu_r \subseteq \mu_{p-1} \cong (\mathbb{Z}/p\mathbb{Z})^\times$, and T_1' is a μ_r-torsor;*

(b) *Projection to T_1' defines an isomorphism $T_\omega'^\times \cong (T_1'^\times)_\omega$, where*

$$T_\omega'^\times = \left\{\alpha \in T'^\times/(T'^\times)^p : \tau_c(\alpha) = \alpha^c \,\forall c \in \mu_t\right\} \tag{43}$$

$$(T_1'^\times)_\omega = \left\{\alpha \in T_1'^\times/(T_1'^\times)^p : \tau_c(\alpha) = \alpha^c \,\forall c \in \mu_r\right\}. \tag{44}$$

(c) *More generally, for any s with $r|s|t$, the orbit $\mu_s(T_1')$ consists of s/n field factors whose product T_s' is a μ_s-torsor. Projection onto T_s' and then onto T_1' defines isomorphisms*

$$T_\omega'^\times \cong (T_s'^\times)_\omega \cong (T_1'^\times)_\omega.$$

Remark 7.16. A result with much the same content, but in a slightly different setting, is proved by Del Corso and Dvornicich ([13], Proposition 7).

Proof. The torsor action must permute the field factors transitively; since μ_n is cyclic, a generator ζ_n must cyclically permute them, and the stabilizer of T_1 (as a set) is $\langle \zeta^{n/r} \rangle = \mu_r$, proving(a). Since the action simply transitively permutes the coordinates of T_1, T_1 is a μ_r-torsor. If we know the T_1-component $\alpha|_{T_1^\times}$ of an $\alpha \in (T^\times/(T^\times)^p)_\omega$, then all the other components are uniquely determined by the eigenvector condition; it is only necessary for $\alpha|_{T_1^\times}$ to behave properly under μ_r, namely that $\alpha_{T_1^\times} \in (T_1^\times)_{\omega^k}$.

This proves (b). Also, it is clear from our analysis that $\mu_s(T_1)$ is a μ_s-torsor. Applying (b) to this torsor proves (c). ∎

We now filter $T_1'^\times$ as above to discover its ω-component.

Proposition 7.17 (**the Shafarevich basis for $T_\omega'^\times$**). *As above, let $T' = K[\sqrt[p-1]{\beta}]$ be the $(\mathbb{Z}/p\mathbb{Z})^\times$-torsor corresponding to the Tate dual M' of a cyclic Galois module M of order p with Kummer element $\beta \in K^\times/(K^\times)^{p-1}$, and let T_1' be the field factor of T'. Filter $\bar{U} = T_1'^\times/(T_1'^\times)^p$ by the subgroups $\bar{U}_i$ as in the previous subsection. Since the μ_r-torsor action on T_1' preserves the valuation, each U_i is a subrepresentation of $T_1'^\times/(T_1'^\times)^p$. Then:*

(a) *The ω-isotypical component of $\bar{U}/\bar{U}_0$ has dimension 1 if M' is trivial, 0 otherwise.*

(b) *The ω-isotypical component of $\bar{U}_i/\bar{U}_{i+1}$ has dimension*

- *f if*

$$0 < i < \frac{pe_{T_1'/\mathbb{Q}_p}}{p-1}, \quad i \not\equiv 0 \mod p, \quad i \equiv \frac{e_{T_1'/K} v_K(\beta)}{p-1} \mod e_{T_1'/K};$$

- 1 *if* $i = \frac{pe_{T_1'/\mathbb{Q}_p}}{p-1}$ *and* M *is trivial;*
- 0 *otherwise.*

Proof. Note that $U/U_0 = \langle \pi_{T_1'} \rangle$ is a copy of the trivial representation and that ω is trivial (as a representation of μ_r) exactly when $r = 1$, that is, M' is trivial.

Our convention for the Kummer map is such that

$$\tau_c(\sqrt[p-1]{\beta}) = \tilde{c}\sqrt[p-1]{\beta}.$$

By a standard result in Kummer theory, the degree r is the least integer such that $\beta = \beta_1^{(p-1)/r}$ is a $(p-1)/r$th power, and $T_1' = K[\sqrt[r]{\beta_1}]$ with

$$\tau_c(\sqrt[r]{\beta_1}) = \tilde{c}\sqrt[r]{\beta_1}.$$

Let $f' = \gcd\left(v_K(\beta_1), r\right)$ and $e' = r/f'$. We claim that e' and f' are respectively the ramification and inertia indices of T_1' over K. By the Euclidean algorithm, we may choose integers g and h such that

$$gv(\beta_1) - hr = f'. \tag{45}$$

Construct the elements

$$\pi' = \frac{\left(\sqrt[r]{\beta_1}\right)^g}{\pi_K^h} \quad \text{and} \quad u' = \frac{\left(\sqrt[r]{\beta_1}\right)^{e'}}{\pi_K^{v_K(\beta_1)/f'}}.$$

Note that $v_K(\pi') = 1/e'$, so

$$e_{T_1'/K} \geq e'. \tag{46}$$

On the other hand, $v_K(u') = 0$, and u' is an f'th root of the unit

$$\beta_2 = \frac{\beta_1}{\pi_K^{v_K(\beta_1)}}.$$

Note that β_2 is not an ℓth power for any prime $\ell | f'$, as otherwise β would be a $(p-1)\ell/r$th power,

contradicting what we know about r. So the residue class of u' generates a degree-f' extension of k_K inside $k_{T_1'}$; in particular,

$$f_{T_1'/K} \geq f'. \tag{47}$$

Equality must hold in (46) and (47), so T_1' has uniformizer π' and residue field generator u'. Note that for $c \in \mathbb{F}_p^\times$,

$$\tau_c(\pi') = \tilde{c}^g \pi' \quad \text{and} \quad \tau_c(u') = \tilde{c}^{e'} u'.$$

We now have what we need to compute the Galois action on $\bar{U}_i/\bar{U}_{i+1}$. By Proposition 7.8, the space $\bar{U}_i/\bar{U}_{i+1}$ is nonzero only for

$$0 < i < \frac{pe_{T_1'}}{p-1}, \quad p \nmid i$$

(the generic units) and possibly for $i = pe_K/(p-1)$ also (the intimate units).

We begin with the first case. Here $\bar{U}_i/\bar{U}_{i+1} \cong U_i/U_{i+1}$ has a basis

$$1 + \pi'^i u'^j, \quad 0 \leq j < f'.$$

For $c \in \mu_r$,

$$\begin{aligned} \tau_c(1 + \pi'^i u'^j) &= 1 + \tilde{c}^{gi+e'j} \pi'^i u'^j \\ &\equiv (1 + \pi'^i u'^j)^{c^{gi+e'j}} \mod \pi'^{i+1}. \end{aligned}$$

Thus the basis element $1 + \pi'^i u'^j$ generates a 1-dimensional μ_r-submodule of U_i/U_{i+1} isomorphic to $\omega^{gi+e'j}$. Accordingly, we select the generic units satisfying

$$gi + e'j \equiv 1 \mod r.$$

Since $r = e'f'$, there are exactly f' values of j satisfying this when

$$e' | gi - 1, \tag{48}$$

and none otherwise. By (45), g is the multiplicative inverse of $v(\beta_1)/f' = e'v(\beta)/(p-1) \bmod e'$, so we can rewrite (48) as

$$i \equiv \frac{e'v(\beta)}{p-1} \mod e',$$

as desired.

As to the case that $i = pe_{T_1'}/(p-1)$ (the intimate units), we simply note that, by Proposition 7.4, we have

$$(\bar{U}_i)_\omega \cong H^1_{\mathrm{ur}}(K, M),$$

so

$$|(\bar{U}_i)_\omega| = |H^1_{\mathrm{ur}}(K, M)| = |H^0(K, M)|.$$

(A direct computation of the torsor action on the intimate units is also possible; it turns out that $\bar{U}_i \cong \mu_m$ as μ_{m-1}-modules.) ■

By complete reducibility, we can get a basis for $\bar{U}_\omega$ from the bases for its composition factors:

Corollary 7.18. *If $M \cong \mathcal{C}_p$, then $H^1(K, M)$ has dimension*

$$[K : \mathbb{Q}_p] + \dim_{\mathbb{F}_p} H^0(K, M) + \dim_{\mathbb{F}_p} H^0(K, M'),$$

with a basis consisting of appropriate lifts of the Shafarevich basis elements picked out by Proposition 7.17.

In particular, we have proved Theorem 7.1(e).

7.3 Proof of Theorem 7.1

It now remains to recast the above results in terms of levels and offsets and prove the remaining parts of Theorem 7.1.

Let $\alpha \in (T_1'^{\times})_\omega$, α being a minimal-distance element. We consider the possibilities for the leading factor in α with respect to the Shafarevich basis; this determines $|\alpha - 1|$ by Corollary 7.9, and thence

$d := v_K(\mathrm{Disc}(L/K))$ and hence the level and offset of α.

- If α is led by the uniformizer, then M' is trivial. From Theorem 7.4, we get $d = pe_K + p - 1$, so $\ell(\alpha) = -1$ and $\theta(\alpha) = -1$.

- If α is led by a generic unit, then we have $v_{T_1'}(\alpha - 1) = i$, where i is an integer satisfying

$$0 < i < \frac{pe_{T_1'/\mathbb{Q}_p}}{p-1}, \quad i \not\equiv 0 \mod p, \quad i \equiv \frac{e_{T_1'/K} v_K(\beta)}{p-1} \mod e_{T_1'/K},$$

  and each of these values is attained by some α. Using the one-to-one correspondence of Theorem 7.4, we get that $v_K(\operatorname{disc} L)$ attains exactly the values d such that

$$p - 1 < d < pe_K + p - 1, \quad d \not\equiv -1 \mod p, \quad d \equiv e_K - v_K(\beta) \mod p - 1.$$

  Thus $0 \le \ell(\alpha) < e_K$, $0 \le \theta(\alpha) \le p - 2$, and θ is determined by ℓ via the condition mod $p - 1$.

- If α is led by an intimate unit or $\alpha = 1$, then $d = v_K(\operatorname{disc} L) = v_K(\operatorname{disc} T')$ was already computed in proving Theorem 7.4. Since T' is a product of tamely ramified extensions, we have $d < [T' : K] = p - 1$, so $\ell = 0$.

This proves (a) and (c).

In the case that α is led by a generic unit of level ℓ, $0 \le \ell < e$, there are alternative ways to characterize θ. We have

$$\theta = \left\{ \frac{\ell - v_K(\beta)}{p-1} \right\} (p-1),$$

from which

$$v_K(\operatorname{disc} L) = p(e - \ell) + \theta = p(e - \ell) + \left\{ \frac{\ell - v_K(\beta)}{p-1} \right\} (p-1)$$

Since $v_K(\operatorname{disc} L)$ is in bijection with $|\alpha - 1|$ by Theorem 7.4, we can likewise determine

$$v_K(\alpha - 1) = \left\lfloor \frac{p\ell - v_K(\beta)}{p-1} \right\rfloor + 1 + \frac{v_K(\beta)}{p-1}.$$

Item (f) demands that we invert this to determine how the level $\ell(\alpha)$ changes as α ranges in a ball

$$|\alpha - 1| \leq d.$$

If $d < d_{\min}$, then every α in this ball is a pth power (by Proposition 7.8, or simply by noting that the Taylor series for pth root converges on this ball), so the range of $[\alpha]$ is $\{1\} = \mathcal{L}_{e+1}$. If $d \geq d_{\min}$, then the intimate units are certainly included, so the range of $[\alpha]$ is at least $\mathcal{L}_e$; it also includes all generic units whose levels ℓ satisfy

$$\begin{aligned} v_K(\alpha - 1) &\geq \frac{\log d}{\log|\pi_K|} \\ \left\lfloor \frac{p\ell - v_K(\beta)}{p-1} \right\rfloor + 1 + \frac{v_K(\beta)}{p-1} &\geq \frac{\log d}{\log|\pi_K|} \\ \left\lfloor \frac{p\ell - v_K(\beta)}{p-1} \right\rfloor &\geq \frac{\log d}{\log|\pi_K|} - 1 - \frac{v_K(\beta)}{p-1}. \end{aligned}$$

Using the exchange

$$\lfloor x \rfloor \geq y \iff \lfloor x \rfloor \geq \lceil y \rceil \iff x \geq \lceil y \rceil,$$

valid for all real numbers x and y, we can get this into a form solvable for ℓ:

$$\begin{aligned} \frac{p\ell - v_K(\beta)}{p-1} &\geq \left\lceil \frac{\log d}{\log|\pi_K|} - 1 - \frac{v_K(\beta)}{p-1} \right\rceil \\ \ell &\geq \frac{v_K(\beta)}{p} + \frac{p-1}{p} \left\lceil \frac{\log d}{\log|\pi_K|} - 1 - \frac{v_K(\beta)}{p-1} \right\rceil. \end{aligned}$$

So the range of $[\alpha]$ is $\mathcal{L}_i$, where

$$\left\lceil \frac{v_K(\beta)}{p} + \frac{p-1}{p} \left\lceil \frac{\log d}{\log|\pi_K|} - 1 - \frac{v_K(\beta)}{p-1} \right\rceil \right\rceil, \tag{49}$$

as claimed in (f).

For (b), we note that as d decreases from 1 to $d_{\min}$, the corresponding i in (49) hits every value from 0 to e, since the argument to the outer ceiling increases by jumps of $(p-1)/p < 1$. So each $\mathcal{L}_i$

is a subgroup. For (d), we note that $|\mathcal{L}_0| = |H^0(K, M)|$, while for $1 \leq i \leq e$,

$$\mathcal{L}_{i+1}/\mathcal{L}_i \cong \bar{U}_j/\bar{U}_{j+1}$$

has $p^f = q$ elements, where j is the unique value of $v_{T_1'}(\alpha - 1)$ for values of α having level i.

Finally, we have claimed a relation (g) regarding how level spaces interact with the Tate pairing. In the case of the Hilbert pairing, the result we need is as follows:

Lemma 7.19 (an explicit reciprocity law). *Let K be a local field with $\mu_p \subseteq K$. If $\alpha, \beta \in \mathcal{O}_K^\times$ satisfy*

$$|\alpha - 1| \cdot |\beta - 1| < d_{\min} = |p|^{p/(p-1)},$$

then the Hilbert pairing $\langle \alpha, \beta \rangle_K$ vanishes.

Proof. This is a consequence of the *conductor-discriminant formula* (see Neukirch [39], VII.11.9): For a Galois extension L/K,

$$\mathrm{Disc}(L/K) = \prod_\chi \mathfrak{f}(\chi)^{\chi(1)},$$

where χ ranges over the irreducible characters of $\mathrm{Gal}(L/K)$. Here we apply the formula to $L = K[\sqrt[p]{\alpha}]$. Scale α by pth powers to be as close to 1 as possible. If $\alpha = 1$ or α is an intimate unit, the Hilbert pairing clearly vanishes since L is unramified and β is a unit. So we can assume that L is a ramified extension of degree p. Then there are p-many characters on $\mathrm{Gal}(L/K)$, all of dimension 1. One is the trivial character, whose conductor is 1. The others all have the same conductor $\mathfrak{f}$, so

$$\mathrm{Disc}(L/K) = \mathfrak{f}^{p-1}.$$

By Theorem 7.4, we have

$$\mathrm{Disc}(L/K) \sim \frac{p^p \cdot \pi_K^{p-1}}{(\alpha - 1)^{p-1}},$$

so $\mathfrak{f}$ is generated by any element f with

$$|f| = \left| \frac{p^{p/(p-1)} \cdot \pi_K}{\alpha - 1} \right|.$$

Note that $d_{\min} = |p|^{p/(p-1)}$ is actually an attainable norm of an element of K, namely $(\zeta_p - 1)^p$. By the given inequality, $\beta \equiv 1 \mod \mathfrak{f}$ which implies that the Hilbert symbol

$$\langle \alpha, \beta \rangle_K = \phi_{L/K}(\beta)$$

vanishes. ■

If $0 \leq i \leq e$, $\alpha \in \mathcal{L}_i(M)$, and $\beta \in \mathcal{L}_{e-i}(M)$, then it is easy to verify that the hypothesis of Lemma 7.19 holds in each field factor of $T[\mu_m]$, in which the Hilbert pairing is being computed. Hence

$$\mathcal{L}_i(M)^\perp \supseteq \mathcal{L}_{e-i}(M').$$

However, since

$$|\mathcal{L}_i(M)| \cdot |\mathcal{L}_{e-i}(M')| = q^{e_K} \cdot |H^0(K, M)| \cdot |H^0(K, M')| = |H^1(K, M)|,$$

equality must hold. ■

7.4 The tame case

If K is a tame local field, that is, $\operatorname{char} k_K \neq p$, the structure of $H^1(K, M)$ is well known. We put

$$e = 0, \quad \mathcal{L}_{-1} = \{0\}, \quad \mathcal{L}_0 = H^1_{\mathrm{ur}}(K, M), \quad \mathcal{L}_1 = H^1(K, M)$$

and observe that Theorem 7.1(c), (d), (e), (g) and Corollary 7.2 still hold.

The *wild function field* case $K = \mathbb{F}_{p^r}(\!(t)\!)$ admits a similar treatment, but now the number of levels is infinite. We do not address this case here.

Part III

Composed varieties

8 Composed varieties

It has long been noted that orbits of certain algebraic group actions on varieties over a field K parametrize rings of low rank over K, which can also be identified with the cohomology of small Galois modules over K. The aim of this section is to explain all this in a level of generality suitable for our applications.

Definition 8.1. Let K be a field and $\bar{K}$ its separable closure. A *composed variety* over K is a quasi-projective variety V over K with an action of a quasi-projective algebraic group Γ over K such that:

(a) V has a K-rational point x_0;

(b) the $\bar{K}$-points of V consist of just one orbit $\Gamma(\bar{K})x_0$;

(c) the point stabilizer $M = \mathrm{Stab}_{\Gamma(\bar{K})} x_0$ is a *finite abelian* subgroup.

The term *composed* is derived from Gauss composition of binary quadratic forms and the "higher composition laws" of the work of Bhargava and others, from which we derive many of our examples.

Proposition 8.2.

(*a*) *Once a base orbit* $\Gamma(K)x_0$ *is fixed, there is a natural injection*

$$\psi : \Gamma(K)\backslash V(K) \hookrightarrow H^1(K, M)$$

by which the orbits $\Gamma(K)\backslash V(K)$ *parametrize some subset of the Galois cohomology group* $H^1(K, M)$.

(*b*) *The* $\Gamma(K)$*-stabilizer of every* $x \in V(K)$ *is canonically isomorphic to* $H^0(K, M)$.

Proof. (a) Let $x \in V(K)$ be given. Since there is only one $\Gamma(\bar{K})$-orbit, we can find $\gamma \in \Gamma(\bar{K})$ such that $\gamma(x_0) = x$. For any $g \in \mathrm{Gal}(\bar{K}/K)$, $g(\gamma)$ also takes x_0 to x and so differs from γ by right-multiplication by an element in $\mathrm{Stab}_{\Gamma(\bar{K})} x_0 = M$. Define a cocycle $\sigma_x : \mathrm{Gal}(\bar{K}/K) \to M$ by

$$\sigma_x(g) = g(\gamma) \cdot \gamma^{-1}.$$

It is routine to verify that

- σ_x satisfies the cocycle condition $\sigma_x(gh) = \sigma_x(g) \cdot g(\sigma_x(h))$ and hence defines an element of $H^1(K, M)$;
- If a different γ is chosen, then σ_x changes by a coboundary;
- If x is replaced by αx for some $\alpha \in \Gamma_K$, the cocycle σ_x is unchanged;
- If the basepoint x_0 is replaced by αx_0 for some $\alpha \in \Gamma(K)$, the cocycle σ_x is unchanged, up to identifying M with $\mathrm{Stab}_{\Gamma(\bar{K})}(\alpha x_0) = \alpha M \alpha^{-1}$ in the obvious way. (This is why we can fix merely a base *orbit* instead of a basepoint.)

So we get a map

$$\psi : \Gamma(K) \backslash V(K) \to H^1(K, M).$$

We claim that ψ is injective. Suppose that $x_1, x_2 \in V(K)$ map to equivalent cocycles σ_{x_1}, σ_{x_2}. Let $\gamma_i \in \Gamma(\bar{K})$ be the associated transformation that maps x_0 to x_i. By right-multiplying γ_1 by an element of M, as above, we can remove any coboundary discrepancy and assume that $\sigma_{x_1} = \sigma_{x_2}$ on the nose. That is, for every $g \in \mathrm{Gal}(\bar{K}/K)$,

$$g(\gamma_1) \cdot \gamma_1^{-1} = g(\gamma_2) \cdot \gamma_2^{-1},$$

which can also be written as

$$g(\gamma_2 \gamma_1^{-1}) = \gamma_2 \gamma_1^{-1}.$$

Thus, $\gamma_2 \gamma_1^{-1}$ is Galois stable and hence defined over K. It takes x_1 to x_2, establishing that

these points lie in the same $\Gamma(K)$-orbit, as desired.

(b) If $\gamma(x_0) = x$, then the $\Gamma(\bar{K})$-stabilizer of x is of course $\gamma M \gamma^{-1}$. We claim that the obvious map

$$M \to \gamma M \gamma^{-1}$$

$$\mu \mapsto \gamma \mu \gamma^{-1}$$

is an isomorphism of Galois modules. We compute, for $g \in \mathrm{Gal}(\bar{K}/K)$,

$$g\left(\gamma\mu\gamma^{-1}\right) = g(\gamma)g(\mu)g(\gamma)^{-1} = \gamma\sigma_x(g)g(\mu)\sigma_x(g)^{-1}\gamma^{-1} = \gamma g(\mu)\gamma^{-1},$$

establishing the isomorphism. In particular, the Galois-stable points $\mathrm{Stab}_{\Gamma(K)} x_0 = H^0(K, M)$ are the same at x as at x_0. Note the crucial way that we used that M is abelian. By the same token, the identification of stabilizers is independent of γ and is thus canonical. ■

The base orbit is distinguished only insofar as it corresponds to the zero element $0 \in H^1(K, M)$. Changing base orbits changes the parametrization minimally:

Proposition 8.3. *The parametrizations $\psi_{x_0}, \psi_{x_1} : \Gamma(K)\backslash V(K) \to H^1(K, M)$ corresponding to two basepoints $x_0, x_1 \in V(K)$ differ only by translation:*

$$\psi_{x_1}(x) = \psi_{x_0}(x) - \psi_{x_0}(x_1),$$

under the isomorphism between the stabilizers M established in the previous proposition.

Proof. Routine calculation. ■

While ψ is always injective, it need not be surjective, as we will see by examples in the following section.

Definition 8.4.

(a) A composed variety is *full* if ψ is surjective, that is, it includes a $\Gamma(K)$-orbit for every cohomology class in $H^1(K, M)$.

(b) If K is a global field, a composed variety is *Hasse* if for every $\alpha \in H^1(K, M)$, if the localization $\alpha_v \in H^1(K_v, M)$ at each place v lies in the image of the local parametrization

$$\psi_v : V(K_v)\backslash\Gamma(K_v) \to H^1(K_v, M),$$

then α also lies in the image of the global parametrization ψ.

8.1 Examples

In this section, K is any field not of one of finitely many bad characteristics for which the exposition does not make sense.

Example 8.5. The group $\Gamma = \mathbb{G}_m$ can act on the variety $V = \mathbb{A}^1\backslash\{0\}$, the punctured affine line, by

$$\lambda(x) = \lambda^n \cdot x.$$

There is a unique $\bar{K}$-orbit. The point stabilizer is μ_n, and the parametrization corresponding to this composed variety (choosing basepoint $x_0 = 1$) is none other than the Kummer map

$$K^\times/(K^\times)^n \to H^1(K, \mu_n).$$

That V is full follows from Hilbert's Theorem 90.

Example 8.6. Let V be the variety of binary cubic forms f over K with fixed discriminant D_0. This has an algebraic action of SL_2, which is transitive over $\bar{K}$ (essentially because PSL_2 carries any three points of $\mathbb{P}^1$ to any other three), and there is a ready-at-hand basepoint

$$f_0(X, Y) = X^2Y - \frac{D}{4}Y^3.$$

The point stabilizer M is isomorphic to $\mathbb{Z}/3\mathbb{Z}$, but twisted by the character of $K(\sqrt{D})$; that is, $M \cong \{0, \sqrt{D}, -\sqrt{D}\}$ as sets with Galois action. Coupled with the appropriate higher composition law (Theorem 6.9), this recovers the parametrization of cubic étale algebras with fixed quadratic resolvent by $H^1(K, M)$ in Proposition 4.18. To see that it is the same parametrization, note that a $\gamma \in \Gamma(\bar{K}/K)$ that takes f_0 to f is determined by where it sends the rational root $[1:0]$ of f_0, so the three γ's are permuted by $\mathrm{Gal}(\bar{K}/K)$ just like the three roots of f. In particular, V is full.

Example 8.7. Continuing with the sequence of known ring parametrizations, we might study the variety V of pairs of ternary quadratic forms with fixed discriminant D_0. This has one orbit over $\bar{K}$ under the action of the group $\Gamma = \mathrm{SL}_2 \times \mathrm{SL}_3$; unfortunately, the point stabilizer is isomorphic to the alternating group A_4, which is not abelian.

So we narrow the group, which widens the ring of invariants and requires us to take a smaller V. We let $\Gamma = \mathrm{SL}_3$ alone act on pairs (A, B) of ternary quadratic forms, which preserves the resolvent

$$g(X, Y) = 4 \det(AX + BY),$$

a binary cubic form. We let V be the variety of (A, B) for which $g = g_0$ is a fixed separable polynomial. These parametrize quartic étale algebras L over K whose cubic resolvent R is fixed. There is a natural base orbit (A_0, B_0) whose associated $L \cong K \times R$ has a linear factor. The point stabilizer $M \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$, with the three non-identity elements permuted by $\mathrm{Gal}(\bar{K}/K)$ in the same manner as the three roots of g_0. We have reconstructed the parametrization of quartic étale algebras with fixed cubic resolvent by $H^1(K, M)$ in Proposition 4.18. In particular, V is full.

Example 8.8. Alternatively, we can consider the space V of binary quartic forms whose invariants $I = I_0$, $J = J_0$ are fixed. The orbits of this space have been found useful for parametrizing 2-Selmer elements of the elliptic curve $E : y^2 = x^3 + xI + J$, because the point stabilizer is $M \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ with the Galois-module structure $E[2]$. This space V embeds into the space of the preceding example

via a map which we call the *Wood embedding* after its prominent role in Wood's work [59]:

$$f \mapsto (A, B)$$

$$ax^4 + bx^3y + cx^2y^2 + dxy^3 + ey^4 \mapsto \left(\begin{bmatrix} & & 1/2 \\ & -1 & \\ 1/2 & & \end{bmatrix}, \begin{bmatrix} a & b/2 & c/3 \\ b/2 & c/3 & d/2 \\ c/3 & d/2 & e \end{bmatrix} \right).$$

In general, V is *not* full. For instance, over $K = \mathbb{R}$, if E has full 2-torsion, there are only three kinds of binary quartics over $\mathbb{R}$ with positive discriminant (positive definite, negative definite, and those with four real roots) which cover three of the four elements in $H^1(\mathbb{R}, \mathbb{Z}/2\mathbb{Z})$. Two of these three (positive definite, four real roots) form the subgroup of elements whose corresponding E-torsor $z^2 = f(x, y)$ is soluble at ∞: these are the ones we retain when studying $\mathrm{Sel}_2 E$. The fourth element of $H^1(\mathbb{R}, \mathbb{Z}/2\mathbb{Z})$ yields étale algebras whose (A, B) has

$$A = \begin{bmatrix} 1/2 & & \\ & 1 & \\ & & 1/2 \end{bmatrix},$$

a conic with no real points. However, over global fields, it is possible to show that V is Hasse, using the Hasse-Minkowski theorem for conics.

Remark 8.9. Because of the extreme flexibility afforded by general varieties, it is reasonable to suppose that any finite K-Galois module M appears as the point stabilizer of some full composed variety over K. However, we do not pursue this question here.

8.2 Integral models; localization of orbit counts

Let K be a number field and $\mathcal{O}_K$ its ring of integers. Let (V, Γ) be a composed variety, and let $(\mathcal{V}, \mathcal{G})$ be an *integral model,* that is, a pair of a flat separated scheme and a flat algebraic group over $\mathcal{O}_K$ acting on it, equipped with an identification of the generic fiber with (V, Γ). Then $\mathcal{G}(\mathcal{O}_K) \hookrightarrow \Gamma(K)$,

and the $\Gamma(K)$-orbits on $V(K)$ decompose into $\mathcal{G}(\mathcal{O}_K)$-orbits.

Lemma 8.10 (**localization of global class numbers**). *Let $(\mathcal{V}, \mathcal{G})$ be an integral model for a composed variety (V, Γ). For each place v, let*

$$w_v : \mathcal{G}(\mathcal{O}_v)\backslash\mathcal{V}(\mathcal{O}_v) \to \mathbb{C}$$

be a function on the local orbits, which we call a local weighting. *Suppose that:*

(*i*) *(V, Γ) is Hasse.*

(*ii*) *$\mathcal{G}$ has* class number one, *that is, the natural localization embedding*

$$\mathcal{G}(\mathcal{O}_K)\backslash\Gamma(K) \hookrightarrow \bigoplus_v \mathcal{G}(\mathcal{O}_v)\backslash\Gamma(K_v)$$

is surjective.

(*iii*) *For each place v, there are only finitely many orbits of $\mathcal{G}(\mathcal{O}_v)$ on $\mathcal{V}(\mathcal{O}_v)$. This ensures that the* weighted local orbit counter

$$g_{v,w_v} : H^1(K_v, M) \to \mathbb{C}$$
$$\alpha \mapsto \sum_{\substack{\mathcal{G}(\mathcal{O}_{K_v})\gamma\in\mathcal{G}(\mathcal{O}_v)\backslash\Gamma(K_v) \\ \text{such that } \gamma x_\alpha\in\mathcal{V}(\mathcal{O}_v)}} w_v(\gamma x_\alpha)$$

takes finite values. (Here x_α is a representative of the $\Gamma(K_v)$-orbit corresponding to α. If there is no such orbit because V is not full, we take $g_{v,w_v}(\alpha) = 0$.)

(*iv*) *For almost all v, $\mathcal{G}(\mathcal{O}_v)\backslash\mathcal{V}(\mathcal{O}_v)$ consists of at most one orbit in each $\Gamma(K_v)$-orbit, and $w_v = 1$ identically.*

Then the global integral points $\mathcal{V}(\mathcal{O}_K)$ consist of finitely many $\mathcal{G}(\mathcal{O}_K)$-orbits, and the global weighted

orbit count *can be expressed in terms of the* g_{v,w_v} *by*

$$h_{\{w_v\}} \coloneqq \sum_{\mathcal{G}(\mathcal{O}_K)x \in \mathcal{G}(\mathcal{O}_K)\backslash\mathcal{V}(\mathcal{O}_K)} \frac{\prod_v w_v(x)}{|\mathrm{Stab}_{\mathcal{G}(\mathcal{O}_K)}\, x|} = \frac{1}{|H^0(K,M)|} \sum_{\alpha \in H^1(K,M)} \prod_v g_{v,w_v}(\alpha). \tag{50}$$

Proof. Grouping the $\mathcal{G}(\mathcal{O}_K)$-orbits into $\Gamma(K)$-orbits, it suffices to prove that for all $\alpha \in H^1(K,M)$,

$$\sum_{\mathcal{G}(\mathcal{O}_K)x \subseteq \Gamma(K)x_\alpha} \frac{\prod_v w_v(x)}{|\mathrm{Stab}_{\mathcal{G}(\mathcal{O}_K)}\, x|} = \frac{1}{|H^0(K,M)|} \prod_v g_{v,w_v}(\alpha). \tag{51}$$

If there is no x_α, the left-hand side is zero by definition, and at least one of the $g_{v,w_v}(\alpha)$ is also zero since V is Hasse. So we fix an x_α. The right-hand side of (51), which is finite by hypothesis (iv) since α is unramified almost everywhere, can be written as

$$\frac{1}{|H^0(K,M)|} \sum_{\{\mathcal{G}(\mathcal{O}_v)\gamma_v\}_v} \prod_v w_v(\gamma_v x_\alpha),$$

the sum being over systems of $\gamma_v \in \Gamma(K_v)$ such that $\gamma_v x_\alpha$ is $\mathcal{O}_v$-integral. Since $\mathcal{G}$ has class number one, each such system glues uniquely to a global orbit $\mathcal{G}(\mathcal{O}_K)\gamma, \gamma \in \Gamma(K)$, for which γx_α is $\mathcal{O}_v$-integral for all v, that is, $\mathcal{O}_K$-integral. Thus the right-hand side of (51) is now transformed to

$$\frac{1}{|H^0(K,M)|} \sum_{\substack{\mathcal{G}(\mathcal{O}_K)\gamma \\ \gamma x_\alpha \in \mathcal{V}(\mathcal{O}_K)}} \prod_v w_v(\gamma_v x_\alpha).$$

Now each γ corresponds to a term of the left-hand side of (51) under the map

$$\mathcal{G}(\mathcal{O}_K)\backslash\Gamma(K) \to \mathcal{G}(\mathcal{O}_K)\backslash V(K)$$

$$\mathcal{G}(\mathcal{O}_K)\gamma \mapsto \mathcal{G}(\mathcal{O}_K)\gamma x_\alpha.$$

The fiber of each $\mathcal{G}(\mathcal{O}_K)x$ has size

$$[\mathrm{Stab}_{\Gamma(K)}\, x : \mathrm{Stab}_{\mathcal{G}(\mathcal{O}_K)}\, x] = \frac{|H^0(K,M)|}{|\mathrm{Stab}_{\mathcal{G}(\mathcal{O}_K)}\, x|}.$$

So we match up one term of the left-hand side, having value

$$\prod_v w_v(x)/|\mathrm{Stab}_{\mathcal{G}(\mathcal{O}_K)}\, x|,$$

with $|H^0(K,M)|/|\mathrm{Stab}_{\mathcal{G}(\mathcal{O}_K)}\, x|$-many elements on the right-hand side. In view of the outlying factor $1/|H^0(K,M)|$, this completes the proof. ■

8.3 Fourier analysis of the local and global Tate pairings

We now introduce the main innovative technique of this thesis: Fourier analysis of local and global Tate duality. In structure we are indebted to Tate's celebrated thesis [55], in which he

1. constructs a perfect pairing on the additive group of a local field K, taking values in the unit circle $\mathbb{C}^{N=1}$, and thus furnishing a notion of Fourier transform for $\mathbb{C}$-valued L^1 functions on K;

2. derives thereby a pairing and Fourier transform on the adele group $\mathbb{A}_K$ of a global field K;

3. proves that the discrete subgroup $K \subseteq \mathbb{A}_K$ is a self-dual lattice and that the Poisson summation formula

$$\sum_{x\in K} f(x) = \sum_{x\in K} \hat{f}(x) \tag{52}$$

holds for all f satisfying reasonable integrability conditions.

In this paper, we work not with the additive group K but with a Galois cohomology group $H^1(K,M)$. The needed theoretical result is *Poitou-Tate duality*, a nine-term exact sequence of which the middle three terms are of main interest to us:

$$(\text{finite kernel}) \to H^1(K,M) \to \bigoplus_v{}' H^1(K_v,M) \to H^1(K,M')^\vee \to (\text{finite cokernel}).$$

This can be interpreted as saying that $H^1(K,M)$ and $H^1(K,M')$ (where $M' = \mathrm{Hom}(M,\mu)$ is the

Tate dual) map to dual lattices in the respective adelic cohomology groups

$$H^1(\mathbb{A}_K, M) = \bigoplus_v{}' H^1(K_v, M) \quad \text{and} \quad H^1(\mathbb{A}_K, M') = \bigoplus_v{}' H^1(K_v, M'),$$

which are mutually dual under the product of the local Tate pairings

$$\langle \{\alpha_v\}, \{\beta_v\} \rangle = \prod_v \langle \alpha_v, \beta_v \rangle \in \mu.$$

Here, for K a local field, the local Tate pairing is given by the cup product

$$\langle \bullet, \bullet \rangle : H^1(K, M) \times H^1(K, M') \to H^2(K, \mu) \cong \mu.$$

It is well known that this pairing is perfect. (The Brauer group $H^2(K, \mu)$ is usually described as being $\mathbb{Q}/\mathbb{Z}$ but, having no need for a Galois action on it, we identify it with μ to avoid the need to write an exponential in the Fourier transform.) Now, for any sufficiently nice function $f : H^1(\mathbb{A}_K, M) \to \mathbb{C}$ (locally constant and compactly supported is more than enough), we have Poisson summation

$$\sum_{\alpha \in H^1(K,M)} f(\alpha) = c_M \sum_{\beta \in H^1(K,M')} \hat{f}(\beta)$$

for some constant c_M which we think of as the covolume of $H^1(K, M)$ as a lattice in the adelic cohomology. (In fact, by examining the preceding term in the Poitou-Tate sequence, $H^1(K, M)$ need not inject into $H^1(\mathbb{A}_K, M)$, but maps in with finite kernel; but this subtlety can be absorbed into the constant c_M.)

We apply Poisson summation to the local orbit counters g_v defined in the preceding subsection and get a very general reflection theorem.

Definition 8.11. Let K be a local field. Let $(V^{(1)}, \Gamma^{(1)})$ and $(V^{(2)}, \Gamma^{(2)})$ be a pair of composed varieties over K whose associated point stabilizers $M^{(1)}$, $M^{(2)}$ are Tate duals of one another, and

let $(\mathcal{V}^{(i)}, \mathcal{G}^{(i)})$ be an integral model of $(V^{(i)}, \Gamma^{(i)})$. Two weightings on orbits

$$w^{(i)} : \mathcal{G}(\mathcal{O}_K)\backslash\mathcal{V}(\mathcal{O}_K) \to \mathbb{C}$$

are called (mutually) *dual* with *duality constant* $c \in \mathbb{Q}$ if their local orbit counters $g_{w^{(i)}}$ are mutual Fourier transforms:

$$g^{(2)} = c \cdot \hat{g}^{(1)}. \tag{53}$$

where the Fourier transform is scaled by

$$\hat{f}(\beta) = \frac{1}{H^0(K, M)} \sum_{\alpha \in H^1(K,M)} f(\alpha).$$

An equation of the form (53) is called a *local reflection theorem.* If the constant weightings $w^{(i)} = 1$ are mutually dual, we say that the two integral models $(\mathcal{V}^{(i)}, \mathcal{G}^{(i)})$ are *naturally dual.*

Theorem 8.12 (**local-to-global reflection engine**)**.** *Let K be a number field. Let $(V^{(1)}, \Gamma^{(1)})$ and $(V^{(2)}, \Gamma^{(2)})$ be a pair of composed varieties over K whose associated point stabilizers $M^{(1)}$, $M^{(2)}$ are Tate duals of one another. Let $(\mathcal{V}^{(i)}, \mathcal{G}^{(i)})$ be an integral model for each $(V^{(i)}, \Gamma^{(i)})$, and let*

$$w_v^{(i)} : \mathcal{G}^{(i)}(\mathcal{O}_v)\backslash\mathcal{V}^{(i)}(\mathcal{O}_v) \to \mathbb{C}$$

be a local weighting on each integral model. Suppose that each integral model and local weighting satisfies the hypotheses of Lemma 8.10, and suppose that at each place v, the two integral models are dual with some duality constant $c_v \in \mathbb{Q}$. Then the weighted global class numbers are in a simple ratio:

$$h_{\left\{w_v^{(2)}\right\}} = \prod_v c_v \cdot h_{\left\{w_v^{(1)}\right\}}.$$

Proof. By Lemma 8.10,

$$h_{\left\{w_v^{(i)}\right\}} = \frac{1}{|H^0(K, M^{(i)})|} \sum_{\alpha \in H^1(K,M^{(i)})} \prod_v g_{v,w_v^{(i)}}(\alpha).$$

At almost all v, each $g_{v,w_v^{(i)}}$ is supported on the unramified cohomology, and must be constant there because otherwise its Fourier transform would not be supported on the unramified cohomology. However, $g_{v,w_v^{(i)}}$ cannot be identically 0 because of the existance of a global basepoint. So for such v,

$$g_{v,w_v^{(i)}} = \mathbf{1}_{H^1_{\mathrm{ur}}(K,M^{(i)})} \quad \text{and} \quad c_v = 1.$$

In particular, the product $\prod_v g_{v,w_v^{(i)}}$ is a locally constant, compactly supported function on $H^1(K,\mathbb{A}_K)$, which is more than enough for Poisson summation to be valid.

Since the pairing between the adelic cohomology groups $H^1(\mathbb{A}_K, M^{(i)})$ is made by multiplying the local Tate pairings, a product of local factors has a Fourier transform with a corresponding product expansion:

$$\widehat{\prod_v g_{v,w_v^{(1)}}} = \prod_v \hat{g}_{v,w_v^{(1)}} = \prod_v c_v \cdot \prod_v g_{v,w_v^{(2)}}.$$

We then apply Poisson summation to get a formula for the ratio of the global weighted class numbers:

$$h_{\left\{w_v^{(2)}\right\}} = \frac{|H^0(K,M^{(1)})|}{|H^0(K,M^{(2)})|} \cdot c_{M^{(1)}} \prod_v c_v \cdot h_{\left\{w_v^{(1)}\right\}}.$$

This gives the desired identity, except for determining the scalar c_M, which depends only on the Galois module $M = M^{(1)}$. This can be ascertained by applying Poisson summation to just one function $f : H^1(\mathbb{A}_K, M) \to \mathbb{C}$ for which either side is nonzero. The easiest such f to think of is the characteristic function of a compact open box

$$X = \prod_v X_v,$$

with $X_v = H^1(K,M)$ for almost all v. Such a specification is often called a *Selmer system,* and the sum

$$\sum_{\alpha \in H^1(K,M)} \mathbf{1}_{\alpha_v \in X_v \forall v}$$

is the order of the *Selmer group* $\mathrm{Sel}(X)$ of global cohomology classes obeying the specified local

conditions. Poisson summation becomes a formula for the ratio $|\mathrm{Sel}(X)|/|\mathrm{Sel}(X^\perp)|$ as a product of local factors, commonly known as the *Greenberg-Wiles formula*. By appealing to any of the known proofs of the Greenberg-Wiles formula (see Darmon, Diamond, and Taylor [17, Theorem 2.19] or Jorza [29, Theorem 3.11]), we pin down the value

$$c_M = \frac{|H^0(K, M')|}{|H^0(K, M)|}.$$ ■

At certain points in this paper, it will be to our advantage to consider multiple integral models at once. The following theorem has sufficient generality.

Theorem 8.13 (**local-to-global reflection engine: general version**). *Let K be a number field. Let $(V^{(1)}, \Gamma^{(1)})$ and $(V^{(2)}, \Gamma^{(2)})$ be a pair of composed varieties over K whose associated point stabilizers $M^{(1)}$, $M^{(2)}$ are Tate duals of one another. For each place v of K, let*

$$\left\{(\mathcal{V}^{(i)}_{j_v}, \mathcal{G}^{(i)})_{j_v} : j_v \in J^{(i)}_v\right\}$$

be a family of integral models for each ($V^{(i)}$ indexed by some finite set $J^{(i)}_v$, and let

$$w^{(i)}_{j_v} : \mathcal{G}^{(i)}(\mathcal{O}_v)\backslash\mathcal{V}^{(i)}(\mathcal{O}_v) \to \mathbb{C}$$

be a weighting on the orbits of each integral model. Similarly to Lemma 8.10 and Theorem 8.12, assume that

(*i*) *(V, Γ) is Hasse.*

(*ii*) *For each combination of indices $j = (j_v)_v$, $j_v \in J^{(i)}_v$, the local integral models $(\mathcal{V}^{(i)}_{j_v}, \mathcal{G}^{(i)}_{j_v})$ glue together to form a global integral model $(\mathcal{V}^{(i)}_j, \mathcal{G}^{(i)}_j)$. (Since the integral models are equipped with embeddings $\mathcal{V}^{(i)}_{j_v} \to V^{(i)}_v$, the gluing is seen to be unique; and its existence will be obvious in all the examples we consider.)*

(*iii*) *Each such $\mathcal{G}^{(i)}_j$ has class number one.*

(iv) *For each j_v, there are only finitely many orbits of $\mathcal{G}_{j_v}^{(i)}$ on $\mathcal{V}_{j_v}^{(i)}$, ensuring that the local orbit counter $g_{j_v,w_{j_v}}$ takes finite values.*

(v) *For almost every v, the index set $J_v = \{j_v\}$ has just one element, with the corresponding integral model $\mathcal{V}_{j_v}^{(i)}$ consisting of at most one orbit in each $\Gamma(K_v)$-orbit, and $w_{j_v}^{(i)} = 1$ identically.*

(vi) *At each v, we have a local reflection theorem*

$$\sum_{j_v \in J_v^{(1)}} \hat{g}_{j_v,w_{j_v}} = \sum_{j_v \in J_v^{(2)}} g_{j_v,w_{j_v}}.$$

Then the class numbers of the global integral models $(\mathcal{V}_j^{(i)}, \mathcal{G}_j^{(i)})$ with respect to the weightings $w_j^{(i)} = \prod_v w_{j_v}^{(i)}$ satisfy global reflection:

$$\sum_{j \in \prod_v J_v^{(1)}} h\left(\mathcal{V}_j^{(1)}, w_j^{(1)}\right) = \sum_{j \in \prod_v J_v^{(2)}} h\left(\mathcal{V}_j^{(2)}, w_j^{(2)}\right).$$

Proof. Except for complexities of notation, the proof closely follows the preceding one. The first five hypotheses ensure that each global integral model $\left(\mathcal{V}_j^{(i)}, \mathcal{G}_j^{(i)}\right)$ satisfies the hypotheses of Lemma 8.10, so its class number is representable as a sum over the lattice of global points in adelic cohomology:

$$h\left(\mathcal{V}_j^{(i)}, w_j^{(i)}\right) = \frac{1}{|H^0(K, M^{(i)})|} \sum_{\alpha \in H^1(K,M^{(i)})} \prod_v g_{j_v,w_{j_v}}(\alpha).$$

When we sum over all j, the contributions of each α factor to give

$$\sum_{j \in \prod_v J_v^{(i)}} h\left(\mathcal{V}_j^{(i)}, w_j^{(i)}\right) = \frac{1}{|H^0(K, M^{(i)})|} \sum_{\alpha \in H^1(K,M^{(i)})} \prod_v \sum_{j_v \in J_v^{(i)}} g_{j_v,w_{j_v}}(\alpha).$$

But by the assumed local reflection identity, we have

$$\left(\prod_v \sum_{j_v \in J_v^{(1)}} g_{j_v,w_{j_v}}\right)^{\widehat{}} = \prod_v \left(\sum_{j_v \in J_v^{(1)}} g_{j_v,w_{j_v}}\right)^{\widehat{}} = \prod_v \sum_{j_v \in J_v^{(2)}} g_{j_v,w_{j_v}}.$$

So we get the desired identity from Poisson summation. The scale factor was determined in proving

the previous theorem. ■

Remark 8.14. Unlike in the previous theorem, we have not included duality constants c_v, but the same effect can be obtained by taking the appropriate constant for the weighting $w_j^{(i)}$.

8.3.1 Examples

As one might guess, there are many pairs of composed varieties whose point stabilizers $M^{(1)}$, $M^{(2)}$ are Tate duals; and, given any integral models, it is usually possible to concoct weights $w^{(i)}$ that are mutually dual, thereby getting reflection theorems from Theorem 8.12. More noteworthy is when a pair of integral models are *naturally* dual at all finite places. Even more significant is if a group $\mathcal{G}$ acts on a large variety Λ, leaving certain functions I on Λ invariant, such that *every* level set of I is an integral model for a composed variety with natural duality. This is the case for O-N.

We have found three families of naturally dual composed varieties of this sort:

Γ	Λ	I	Parametrizes	M
$\left\{\begin{bmatrix}\lambda & t\\ 0 & \lambda^{-2}\end{bmatrix}\right\} \subset \mathrm{GL}_2$	Quadratic forms, $\mathrm{Sym}^2(2)$	$a(b^2-4ac)$	?	$\mathcal{C}_2$
SL_2	Cubic forms, $\mathrm{Sym}^3(2)$	Discriminant	Cubic rings / 3-torsion in quadratic rings	$\mathcal{C}_3$
SL_3	Pairs of ternary quadratic forms, $\mathrm{Sym}^2(3)^{\oplus 2}$	Cubic resolvent	Quartic rings / 2-torsion in cubic rings	$\mathcal{C}_2 \times \mathcal{C}_2$

These three representations will be considered in detail in Section 9, Part V, and Parts VI–VII, respectively. In each case, there is a local reflection that pairs two integral models of V over $\mathcal{O}_K$ which look alike over K.

Remark 8.15. In the latter two cases, the integral models are *dual* under an identification of V with its dual V^* (which are isomorphic, up to an outer automorphism of $\Gamma = \mathrm{SL}_3$ in the last case). But

in the quadratic case, V^* decomposes into $\bar{K}$-orbits according to a different invariant $J = a/\Delta^2$, and the integral orbit counts are infinite, so the alignment with duals in the classical sense must be considered at least partly coincidental.

Closely related to the quartic rings example is the action of SL_2 on binary quartic forms $\mathrm{Sym}^4(2)$. Here, the orbits are parametrized by a subset of a cohomology group $H^1(K, M)$ ($M \cong \mathcal{C}_2 \times \mathcal{C}_2$ as a group) cut out by a quadratic relation. Nevertheless, we will state some interesting reflection identities for these spaces in Section 13.1.

More generally, we can consider the space Λ of pairs (A, B) of n-ary quadratic forms, on which $\Gamma = \mathrm{SL}_n$ acts preserving a binary n-ic resolvent

$$I = \det(Ax - By).$$

Although we do not consider it in this paper, preliminary investigations suggest that its integral models are naturally dual to one another for n odd, yielding a corresponding global reflection theorem (Conjecture 2.13). This composed variety figures prominently in the study of Selmer elements of hyperelliptic curves [6].

On the other hand, the following families of composed varieties do *not* admit natural duality:

- The action of $\mathbb{G}_m$ on the punctured affine line by multiplication by nth powers. The orbits do parametrize $H^1(K, \mu_m) = K^\times/(K^\times)^n$. But over a local or global field, there are infinitely many integral orbits in each rational orbit.

- The action of SO_2 (the group of rotations preserving the quadratic form $x^2 + xy + y^2$) on binary cubic forms of the shape

  $$f(x, y) = ax^3 + bx^2y + (-3a + b)xy^2 + ay^3$$

  which is symmetric under the threefold shift $x \mapsto y$, $y \mapsto -x - y$. This representation is used by Bhargava and Shnidman [9] to parametrize *cyclic* cubic rings, that is, those with an

automorphism of order 3. The reason for failure of natural duality is quite simple. Within the representation over $\mathbb{Z}_p$ for $p \equiv 1 \mod 3$, take the composed variety where the discriminant is p^2. The cohomology group $H^1(\mathbb{Q}_p, \mathbb{Z}/3\mathbb{Z})$ is isomorphic to $\mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}$, and a function f on it may be written as a matrix

$f(0)$	$f(\alpha)$	$f(2\alpha)$
$f(\beta)$	$f(\alpha+\beta)$	$f(2\alpha+\beta)$
$f(2\beta)$	$f(\alpha+2\beta)$	$f(2\alpha+2\beta)$

in which the zero-element and the unramified cohomology $\langle\alpha\rangle$ are marked off by dividers.

The six *ramified* cohomology elements each have one integral orbit, corresponding to the maximal order; the three *unramified* cohomology elements—the zero element for $\mathbb{Q}_p^3$, and the other two for the degree-3 unramified field extension in its two orientations—all have *no* integral orbits, because the three orders

$$\{(x_1, x_2, x_3) \in \mathbb{Z}_p^3 : x_i \equiv x_j \mod p\}$$

are all asymmetric under the threefold automorphism of $\mathbb{Z}_p^3$. So we get a local orbit counter

0	0	0
1	1	1
1	1	1

whose Fourier transform

2	−1	−1
0	0	0
0	0	0

has mixed signs and thus cannot be the local orbit counter of any composed variety. Similar obstructions to natural duality have obtained in many of the composed varieties parametrizing

rings with automorphisms found by Gundlach [25].

Part IV

Reflection theorems: first examples

The remainder of this thesis will be devoted to stating and proving explicit reflection theorems for various objects of interest.

9 Quadratic forms by superdiscriminant

We begin with the simplest Galois module $M \cong \mathbb{Z}/2\mathbb{Z}$.

There are many full composed varieties whose point stabilizer is of order 2, and the one we take is, to say the least, one of the more unexpected. The group GL_2 acts on the space

$$V = \mathrm{Sym}^2(2) = \{ax^2 + bxy + cy^2 : a, b, c \in \mathbb{G}_a\}$$

of binary quadratic forms in the natural way. Let Γ be the algebraic subgroup, defined over $\mathbb{Z}$, of elements of a peculiar form:

$$\left\{ \begin{bmatrix} u & t \\ 0 & u^{-2} \end{bmatrix} : u \in \mathbb{G}_m, t \in \mathbb{G}_a \right\}.$$

Abstractly, this group is a certain semidirect product of $\mathbb{G}_a$ by $\mathbb{G}_m$. As is not too hard to verify, the restriction of Λ to Γ has a single polynomial invariant, the *superdiscriminant*

$$I := aD = a(b^2 - 4ac).$$

Because of the asymmetry between x and y, there is no harm in writing forms in V inhomogeneously as $f(x) = ax^2 + bx + c$, as was done in Section 2.

Then the variety

$$V(I) = \{f \in V : I(f) = I\}$$

is full composed. We take the basepoint

$$f_0 = Ix^2 + \frac{1}{4I}$$

of discriminant 1. Then the rational orbits are parametrized by $D = b^2 - 4ac \in K^\times/(K^\times)^2$ consistent with the parametrization of their splitting fields via Kummer theory.

Remark 9.1. The group Γ is not reductive, that is, does fit into the classical Dynkin-diagram parametrization for Lie groups. Non-reductive groups are decidedly in the minority within the whole context of using orbits to parametrize arithmetic objects, but they have occurred before: Altuğ, Shankar, Varma, and Wilson [1] count D_4-fields using orbits of pairs of ternary quadratic forms under a certain nonreductive subgroup of $\mathrm{GL}_2 \times \mathrm{SL}_3$.

Now we introduce integral models. Suppose $\mathcal{O}_K \subseteq K$ is a PID with field of fractions K. If $\tau \in \mathcal{O}_K$ divides 2, then

$$V_\tau = \{ax^2 + bx + c : a, c \in \mathcal{O}_K, \tau \mid b\}$$

is a $\mathrm{GL}_2(\mathcal{O}_K)$-invariant lattice in V. For any $I \in \mathcal{O}_K$, we can take $(\mathcal{V}, \mathcal{G}) = (V_\tau(I), \Gamma(\mathcal{O}_K))$ as an integral model for $V(I)$. For it to have any integral points, we must have $\tau^2 \mid I$.

Our first local reflection theorem says that each of these integral models has a natural dual.

Theorem 9.2 ("Local Quadratic O-N"). *Let K be a non-archimedean local field,* $\operatorname{char} K \neq 2$. *For $I, \tau \in \mathcal{O}_K$ elements dividing 2, the integral models*

$$V_\tau(I) \quad \textit{and} \quad V_{2\tau^{-1}}\left(4\tau^{-4}I\right)$$

are naturally dual with scale factor the absolute norm $N(\tau) = |\mathcal{O}_K/\tau\mathcal{O}_K|$. In other words, the local orbit counters are related by

$$\hat{g}_{V_\tau(I)} = N(\tau) \cdot g_{V_{2\tau^{-1}}(4\tau^{-4}I)}. \tag{54}$$

Proof. We prove this result by explicitly computing the local orbit counter $g_{V_\tau(I)}$, which sends each $[D] \in K^\times/(K^\times)^2 \cong H^1(K, \mathbb{Z}/2\mathbb{Z})$ to the number of cosets $[\gamma] \in \Gamma(\mathcal{O}_K)\backslash\Gamma(K)$ such that $\gamma v_0 \in V_\tau(I)(\mathcal{O}_K)$, where v_0 is an arbitrary vector in $V(K)$ with $I(v_0) = I$ and $D(v_0) = D$. Let $t = v(\tau)$ and $e = v(2)$; we have $e > 0$ exactly when K is 2-adic, and

$$0 \leq t \leq e.$$

A coset $[\gamma]$ is specified by two pieces of information. First is the valuation $v(u)$ of the diagonal elements; this is equivalent to specifying $v(D)$ and $v(a)$, where, as is natural we set

$$\gamma v_0 = ax^2 + bxy + cy^2 \quad \text{and} \quad D = b^2 - 4ac.$$

Second, we specify t modulo the appropriate integral sublattice. If (as we may assume) $v(u) = 0$, then t is defined modulo 1, which is the same as specifying b modulo $2a$. So the problem of computing $g_{V_\tau(I)}$ devolves onto computing how many $b \in \tau\mathcal{O}_K$, up to translation by $2a$, yield an integral value for

$$c = \frac{b^2 - D}{4a};$$

that is, we must solve the quadratic congruence

$$b^2 \equiv D \mod 4a. \tag{55}$$

The answer, in general, depends on how close D is to being a square in K. So we will express our answer in terms of the *level spaces* introduced in Theorem 7.1. Here the level of a coclass $[\alpha], \alpha \in K^\times$, is defined in terms of the discriminant of $K[\sqrt{\alpha}]$, which, by Theorem 7.3, can be computed from the minimal distance $|\alpha - 1|$, over all rescalings of α by squares. The level spaces thus correspond to

the natural filtration of $K^\times/(K^\times)^2$ by neighborhoods of 1:

$$\mathcal{L}_i = \begin{cases} K^\times/(K^\times)^2, & i = -1 \\ \{[\alpha] \in \mathcal{O}_K^\times/(\mathcal{O}_K^\times)^2 : \alpha \in 1 + \pi^{2e-2i}\mathcal{O}_K\}, & 0 \le i \le e \\ \{1\}, & i = e+1. \end{cases}$$

Let L_i be the characteristic function of $\mathcal{L}_i$. By Corollary 7.2, the Fourier transform of each L_i is a scalar multiple of L_{e-i}.

We now claim that, if we fix $v(I)$ and $v(a)$ (and hence $v(D)$), then the contribution of all solutions of (55) to $g_{\tau,I}$ can be expressed as a linear combination of the L_i. The basic idea, which will be a recurring one, is to group the solutions into *families* that have a constant number of solutions over some subset $S \subseteq K^\times/(K^\times)^2$. The subset S will be called the *support* of the family, and the number of solutions for each $D \in S$ will be called the *thickness* of the family.

If $v(D) \ge v(4a)$, then (55) simplifies to $4a|b^2$, that is,

$$v(b) \ge \left\lceil e + \frac{1}{2}v(a) \right\rceil.$$

Since we are counting values of b modulo $2a$, the number of solutions is simply

$$q^{(e+v(a))-\lceil e-\frac{1}{2}v(a)\rceil} = q^{\lfloor \frac{1}{2}v(a)\rfloor}.$$

We get a family with this thickness, supported on either $\mathcal{L}_0$ or $\mathcal{L}_{-1} \setminus \mathcal{L}_0$ according as $v(D)$ is even or odd.

If $v(D) < v(4a)$, then b^2 must be actually able to cancel at least the leading term of D to get any solutions. In particular, $v(D)$ must be even. Let $\tilde{D} = D/\pi^{v(D)}$, and let $\tilde{b} = b/\pi^{\frac{1}{2}v(D)}$, so $\tilde{b}$ must be a unit satisfying

$$\tilde{b}^2 \equiv \tilde{D} \mod \frac{4a}{D}. \tag{56}$$

Let $m = v(4a/D)$. If $m \ge 2e+1$, a unit is a square modulo π^m only if it is a square outright, so

we get a family supported just on the trivial class $1 \in K^\times/(K^\times)^2$. Otherwise, we have $1 \le m \le 2e$, and the support is $L_{\lceil m/2 \rceil}$. The corresponding thicknesses are easy to compute. The $\tilde{b}$ satisfying (56) form a fiber of the group homomorphism

$$\phi = \bullet^2 \colon \left(\mathcal{O}_K/\pi^{v(2a)-\frac{1}{2}v(D)}\right)^\times \to \left(\mathcal{O}_K/\pi^{v(4a)-v(D)}\right)^\times,$$

and the cokernel of this homomorphism has size $[\mathcal{L}_0 : \mathcal{L}_i]$, so the thickness is

$$\begin{aligned}
|\ker \phi| &= [\mathcal{L}_0 : \mathcal{L}_i] \cdot \frac{\left|\left(\mathcal{O}_K/\pi^{v(2a)-\frac{1}{2}v(D)}\right)^\times\right|}{\left|\left(\mathcal{O}_K/\pi^{v(4a)-v(D)}\right)^\times\right|} \\
&= [\mathcal{L}_0 : \mathcal{L}_i] \cdot \frac{\left(1-\frac{1}{q}\right) q^{v(2a)-\frac{1}{2}v(D)}}{\left(1-\frac{1}{q}\right) q^{v(4a)-v(D)}} \\
&= [\mathcal{L}_0 : \mathcal{L}_i] \cdot q^{\frac{1}{2}v(D)-e} \\
&= \begin{cases} q^{\frac{1}{2}v(D)-e+\lceil m/2 \rceil} = q^{\lfloor v(a)/2 \rfloor}, & 1 \le m \le 2e \\ 2q^{\frac{1}{2}v(D)}, & m \ge 2e+1. \end{cases}
\end{aligned}$$

We have not mentioned the condition $b \in (\tau)$, because it is equivalent to $v(D) \ge 2v(\tau)$, and eliminates some families, leaving the others intact.

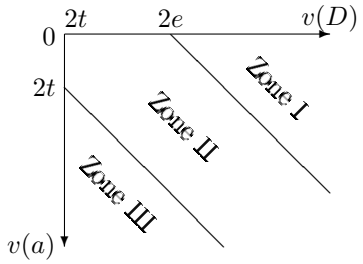
By way of illustration, we tabulate the contributions to $g_{\tau,I}$ in the example where $e = 2$. It is already easy to check many examples of Theorem 9.2.

$\downarrow v(a); v(D) \to$	0	1	2	3	4	5	6	7	8
0	L_2		L_1		L_0	$L_{-1} - L_0$	L_0	$L_{-1} - L_0$	L_0
1	L_3		L_1		L_0	$L_{-1} - L_0$	L_0	$L_{-1} - L_0$	L_0
2	L_3		qL_2		qL_1		qL_0	$q\,(L_{-1} - L_0)$	qL_0
3	L_3		qL_3		qL_1		qL_0	$q\,(L_{-1} - L_0)$	qL_0
4	L_3		qL_3		q^2L_2		q^2L_1		q^2L_0

We have shown the subdivision of the table into three *zones* given by the inequalities:

- Zone I: $v(D) \geq v(4a)$
- Zone II: $v(a) < v(D) \leq v(4a)$
- Zone III: $v(a) > v(D)$.

(A more general definition of a zone will be given later.) In general, the shapes of these zones, together with the needed condition $v(D) \geq 2t$, will look as follows:



The feature to be noted is that, under the transformation $t \mapsto e - t$, the shape of Zone II is flipped about a diagonal line and Zones I and III are interchanged. This will be the basis for our proof of Theorem 9.2; but there will be irregularities owing to the floor functions in the formulas and the fact that $\mathcal{L}_{-1} \setminus \mathcal{L}_0$, instead of $\mathcal{L}_{-1}$, appears as a support.

There are two ways to finish the proof. One is to establish a bijection of families, as outlined in the previous paragraph, so that L_i and L_{e-i} are interchanged as supports and all the thicknesses correspond appropriately. Such an approach will be used for cubic O-N in Section 11.3. The other is to verify the local reflection computationally, by means of a generating function. We choose the second, admittedly less elegant, method, mainly because it shows, in a context simple enough to be worked by hand, transformations that we will relegate to a computer in the succeeding sections.

Let

$$F(Z) = \sum_{n \geq 0} g_{\tau,\pi^n} Z^n,$$

a formal power series whose coefficients are functions of $D \in K^\times/(K^\times)^2$. We write $F = F_{\mathrm{I}} + F_{\mathrm{II}} + F_{\mathrm{III}}$, where $F_{\mathfrak{X}}$ is the contribution coming from Zone $\mathfrak{X}$ in the preceding analysis.

Writing $i = v(a)$ and $d = v(D)$, we proceed to compute

$$F_{\mathrm{I}} = \sum_{i\geq 0} \sum_{d\geq 2e+i+1} \begin{cases} q^{\lfloor i/2 \rfloor} L_0 Z^{i+d}, & d \text{ even} \\ q^{\lfloor i/2 \rfloor} (L_{-1} - L_0) Z^{i+d}, & d \text{ odd} \end{cases}$$

$$= Z^{2e} \sum_{i\geq 0} \sum_{d\geq i+1} \begin{cases} q^{\lfloor i/2 \rfloor} L_0 Z^{i+d}, & d \text{ even} \\ q^{\lfloor i/2 \rfloor} (L_{-1} - L_0) Z^{i+d}, & d \text{ odd.} \end{cases}$$

Splitting $i = 2i_f + i_p$, where $0 \leq i_p \leq 1$, and likewise $d = 2d_f + d_p$, we get

$$\begin{aligned} F_{\mathrm{I}} &= Z^{2e} \sum_{i_p=0}^{1} \sum_{i_f \geq 0} \left(\sum_{d \geq 2i_f + i_p + 1} q^{i_f} (-1)^d L_0 Z^{d+2i_f+i_p} + \sum_{d_f \geq i_f} q^{i_f} L_{-1} Z^{2d_f+2i_f+i_p+1} \right) \\ &= Z^{2e} \sum_{i_p=0}^{1} \sum_{i_f \geq 0} \left(\frac{q^{i_f} (-1)^{i_p} L_0 Z^{4i_f+2i_p+1}}{1+Z} + \frac{q^{i_f} Z^{4i_f+i_p+1} L_{-1}}{1-Z^2} \right) \\ &= Z^{2e} \sum_{i_p=0}^{1} \left(\frac{(-1)^{i_p} Z^{2i_p} L_0}{(1+Z)(1-qZ^4)} + \frac{Z^{i_p+1} L_{-1}}{(1-Z^2)(1-qZ^4)} \right) \\ &= Z^{2e} \left(\frac{(1-Z^2)}{(1+Z)(1-qZ^4)} L_0 + \frac{Z(1+Z)}{(1-Z^2)(1-qZ^4)} L_{-1} \right) \\ &= \frac{Z^{2e}(1-Z)}{1-qZ^4} L_0 + \frac{Z^{2e+1}}{(1-Z)(1-qZ^4)} L_{-1}. \end{aligned}$$

For Zone II, which appears only when $e > 0$, the most sensible way to evaluate the sum

$$F_{\mathrm{II}} = \sum_{i\geq 0} \sum_{\substack{i \leq d < i+2e \\ d \geq 2t \\ d \text{ even}}} q^{e + \lfloor \frac{i}{2} \rfloor - \frac{d}{2}} L_{e+\lfloor \frac{i}{2} \rfloor - \frac{d}{2}} Z^{i+d}$$

is to group terms with the same level L_j. We have $j = e + \lfloor \frac{i}{2} \rfloor - \frac{d}{2}$, so the values of i and j determine d. The condition $d \geq 2t$ reduces to $i \geq 2(j+t-e)$; the other condition $i \leq d < i+2e$ is automatically satisfied if $1 \leq j \leq e-1$, while if $j = 0$ or $j = e$, we must have i odd or i even respectively. For

$1 \le j \le e-1$, the L_j-piece of F_{II} is therefore

$$\begin{aligned}
&\sum_{i \ge \max\{0,2(j+t-e)\}} q^{\lfloor i/2 \rfloor} L_j Z^{i+2\left(e+\left\lfloor \frac{i}{2} \right\rfloor -2j\right)} \\
&= \sum_{i_p=0}^{1} \sum_{i_f \ge \max\{0,j+t-e\}} q^{i_f} Z^{4i_f+i_p+2e-2j} L_j \\
&= \left(\sum_{i_p=0}^{1} Z^{i_p} \right) \left(\sum_{i_f \ge \max\{0,j+t-e\}} \left(qZ^4\right)^{i_f} \right) Z^{2e-2j} L_j \\
&= \frac{(1+Z)\left(qZ^4\right)^{\max\{0,j+t-e\}}}{1-qZ^4} \cdot Z^{2e-2j} L_j .
\end{aligned}$$

For $j = 0$ and $j = e$, since i_p can only take one of its two values, the initial factor $1 + Z$ is to be replaced by Z and 1 respectively. Finally, Zone III presents no particular difficulties:

$$\begin{aligned}
F_{\mathrm{III}} &= \sum_{\substack{d \ge 2t \\ d \text{ even}}} \sum_{i \ge d+1} 2q^{d/2} L_{e+1} Z^{i+d} \\
&= 2 \sum_{\substack{d \ge 2t \\ d \text{ even}}} q^{d/2} \cdot \frac{Z^{2d+1}}{1-Z} \cdot L_{e+1} \\
&= \frac{2q^s Z^{4t+1}}{(1-Z)(1-qZ^4)} L_{e+1} .
\end{aligned}$$

Summing up, we get for $e \ge 1$ (the case $e = 0$ can be handled similarly)

$$\begin{aligned}
F &= F_{\mathrm{I}} + F_{\mathrm{II}} + F_{\mathrm{III}} \\
&= \frac{Z^{2e+1}}{(1-Z)(1-qZ^4)} L_{-1} + \frac{Z^{2e}(1-Z)}{1-qZ^4} L_0 + \frac{Z^{2e+1}}{1-qZ^4} L_0 + \sum_{1 \le j \le e-1} \frac{(1+Z)\left(qZ^4\right)^{\max\{0,j+t-e\}}}{1-qZ^4} \cdot Z^{2e-2j} L_j \\
&\quad + \frac{\left(qZ^4\right)^t}{1-qZ^4} L_e + \frac{2q^s Z^{4t+1}}{(1-Z)(1-qZ^4)} L_{e+1} \\
&= \frac{Z^{2e+1}}{(1-Z)(1-qZ^4)} L_{-1} + \frac{Z^{2e}}{1-qZ^4} L_0 + \sum_{1 \le j \le e-1} \frac{(1+Z)\left(qZ^4\right)^{\max\{0,j+t-e\}}}{1-qZ^4} \cdot Z^{2e-2j} L_j \\
&\quad + \frac{\left(qZ^4\right)^t}{1-qZ^4} L_e + \frac{2Z\left(qZ^4\right)^t}{(1-Z)(1-qZ^4)} L_{e+1} .
\end{aligned}$$

Now the evident symmetry between the coefficients of L_j and L_{e-j}, when the transformation $t \mapsto e-t$

is made, establishes the theorem. ∎

Inserting this into the machinery of Part III produces global reflection theorems:

Theorem 9.3 (**"Quadratic O-N"**). *Let K be a number field of class number 1. Then for any $I, \tau \in \mathcal{O}_K$ with $\tau \mid 2$,*

$$\sum_{\substack{f \in \Gamma(\mathcal{O}_K)\backslash V_\tau(I)(\mathcal{O}_K) \\ \operatorname{disc} f > 0 \text{ at every real place}}} \frac{1}{|\mathrm{Stab}_{\Gamma(\mathcal{O}_K)f}|} = \frac{|N_{K/\mathbb{Q}}(\tau)|}{2^{r_2(K)}} \sum_{f \in \Gamma(\mathcal{O}_K)\backslash V_{2\tau^{-1}}(4\tau^{-4}I)(\mathcal{O}_K)} \frac{1}{|\mathrm{Stab}_{\Gamma(\mathcal{O}_K)f}|}$$

where $r_2(K)$ is the number of complex places of K.

Proof. We verify the hypotheses of Lemma 8.10 on the integral models $V_\tau(I)$ and $V_{2\tau^{-1}}(4\tau^{-4}I)$:

(i) $V(I)$ is Hasse because it is full, as previously noted.

(ii) To check that Γ has class number 1, it suffices to check the factors $\mathbb{G}_m$ and $\mathbb{G}_a$ of which Γ is a semidirect product. The former of these has the same class number as K, explaining the restriction in the theorem statement.

(iii) The finiteness of the local orbit counter follows from the formulas for it computed in the previous theorem.

(iv) Finally, at almost all places, we plug in $e = t = 0$ to get $F = L_0$, establishing the needed convergence.

Now we need the local reflection itself. We keep track of the constants c_v accrued:

- If $v \nmid 2\infty$, the integral models are naturally dual with constant $c_v = 1$.
- If $v \mid 2$, the integral models are naturally dual with constant $c_v = [\mathcal{O}_v : \tau\mathcal{O}_v]$. Multiplying over all $v \mid 2$ and using that $\tau \mid 2$ yields a factor

$$\prod_{v|2} c_v = [\mathcal{O}_K : \tau\mathcal{O}_K] = |N_{K/\mathbb{Q}}\tau|.$$

- If v is real, the integral models are no longer naturally dual at v. We place the non-natural weighting

$$w^{(2)} = \mathbf{1}_0$$

that picks out $\alpha \in H^1(K, \mathbb{Z}/2\mathbb{Z})$ that vanish at v, that is, forms with positive discriminant at v. This is the Fourier transform of $w^{(1)} = 1$, so $c_v = 1$.

- Finally, if v is complex, then the integral models are certainly naturally dual at v, because $|H^1| = 1$. However, the scaling of the Fourier transform by $1/|H^0(\mathbb{C}, M)| = 1/2$ requires that we take $c_v = 1/2$.

Multiplying these constants gives the constant claimed. ■

Remark 9.4. The condition that $\mathcal{O}_K$ be a PID can be dropped, but then Γ no longer has class number 1, and each side of the theorem becomes a sum of orbit counts on $\mathrm{Cl}(\mathcal{O}_K)$-many global integral models that locally look alike. We do not spell out the details here. We wonder whether such a method works in general to circumvent the class-number-1 hypothesis in Theorem 8.12.

We conclude by specializing further to the case $K = \mathbb{Q}$. We replace $\Gamma(\mathbb{Z})$ by its index-2 subgroup, the group $\mathbb{Z}$ of translations. This merely doubles all orbit counts, and it acts freely on quadratics with nonzero discriminant, so we can suppress all mention of stabilizers for the following charmingly simple statement, also featured in Section 2:

Theorem 9.5 ("Quadratic O-N"). *If n is a nonzero integer, let $q(n)$ be the number of integer quadratic polynomials $f(x) = ax^2 + bx + c$ with*

$$a(b^2 - 4ac) = n,$$

up to the trivial change $x \mapsto x + t$ ($t \in \mathbb{Z}$). Let $q_2(n)$, $q^+(n)$, and $q_2^+(n)$, respectively, be the number of these f such that $2|b$ (for q_2), such that the roots of f are real (for q^+), or which satisfy both

conditions (for q_2^+). Then for all nonzero integers n,

$$q_2^+(4n) = q(n)$$

$$q_2(4n) = 2q^+(n).$$

Example 9.6. Looking at $n = p_1p_3$, where $p_1 \equiv 1 \pmod 4$ and $p_3 \equiv 3 \pmod 4$ are primes, the counts involve certain Legendre symbols. For instance, the combination $a = p_3$, $b^2 - 4ac = p_1$ is feasible if and only if the congruence

$$b^2 \equiv p_1 \mod 4p_3$$

has a solution, which happens exactly when $\left(\frac{p_1}{p_3}\right) = 1$. Working out all cases, we find that

$$q^+(p_1p_3) = 5 + \left(\frac{p_1}{p_3}\right) \quad \text{and} \quad q_2(4p_1p_3) = 10 + 2\left(\frac{p_3}{p_1}\right).$$

Thus our reflection theorem recovers the quadratic reciprocity law

$$\left(\frac{p_1}{p_3}\right) = \left(\frac{p_3}{p_1}\right).$$

We wonder: does there exist a proof of Theorem 9.5 using no tools more advanced than quadratic reciprocity?

10 Class groups: generalizations of the Scholz and Leopoldt reflection theorems

We now return to the consideration with which we began: reflection theorems for class groups. Scholz [49] proved a relation between the 3-torsion in the class groups of $\mathbb{Q}(\sqrt{D})$ and $\mathbb{Q}(\sqrt{-3D})$. Leopoldt [31] significantly generalized this result. We here present a generalization of Leopoldt's

result to orders in $\mathcal{GA}(\mathbb{F}_p)$-extensions, where exact formulas (as opposed to bounds) can often be obtained. We will not use composed varieties; instead, we will use Poisson summation in the form of the Greenberg-Wiles formula to get reflection theorems.

Let T/K be a $(\mathbb{Z}/p\mathbb{Z})^\times$-torsor. If $\mathcal{O} \subseteq T$ is a Galois-invariant $\mathcal{O}_K$-order, then $(\mathbb{Z}/p\mathbb{Z})^\times$ acts on the class group $\mathrm{Cl}(\mathcal{O})$. The p-primary part $\mathrm{Cl}(\mathcal{O})_p$ is broken up into eigenspaces, one for each character $\chi : (\mathbb{Z}/p\mathbb{Z})^\times \to \mu_{p-1} \subseteq \mathbb{Z}_p^\times$. There is a distinguished character $\chi = \omega$ lifting the reduction map modulo p (the Teichmüller lift). We will concern ourselves with the ω-part $\mathrm{Cl}(\mathcal{O})_{p,\omega}$. (The remaining parts are related to the ω-parts of the class groups of other torsors.) We look at the p-torsion, or equivalently the p-cotorsion:

$$\mathrm{Cl}(\mathcal{O})[p]_\omega \cong (\mathrm{Cl}(\mathcal{O})/p\,\mathrm{Cl}(\mathcal{O}))_\omega.$$

10.1 Dual orders

We now develop a condition on two orders $\mathcal{O}_1 \subseteq T$, $\mathcal{O}_2 \subseteq T'$ that will suffice to produce a reflection theorem between their class groups. First, a simple lemma:

Lemma 10.1. *Let L be an étale algebra over a number field K, let $\mathcal{O} \subseteq L$ be an order, and let M/L be a G-torsor. The following conditions are equivalent:*

(*a*) *M is a ring class algebra for $\mathcal{O}$; that is, the global Artin map*

$$\psi_{M/L} = \prod_i \psi_{M_i/L_i} : \mathcal{I}(L, \mathfrak{m}) \to G$$

factors through $\mathrm{Cl}(\mathcal{O})$, where $\mathfrak{m} \subseteq \mathcal{O}_K$ is an admissible modulus for M/L, $\mathcal{I}(L, \mathfrak{m})$ is the group of invertible fractional ideals of L prime to $\mathfrak{m}$, and the product runs through all field factors M_i of M, with L_i being the corresponding field factor of L;

(*b*) *For every valuation v of K, the local Artin map*

$$\phi_{M_v/L_v} = \prod_{u|w|v} \phi_{M_u/L_w} : L_v^\times \to G$$

vanishes on $\mathcal{O}_v^\times$.

Proof. By local-global compatibility, the global Artin map can be described idelically as the product of the local ones. Indeed, $\mathcal{I}(L,\mathfrak{m})$ embeds into $\mathbb{A}_L^\times / \prod_{v\nmid\mathfrak{m}} \mathcal{O}_{L_v}^\times$, and

$$\psi_{M/L} = \prod_v \phi_{M_v/L_v} : \mathbb{A}_L^\times \to G.$$

Now the idele-theoretic description of $\mathrm{Cl}(\mathcal{O})$ is

$$\mathrm{Cl}(\mathcal{O}) = \mathbb{A}_L^\times / \left(L^\times \cdot \prod_v \mathcal{O}_v^\times \right).$$

Since $\psi_{M/L}$ always vanishes on the principal ideles $L^\times$, it factors through $\mathrm{Cl}(\mathcal{O})$ if and only if it vanishes on each $\mathcal{O}_v^\times$ (v a place of K), where it reduces to the product ϕ_{M_v/L_v} of the local Artin maps at the primes dividing v, as desired. ∎

There is an analogue for *narrow* ring class algebras: here ϕ_{M_v/L_v} is required to vanish on $\mathcal{O}_v^\times$ for v finite only.

This motivates the following definitions.

Definition 10.2.

(a) Let K be a local field, T/K a $(\mathbb{Z}/p\mathbb{Z})^\times$-torsor and T' its Tate dual. Two $(\mathbb{Z}/p\mathbb{Z})^\times$-invariant orders $\mathcal{O}_1 \subseteq T$, $\mathcal{O}_2 \subseteq T'$ are called *dual* if the ω-parts of the multiplicative groups, $(\mathcal{O}_1^\times)_\omega$ and $(\mathcal{O}_2^\times)_\omega$, are orthogonal complements under the Hilbert pairing, which as we know is perfect between $(T^\times)_\omega$ and $(T'^\times)_\omega$.

(b) Let K be a global field, T/K a $(\mathbb{Z}/p\mathbb{Z})^\times$-torsor and T' its Tate dual. Two orders $\mathcal{O}_1 \subseteq T$, $\mathcal{O}_2 \subseteq T'$ are called *dual* if the completions $\mathcal{O}_{1,\mathfrak{q}}$, $\mathcal{O}_{2,\mathfrak{q}}$ are dual for all primes $\mathfrak{q}$ of K.

A dual pair yields a reflection theorem, as follows.

Theorem 10.3. *Let $\mathcal{O}_1 \subseteq T$, $\mathcal{O}_2 \subseteq T'$ be dual orders. Then*

$$\frac{|\mathrm{Cl}^+(\mathcal{O}_1)[p]_\omega|}{|\mathrm{Cl}(\mathcal{O}_2)[p]_\omega|} = \frac{p^{\mathbf{1}_{T \text{ is totally split}}}}{p^{\mathbf{1}_{T' \text{ is totally split}}}} \cdot \prod_{v \text{ of } K} \frac{|\mathcal{O}_{2,\ell,\omega}^\times|}{p^{\mathbf{1}_{T_p \text{ is totally split}}}} \tag{57}$$

Proof of Theorem 10.3. The maps $\psi : \mathrm{Cl}(\mathcal{O}_1) \to \mathbb{Z}/p\mathbb{Z}$ are the Artin maps of ring class algebras E/T of $\mathcal{O}_1$. Now $(\mathbb{Z}/p\mathbb{Z})^\times$ acts both on maps ψ and algebras E, and it is easy to see that the ψ belonging to the ω-component correspond to E that are *symmetric,* that is, are $\mathcal{GA}(\mathbb{F}_p)$-torsors with resolvent subtorsor T. So we get an injection of groups

$$i : \mathrm{Hom}(\mathrm{Cl}(\mathcal{O}_1), \mathbb{Z}/p\mathbb{Z}) \to H^1(K, M_T).$$

By Lemma 10.1, the image of i is a Selmer group $\mathrm{Sel}_X(K, M_T)$, where the local conditions X_v are given by

$$X_v = \text{the whole of } H^1(K_v, M_T) \text{ if } v|\infty$$
$$X_v = \mathcal{O}_{1,v,\omega}^\perp = \mathcal{O}_{2,v,\omega}, \quad v \text{ finite}$$

where the second equality uses the duality of $\mathcal{O}_1$ and $\mathcal{O}_2$ and the Kummer parametrization

$$H^1(K_v, M_T) \cong T_\omega'^\times.$$

By the exact same argument, the dual Selmer system

$$X_v = 0 \text{ if } v|\infty$$
$$X_v = \mathcal{O}_{2,v,\omega}^\perp = \mathcal{O}_{1,v,\omega}, \quad v \text{ finite}$$

has Selmer group naturally identified with $\mathrm{Hom}(\mathrm{Cl}^+(\mathcal{O}_2), \mathbb{Z}/p\mathbb{Z})$. (Of course, the distinction between wide and narrow class groups is only relevant if $p = 2$, a case which we will exclude in the next section.)

To finish, we apply the Greenberg-Wiles formula, as mentioned in the end of the proof of Theorem 8.12, and use that $|H^0(M_T)|$ is either p or 1 according as T is totally split. ■

10.2 Dual orders are plentiful for quadratic extensions

It's not hard to show that the maximal orders $\mathcal{O}_T$, $\mathcal{O}_{T'}$ are dual at primes $\ell \nmid p$. At p, however, it is not obvious how one might find a pair of dual orders, or whether such orders exist. However, there is a case in which this is manageable, and it specializes to the Scholz reflection principle in the case $p = 3$.

Let p be an odd prime. We will assume that our base field K contains the element

$$\rho_p = \zeta_p + \zeta_p^{-1} = 2\cos\frac{2\pi}{p}.$$

(Note that $\rho_3 = -1$, so this assumption always holds when $p = 3$.) This entails in particular that $K(\zeta_p)$ is an extension of K of degree at most 2, being $K(\sqrt{D})$ where

$$D = (\zeta_p - \zeta_p^{-1})^2 = \rho_p^2 - 4.$$

We note that D is a unit locally at all finite primes $\mathfrak{q}$ except those dividing p, in which case $|D|_\mathfrak{q} = |p|_\mathfrak{q}^{1/(p-1)} = d_{\min,\mathfrak{q}}^{1/p}$.

If $Q = K[\sqrt{a}]$ is an étale quadratic algebra, we may form the $(\mathbb{Z}/p\mathbb{Z})^\times$-torsor $T = Q^{(p-1)/2}$, with the unique possible torsor action. Q is a μ_2-torsor, and $Q^\times/(Q^\times)^p$ is the direct sum of two components: $Q^\times_{\omega^0} \cong K^\times/(K^\times)^p$, and $Q^\times_\omega = Q^{N=1}/(Q^{N=1})^p$ which parametrizes $\mathcal{GA}(M)$-extensions whose resolvent torsor is T. Due to the splitting of T, these are in fact D_p-extensions, where D_p is the dihedral group (the permutation group that the symmetries of a regular p-gon induce on its vertices).

The Tate dual T' is $Q'^{(p-1)/2}$, a product of copies of the quadratic algebra $Q' = K[\sqrt{Da}]$.

10.3 Local dual generalized orders

Suppose our base field K has a distinguished subring of integers $\mathcal{O}_K$, a Dedekind domain with field of fractions K. If $\mathcal{O} \subseteq \mathcal{O}_Q$ is an order over $\mathcal{O}_K$, denote by $\mathcal{R}(\mathcal{O})$ the projection of $\mathcal{O}^\times$ onto $(Q^\times)_\omega$, quotienting out by both pth powers and the eigenspace corresponding to the trivial character (namely $(\mathcal{O}_K^\times)/(\mathcal{O}_K^\times)^p$).

If K is local, we call a pair of orders $\mathcal{O} \subseteq Q$, $\mathcal{O}' \subseteq Q'$ *dual* if the associated *unit class subgroups* $\mathcal{R}(\mathcal{O}) \subseteq (Q^\times)_\omega$, $\mathcal{R}(\mathcal{O}') \subseteq (Q'^\times)_\omega$ are orthogonal complements. For example, it is not hard to prove that if $\operatorname{char} k_K \neq p$, the maximal orders in Q and Q' are dual to one another. We pose the question of whether any order in Q admits a dual order. The answer is no, because $\mathcal{R}(\mathcal{O})$ can be as small as $\{1\}$ but cannot be as big as $(Q^\times)_\omega$, being always contained in $(\mathcal{O}_Q^\times)_\omega$. This is essentially the only obstruction, and we remedy it by introducing a notion of *generalized order*.

Definition 10.4. If Q is a quadratic étale algebra over a field K, in which a Dedekind domain $\mathcal{O}_K$ is fixed as a ring of integers, a *generalized order* in Q is a finitely generated $\mathcal{O}_K$-subalgebra $\mathcal{O}$ spanning Q over K and closed under the conjugation automorphism of Q.

If $\mathcal{O}_K$ is local, then as soon as $\mathcal{O}$ contains an element of Q with negative valuation, even with respect to only one of the valuations on Q (if Q is split), then taking conjugates and powers shows that $\mathcal{O}$ contains all elements of Q. Thus the only generalized orders in this case are that $\mathcal{O} = Q$ or $\mathcal{O}$ is an order in the ordinary sense, that is, a subring of $\mathcal{O}_Q$ that spans Q. Letting $\mathcal{O}_Q = \mathcal{O}_K[\xi]$, these orders have the form $\mathcal{O} = \mathcal{O}_K[\pi^i \xi]$ for $i \geq 0$.

In general, a generalized order $\mathcal{O}$ over a Dedekind domain $\mathcal{O}_K$ is specified by a collection $(\mathcal{O}_\mathfrak{q})_\mathfrak{q}$ of orders in the completions $K_\mathfrak{q}$, almost all maximal; and particular has the form $\mathcal{O}_1[\mathfrak{q}_1^{-1}, \ldots, \mathfrak{q}_r^{-1}]$ where $\mathcal{O}_1$ is an order in $\mathcal{O}_Q$ and the $\mathfrak{q}_i$ are finitely many primes of K, at which $\mathcal{O}_1$ can be taken maximal. Class groups of generalized orders over number fields are not hard to study: in the foregoing notation, we have that $\operatorname{Cl}(\mathcal{O}) \cong \operatorname{Cl}(\mathcal{O}_1)/\langle \mathfrak{q}_1, \ldots, \mathfrak{q}_r \rangle$ is formed by quotienting out by the classes of the relevant primes.

Lemma 10.5. *If K is a local field and $\mathcal{O} \subseteq \mathcal{O}_Q$ is a quadratic generalized order, then $\mathcal{R}(\mathcal{O})$ is a*

level space in $Q_\omega^\times$ (in the sense of Theorem 7.1). Moreover, all level spaces arise in this way.

Proof. In the tame case that $\operatorname{char} k_K \neq p$, there are at most three level spaces, and it is easy to identify the generalized orders to which they correspond:

$$\begin{aligned} Q_\omega^\times &= \mathcal{R}(Q) \\ (\mathcal{O}_Q)_\omega^\times &= \mathcal{R}(\mathcal{O}_Q) \\ \{1\} &= \mathcal{R}(\mathcal{O}), \text{ any } \mathcal{O} \subsetneq \mathcal{O}_Q. \end{aligned}$$

The last holds because any $x \in \mathcal{O}^\times$ is the product of $x_0 \in K^\times$, which maps into the ω^0-component, and an $x_1 \equiv 1 \bmod \pi_K \mathcal{O}_Q$ which is necessarily a pth power.

In the wild case we use similar methods. Since $p \neq 2$, we may write $\mathcal{O}_Q = \mathbb{Q}_K[\sqrt{\beta_Q}]$, where $v_K(\beta_Q)$ is 0 or 1. The Kummer element β corresponding to the torsor $T = Q^{(p-1)/2}$ is $\beta = \beta_Q^{(p-1)/2}$.

The generalized order Q has unit class subgroup

$$\mathcal{R}(Q) = \mathcal{L}_{-1}.$$

The remaining orders can be described as

$$\mathcal{O}_j = \mathcal{O}_K\left[\pi^{j-v(\beta)/2}\sqrt{\beta}\right],$$

where j, the valuation of a generator, ranges over the nonnegative elements of $\mathbb{Z}$ (if $\beta \sim 1$) or $\mathbb{Z}+1/2$ (if $\beta \sim \pi$). A unit in such an order is of the form

$$u = a\left(1 + b\pi^{j-v(\beta)/2}\sqrt{\beta}\right), \quad a \in \mathcal{O}_K^\times, b \in \mathcal{O}_K$$

Since the factor a belongs to the ω^0-component, it can be ignored. The range of $[u] \in H^1(K, M)$,

by Theorem 7.1(f), is $\mathcal{L}_i$, where

$$i = \begin{cases} \left\lceil \dfrac{(p-1)(j-1)}{p} \right\rceil, & j \le \dfrac{pe}{p-1} + 1 \\ e+1, & j > \dfrac{pe}{p-1} + 1. \end{cases}$$

It is easy to see that all i $(0 \le i \le e+1)$ are attained thereby. ■

Proposition 10.6. *Every generalized order in a quadratic extension Q/K has a (not necessarily unique) dual order in the reflection extension Q'.*

Proof. Follows immediately from Lemma 10.5 and Theorem 7.1(g). ■

In the tame case, we evidently have the dual pairs

$$\mathcal{O}_Q \longleftrightarrow \mathcal{O}_{Q'}, \quad Q \longleftrightarrow \mathcal{O}$$

for any $\mathcal{O} \subsetneq \mathcal{O}_{Q'}$. In the wild case, things are only a bit more involved:

Proposition 10.7. *Let $\mathcal{O}_{Q,j}$, $\mathcal{O}_{Q',j'}$ be the orders in Q and Q' as parametrized in the proof of Lemma 10.5. A dual to Q is any $\mathcal{O}_{Q',j'}$ for which*

$$j > \frac{pe}{p-1} + 1.$$

For $0 \le j \le \frac{pe}{p-1}$, a dual to $\mathcal{O}_{Q,j}$ is $\mathcal{O}_{Q',j'}$ where

$$j' = \frac{pe}{p-1} + 1 - j.$$

Proof. The only slightly nontrivial step is to show that, in the second case, the corresponding level indices

$$i = \left\lceil \frac{(p-1)(j-1)}{p} \right\rceil \quad \text{and} \quad i' = \left\lceil \frac{(p-1)(j'-1)}{p} \right\rceil$$

have sum e. But after noting that the arguments to the two ceilings have sum $\equiv 1/p \mod 1$, the

summation becomes easy. ■

The method of proof of Theorem 10.3 applies without change to generalized orders and yields the following.

Theorem 10.8. *Let $p \geq 3$ be a prime, let K be a global field with $\zeta_p + \zeta_p^{-1} \in K$, and let Let $\mathcal{O}_1 \subseteq Q$, $\mathcal{O}_2 \subseteq Q'$ be dual generalized quadratic orders. Then*

$$\frac{|\mathrm{Cl}(\mathcal{O}_1)[p]_\omega|}{|\mathrm{Cl}(\mathcal{O}_2)[p]_\omega|} = \frac{p^{\mathbf{1}_{Q \cong K \times K}}}{p^{\mathbf{1}_{Q' \cong K \times K}}} \cdot \prod_{v \ of \ K} \frac{|\mathcal{O}_{2,\ell,\omega}^\times|}{p^{\mathbf{1}_{Q_p \cong K \times K}}} \tag{58}$$

10.4 Relation to the Scholz reflection theorem

Example 10.9. Let $p = 3$, $K = \mathbb{Q}$, $T = \mathbb{Q}[\sqrt{D}]$, and $T' = \mathbb{Q}[\sqrt{-3D}]$, where D is a fundamental discriminant with $3 \nmid D$. Construct a pair of dual orders $\mathcal{O}$, $\mathcal{O}'$ by specification at each prime ℓ of $\mathbb{Z}$ as follows:

- If $\ell \neq 3, \infty$, we take $\mathcal{O}$ and $\mathcal{O}'$ to be maximal at ℓ, contributing nothing to the product in Theorem 10.8.
- If $\ell = 3$, using Proposition 10.7, we see that the orders $\mathbb{Q}_3[\sqrt{D}]$ and $\mathbb{Q}_3[\sqrt{-27D}]$ are dual, as are $\mathbb{Q}_3[\sqrt{9D}]$ and $\mathbb{Q}_3[\sqrt{-3D}]$. The first contributes 1 to the product, and the second contributes 3.

The prime $\ell = \infty$ does not enter into the construction of the dual orders, but it introduces a factor $|H^0(\mathbb{R}, M_D)|$ that depends on the sign of D. Finally, note that all of the class group $\mathrm{Cl}(\mathcal{O})$ of a quadratic order belongs to the ω-eigenspace, the 1-eigenspace being $\mathrm{Cl}(\mathbb{Z}) = 0$. So we get an equality, which was also noticed by Nakagawa ([38], Theorem 0.5):

Corollary 10.10. *If $D \equiv 0, 1 \bmod 4$ is an integer, write $\mathrm{Cl}(D)$ for the class group of the quadratic ring over $\mathbb{Z}$ having discriminant D. Let D be a fundamental discriminant not divisible by 3. Then*

$$|\mathrm{Cl}(-27D)[3]| = |\mathrm{Cl}(D)[3]| \cdot 3^{\mathbf{1}_{D=-3} - \mathbf{1}_{D=1} + \mathbf{1}_{D>0}} \tag{59}$$

$$|\mathrm{Cl}(-3D)[3]| = |\mathrm{Cl}(9D)[3]| \cdot 3^{\mathbf{1}_{D=-3} - \mathbf{1}_{D=1} + \mathbf{1}_{D>0} - 1}. \tag{60}$$

Both equations are generalizations of the Scholz reflection principle, which states that for $D \neq 1, -3$,

$$|\mathrm{Cl}(-3D)[3]| = |\mathrm{Cl}(D)[3]| \cdot 3^{\mathbf{1}_{D>0}-\varepsilon}$$

where $\varepsilon \in \{0, 1\}$. This theorem shows that ε can be explained by the size of the kernel of either of the maps

$$\mathrm{Cl}(9D)/\mathrm{Cl}(9D)^3 \to \mathrm{Cl}(D)/\mathrm{Cl}(D)^3 \quad \text{or} \quad \mathrm{Cl}(-27D)/\mathrm{Cl}(-27D)^3 \to \mathrm{Cl}(-3D)/\mathrm{Cl}(-3D)^3. \tag{61}$$

It also shows that exactly one of the maps (61) is an isomorphism, the other having kernel of size 3—a theorem, perhaps, that has not appeared in the literature yet?

Part V

Reflection theorems: cubic rings

11 Cubic Ohno-Nakagawa

The space $V(K)$ of binary cubic forms over a local or global field K can have many integral models. Let $V_{\mathcal{O}_K}$ be the lattice of binary cubic forms with trivial Steinitz class; these can be written as

$$V_{\mathcal{O}_K} = ax^3 + bx^2y + cxy^2 + dy^3 : a, b, c, d \in \mathcal{O}_K,$$

and we abbreviate the form $ax^3 + bx^2y + cxy^2 + dy^3$ to (a, b, c, d). A theorem of Osborne classifies all lattices $L \subseteq V_{\mathcal{O}_K}$ that are $\mathrm{GL}_2(\mathcal{O}_K)$-invariant and *primitive*, in the sense that $\mathfrak{p}^{-1}L \not\subseteq V(\mathcal{O}_K)$ for all finite primes $\mathfrak{p}$ of $\mathcal{O}_K$:

Theorem 11.1 (Osborne [47], Theorem 2)**.** *A primitive* $\mathrm{GL}_2(\mathcal{O}_K)$*-invariant lattice in* $V(\mathcal{O}_K)$ *is determined by any combination of the primitive* $\mathrm{GL}_2(\mathcal{O}_{K,\mathfrak{p}})$*-invariant lattices in the completions*

$V(\mathcal{O}_{K,\mathfrak{p}})$, *which are:*

(a) If $\mathfrak{p}|3$, *the lattices* $\Lambda_{\mathfrak{p},i} = \{(a,b,c,d) : b \equiv c \equiv 0 \bmod \mathfrak{p}^i\}$, *for* $0 \leq i \leq v_{\mathfrak{p}}(3)$;

(b) If $\mathfrak{p}|2$ *and* $N_{K/\mathbb{Q}}(\mathfrak{p}) = 2$, *the five lattices*

$$\begin{aligned}
\Lambda_{\mathfrak{p},1} &= V(\mathcal{O}_{K,\mathfrak{p}}),\\
\Lambda_{\mathfrak{p},2} &= \{(a,b,c,d) \in V(\mathcal{O}_{K,\mathfrak{p}}) : a+b+d \equiv a+c+d \equiv 0 \mod \mathfrak{p}\}\\
\Lambda_{\mathfrak{p},3} &= \{(a,b,c,d) \in V(\mathcal{O}_{K,\mathfrak{p}}) : a+b+c \equiv b+c+d \equiv 0 \mod \mathfrak{p}\}\\
\Lambda_{\mathfrak{p},4} &= \{(a,b,c,d) \in V(\mathcal{O}_{K,\mathfrak{p}}) : b+c \equiv 0 \mod \mathfrak{p}\}\\
\Lambda_{\mathfrak{p},5} &= \{(a,b,c,d) \in V(\mathcal{O}_{K,\mathfrak{p}}) : a \equiv d \equiv b+c \mod \mathfrak{p}\},
\end{aligned}$$

(c) For all other $\mathfrak{p}$, *the maximal lattice* $V(\mathcal{O}_{K,\mathfrak{p}})$ *only.*

From the perspective of algebraic geometry, if $\mathfrak{p}|2$, the latter four lattices are not true integral models, because they lose their SL_2-invariance as soon as we extend scalars so that the residue field has more than 2 elements. By contrast, if $\mathfrak{p}|3$, the SL_2-invariance of the space $L_{\mathfrak{p}_i}$ can be established purely formally. This integral model, which we will call the space of $\mathfrak{p}^i$-*traced* forms, will be the subject of our main reflection theorem in this part.

Although Osborne deals only with the case of $\Gamma(\mathcal{O}_K)$, his method generalizes easily to the lattice

$$V(\mathcal{O}_K, \mathfrak{a}) = \{ax^3 + bx^2y + cxy^2 + dy^3 : a \in \mathfrak{a}, b \in \mathcal{O}_K, c \in \mathfrak{a}^{-1}, d \in \mathfrak{a}^{-2}\}$$

that pops up when considering the maps

$$\Phi : M \to \Lambda^2 M$$

that appear in the higher composition law Theorem 6.9. Here the relevant action of

$$\Gamma(\mathcal{O}_K, \mathfrak{a}) = \mathrm{Aut}_{\mathcal{O}_K}(\mathcal{O}_K \oplus \alpha) = \left\{ \begin{bmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{bmatrix} \in \mathrm{GL}_2(K) : a_{ij} \in \mathfrak{a}^{j-i} \right\}$$

is nontrivial on both M and $\Lambda^2 M$, thus affecting $V(\mathcal{O}_K, \mathfrak{a})$ via a twisted action

$$\left(\begin{bmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{bmatrix} . \Phi \right)(x, y) = \frac{1}{a_{11}a_{22} - a_{12}a_{21}} \Phi(a_{11}x + a_{21}y, a_{12}x + a_{22}y). \tag{62}$$

(Compare [14], p. 142 and [57], Theorem 1.2.) The twist by the determinant does not affect invariance of lattices but renders the action faithful, while otherwise scalar matrices that are cube roots of unity would act trivially. We sidestep this issue entirely by restricting the action to the group SL_2, which preserves the discriminant $D \in \mathfrak{a}^{-2}$ of the form. The corresponding ring has discriminant $(\mathfrak{a}, D)$.

For instance, over $K = \mathbb{Z}$ there are ten primitive invariant lattices, comprising five types at 2 and two types at 3. The O-N-like reflection theorems relating all the types at 2 were computed by Ohno and Taniguchi [45] and will be considered later in this paper (Section 12.4). While the behavior at 2 admits only mild generalization, being based on the combinatorics of the finitely many cubic forms over $\mathbb{F}_2$, the behavior at 3 is robust. We begin by making some definitions needed to track the behavior of cubic forms and rings at primes dividing 3.

If $\mathcal{O}$ is a ring of finite rank over a Dedekind domain $\mathcal{O}_K$, define its *trace ideal* $\mathrm{tr}(\mathcal{O})$ to be the image of the trace map $\mathrm{tr}_{\mathcal{O}/\mathcal{O}_K} : \mathcal{O} \to \mathcal{O}_K$. Note that $\mathrm{tr}(\mathcal{O})$ is an ideal of $\mathcal{O}_K$ and, since $1 \in \mathcal{O}$ has trace $n = \deg(\mathcal{O}/\mathcal{O}_K)$, it is a divisor of the ideal (n). In particular, if $\mathcal{O}_K$ is a DVR, this notion is uninteresting unless $\mathcal{O}_K$ has residue characteristic dividing n. Let $\mathfrak{t}$ be an ideal of $\mathcal{O}_K$ dividing (n). We say that the ring $\mathcal{O}$ is $\mathfrak{t}$-*traced* if $\mathrm{tr}(\mathcal{O}) \subseteq \mathfrak{t}$.

By Theorem 6.9, we can parametrize cubic orders $\mathcal{O}$ by their Steinitz class $\mathfrak{a}$ and index form

$$\Phi(x\xi + y\eta) = (ax^3 + bx^2y + cxy^2 + dy^3)(\xi \wedge \eta)$$

relative to a decomposition $\mathcal{O} = \mathcal{O}_K \oplus \mathcal{O}_K\xi \oplus \mathfrak{a}\eta$, where $a \in \mathfrak{a}$, $b \in \mathcal{O}_K$, $c \in \mathfrak{a}^{-1}$, and $d \in \mathfrak{a}^{-2}$. Then a short computation using the multiplication table from Theorem 6.9 shows that, if $(1, \xi, \eta)$ is a normal basis, then $\mathrm{tr}(\xi) = -b$ and $\mathrm{tr}(\eta) = c$, so $\mathrm{tr}(\mathcal{O}) = \langle 3, b, \mathfrak{a}c\rangle$. Thus the based $\mathfrak{t}$-traced rings over $\mathcal{O}_K$ are parametrized by the rank-4 lattice of cubic forms

$$\mathcal{V}_{\mathfrak{a},\mathfrak{t}}(\mathcal{O}_K) := \{ax^3 + bx^2y + cxy^2 + dy^3 : a \in \mathfrak{a}, b \in \mathfrak{t}, c \in \mathfrak{t}\mathfrak{a}^{-1}, d \in \mathfrak{a}^{-2}\},$$

on which $\mathrm{GL}(\mathcal{O} \oplus \mathfrak{a})$ acts by the twisted action (62). For instance, if $\mathcal{O}_K = \mathbb{Z}$, $\mathfrak{a} = (1)$, and $\mathfrak{t} = (3)$, this is the lattice of integer-matrix cubic forms considered in the introduction. Our goal in this section is to prove a generalization for all number fields K and spaces $V(\mathcal{O}_K, \mathfrak{a}, \mathfrak{t})$.

Theorem 11.2 ("Local cubic O-N"). *Let K be a nonarchimedean local field,* $\mathrm{char}\, K \neq 3$. *Let $V(D)$ be the composed variety of binary cubic forms of discriminant D, under the action of the group $\Gamma = \mathrm{SL}_2$. If $\alpha \in K^\times$ and $\tau \mid 3$ in $\mathcal{O}_K$, let $\mathcal{V}_{\alpha,\tau}(D)$ be the integral model of $V(K)(D)$ consisting of forms of the shape*

$$f(x, y) = a\alpha x^3 + b\tau x^2y + c\alpha^{-1}\tau xy^2 + d\alpha^{-2}y^3,$$

together with its natural action of $\mathcal{G}_\alpha = \mathrm{SL}(\mathcal{O}_K \oplus \alpha\mathcal{O}_K)$. Then the integral models

$$(\mathcal{V}_{1,\tau}(D), \mathrm{SL}_2\mathcal{O}_K) \quad \textit{and} \quad \left(\mathcal{V}_{1,3\tau^{-1}}(-27\tau^{-6}D), \mathrm{SL}_2\mathcal{O}_K\right), \tag{63}$$

and consequently

$$(V_{\alpha,\tau}(D), \mathcal{G}_\alpha) \quad \textit{and} \quad \left(V_{\alpha\tau^{-3},3\tau^{-1}}(-27D), \mathcal{G}_{\alpha\tau^{-3}}\right) \tag{64}$$

are naturally dual with duality constant $N_{K/\mathbb{Q}}(\tau) = |\mathcal{O}_K/\tau\mathcal{O}_K|$.

The two formulations are easily seen to be equivalent. The first one is the one we will prove, but the second one has the needed form of a local reflection theorem to apply at each place to get the following global reflection theorem:

Theorem 11.3 (O-N for traced cubic rings). *Let*

$$\mathcal{V}_{\mathfrak{a},\mathfrak{t}}(\mathcal{O}_K) := \{f(x,y) = ax^3 + bx^2y + cxy^2 + dy^3 : a \in \mathfrak{a}, b \in \mathfrak{t}, c \in \mathfrak{t}\mathfrak{a}^{-1}, d \in \mathfrak{a}^{-2}\},$$

a representation of

$$\mathcal{G}_{\mathfrak{a}} := \mathrm{SL}(\mathcal{O}_K \oplus \mathfrak{a}).$$

Note that $\mathcal{V}_{\mathfrak{a},\mathfrak{t}}$ is the integral model of $(V(K), \Gamma(K))$ parametrizing $\mathfrak{t}$-traced cubic rings over $\mathcal{O}_K$ with Steinitz class $\mathfrak{a}$. For $D \in \mathfrak{t}^2\mathfrak{a}^{-2}$, define the class number

$$h_{\mathfrak{a},\mathfrak{t}}(D) = \sum_{\substack{\Phi \in \mathcal{G}_{\mathfrak{a}} \backslash \mathcal{V}_{\mathfrak{a},\mathfrak{t}}(\mathcal{O}_K) \\ \operatorname{disc} \Phi = D}} \frac{1}{|\mathrm{Stab}\, \Phi|} = \sum_{\substack{\mathrm{Disc}\, \mathcal{O} = (\mathfrak{a}, D) \\ \mathfrak{t}\text{-}traced}} \frac{1}{|\mathrm{Aut}_K\, \mathcal{O}|}.$$

Then we have the global reflection theorem

$$h_{\mathfrak{a},\mathfrak{t}}(D) = \frac{3^{\#\{v|\infty : D \in (K_v^\times)^2\}}}{N_{K/\mathbb{Q}}(\mathfrak{t})} \cdot h_{\mathfrak{a}\mathfrak{t}^{-3}, 3\mathfrak{t}^{-1}}(-27D). \tag{65}$$

Proof. Use Theorem 11.2 at each finite place. At the infinite places, the two integral models are necessarily naturally dual because $H^1(\mathbb{R}, M_D) = 0$; but the duality constant depends on H^0, which depends on the sign of D at each real place, as desired. ∎

Observe that taking $K = \mathbb{Q}$, $\mathfrak{a} = 1$, $\mathfrak{t} = 1$ recovers Ohno-Nakagawa (Theorem 1.1).

This also yields the extra functional equation for the Shintani zeta functions (see Corollary 11.8 below).

We can rewrite our results in terms of Shintani zeta functions.

Definition 11.4. Let K be a number field. If $\mathcal{O}/\mathcal{O}_K$ is a cubic ring of nonzero discriminant, the *signature* $\sigma(\mathcal{O})$ of $\mathcal{O}$ is the Kummer element $\alpha \in (K \otimes_{\mathbb{Q}} \mathbb{R})^\times / ((K \otimes_{\mathbb{Q}} \mathbb{R})^\times)^2$ corresponding to the quadratic resolvent of $\mathcal{O}$. That is, it takes the value $\alpha_v = +1$ or -1 at each real place v of K according as $\mathcal{O}_v \cong \mathbb{R} \times \mathbb{R} \times \mathbb{R}$ or $\mathbb{R} \times \mathbb{C}$, and $\alpha_v = 1$ at each complex place.

Definition 11.5. Given a number field K, a signature $\sigma \in (K \otimes_{\mathbb{Q}} \mathbb{R})^\times / ((K \otimes_{\mathbb{Q}} \mathbb{R})^\times)^2$, an ideal class

$[\mathfrak{a}] \in \mathrm{Cl}(K)$, and an ideal $\mathfrak{t} \mid 3$, we define the *Shintani zeta function*

$$\xi_{K,\sigma,[\mathfrak{a}],\mathfrak{t}}(s) = \sum_{\mathcal{O}} \frac{1}{|\mathrm{Aut}_K(\mathcal{O})|} N_{K/\mathbb{Q}}(\mathrm{disc}_K L)^{-s}$$

where the sum ranges over all cubic orders $\mathcal{O}$ over $\mathcal{O}_K$ having signature σ, Steinitz class $\mathfrak{a}$, and trace ideal contained in $\mathfrak{t}$. We also define the *Shintani zeta function* with unrestricted Steinitz class

$$\xi_{K,\sigma,\mathfrak{t}}(s) = \sum_{[\mathfrak{a}] \in \mathrm{Cl}(K)} \xi_{K,\sigma,[\mathfrak{a}],\mathfrak{t}}(s).$$

Remark 11.6. Confusingly, it is traditional to denote Shintani zeta functions by the Greek letter xi.

Remark 11.7. By Minkowski's theorem on the finite count of number fields with bounded degree and discriminant, each term n^{-s} has a finite coefficient, so the Shintani zeta function at least makes sense as a formal Dirichlet series. It generalizes the Shintani zeta functions for rings over $\mathbb{Z}$ mentioned in the introduction. Datskovsky and Wright [18] study an adelic version of the Shintani zeta function; they show that $\xi_{K,\sigma,(1)}$ and $\xi_{K,\sigma,(3)}$ are entire meromorphic with at most simple poles at $s = 1$ and $s = 5/6$, satisfying an explicit functional equation. We surmise that the same method will prove the same for $\xi_{K,\sigma,[\mathfrak{a}],\mathfrak{t}}$. However, we do not consider the analytic properties here.

Then we have the following corollary, which generalizes Conjecture 1.1 of Dioses [20].

Corollary 11.8 (the extra functional equation for Shintani zeta functions). *Let K be a number field, $\sigma \in (K \otimes_{\mathbb{Q}} \mathbb{R})^\times / ((K \otimes_{\mathbb{Q}} \mathbb{R})^\times)^2$ a signature, $[\mathfrak{a}] \in \mathrm{Cl}(K)$ an ideal class, and $\mathfrak{t} \mid 3$ an ideal. Then the Shintani zeta function $\xi_{K,\sigma,[\mathfrak{a}],\mathfrak{t}}(s)$ satisfies an extra functional equation*

$$\xi_{K,\sigma,[\mathfrak{a}],\mathfrak{t}}(s) = \frac{3^{\#\{v|\infty:\sigma_v=1\}+3[K:\mathbb{Q}]s}}{N_{K/\mathbb{Q}}(t)^{1+6s}} \xi_{K,-\sigma,[\mathfrak{a}\mathfrak{t}^{-3}],3\mathfrak{t}^{-1}}(s), \tag{66}$$

Hence, summing over all $\mathfrak{a}$,

$$\xi_{K,\sigma,\mathfrak{t}}(s) = \frac{3^{\#\{v|\infty:\sigma_v=1\}+3[K:\mathbb{Q}]s}}{N_{K/\mathbb{Q}}(t)^{1+6s}} \xi_{K,-\sigma,3\mathfrak{t}^{-1}}(s), \tag{67}$$

Proof. Fix $\mathfrak{a}$ and $\mathfrak{t}$. Sum Theorem 11.3 over all $D \in \mathfrak{t}^3\mathfrak{a}^{-2}$ of signature σ, weighting each D by

$$N_{K/\mathbb{Q}}\left(D\mathfrak{a}^2\right)^{-s},$$

the norm of the discriminant of the associated cubic rings. Then the left-hand side of the summed equality matches that of (66). The right-hand side involves rings with discriminant ideal $27D\mathfrak{a}^2\mathfrak{t}^{-6}$, so a compensatory factor of

$$\frac{N_{K/\mathbb{Q}}\left(D\mathfrak{a}^2\right)^{-s}}{N_{K/\mathbb{Q}}\left(27D\mathfrak{a}^2\mathfrak{t}^{-6}\right)^{-s}} = \frac{3^{[K:\mathbb{Q}]s}}{N_{K/\mathbb{Q}}(\mathfrak{t})^{6s}}$$

must be added to the right-hand side to pull out the desired Shintani zeta function. ■

In the succeeding subsections, we present three approaches to the local duality (Theorem 11.2). First, we present a short conceptual proof in the special case that $\operatorname{char} k_K \neq 3$, a "tame" case. Second, we explicitly compute the local orbit counters for a computational proof. Third, we organize the local orbits into families for a more conceptual general proof.

11.1 A bijective proof of the tame case

Proof of the tame case of Theorem 11.2. Fix $D \in \mathcal{O}_K$. Let $T = K[\sqrt{D}]$ be the corresponding quadratic algebra, and $T' = K[\sqrt{-3D}]$. For brevity we will write $H^i(T)$ for the cohomology $H^i(K, M_T)$ of the corresponding order-3 Galois module, and $H^i(T')$ likewise.

Denote by $f(\sigma)$, for $\sigma \in H^1(T)$, the number of orders of discriminant D in the corresponding cubic algebra L_σ; and likewise, denote by $f'(\tau)$, for $\tau \in H^1(T')$, the number of orders of discriminant $-3D$ in L_τ. Our task is to prove that $f' = \hat{f}$. We note that if -3 is a square in $\mathcal{O}_K^\times$, then $T = T'$ and $f = f'$.

Note that f is even: σ and $-\sigma$ are parametrized by the same cubic algebra with opposite orientations of its resolvent. The Fourier transform of an even, rational-valued function on a 3-torsion group $H^1(T)$ is again even and rational-valued. So far, so good.

Our method will be first to prove the duality at 0: that is, that

$$f'(0) = \hat{f}(0) \tag{68}$$

$$f(0) = \widehat{f'}(0). \tag{69}$$

Let us explain how this implies that $f' = \hat{f}$. We compute $|H^1(T)|$ using the self-orthogonality of unramified cohomology:

$$|H^1(T)| = |H^1(T)^{\mathrm{ur}}| \cdot |H^1(T')^{\mathrm{ur}}| = |H^0(T)| \cdot |H^0(T')|.$$

So there are basically three cases:

(a) If neither D nor $-3D$ is a square in K_v, then $H^1(T) \cong H^1(T') \cong 0$, and (68) trivially implies that $f' = \hat{f}$.

(b) If one of D, $-3D$ is a square, then $H^1(T)$ and $H^1(T')$ are one-dimensional $\mathbb{F}_3$-vector spaces. The space of even functions on each is 2-dimensional, and

$$g \mapsto (g(0), \hat{g}(0))$$

$$g' \mapsto (\widehat{g'}(0), g'(0))$$

are corresponding systems of coordinates on them. Consequently, the two equations (68) and (69) together imply that $\hat{f} = f'$.

(c) Finally, if D and $-3D$ are both squares, then f is a function on the two-dimensional $\mathbb{F}_3$-space $H^1(T) \cong H^1(T')$ which we would like to prove self-dual. Note that $H^1(T)$ has four subspaces $W_1, \ldots, W_4$ of dimension 1. Consider the following basis for the five-dimensional space of even functions on $H^1(T)$:

$$f_1 = \mathbf{1}_{W_1}, \ldots, f_4 = \mathbf{1}_{W_4}, f_5 = \mathbf{1}_0.$$

Note that $f_1, \ldots, f_4$ are self-dual (the Tate pairing is alternating, so any one-dimensional

subspace is isotropic), while f_5 is not: indeed $\hat{f}_5(0) \neq f_5(0)$. Thus if (68) holds, then f is a linear combination of $f_1, \ldots, f_4$ only and hence $\hat{f} = f$.

We have now reduced the theorem to a pair of identities, (68) and (69). By symmetry, it suffices to prove (69), which may be written

$$f(0) \stackrel{?}{=} \hat{f}(0) = \frac{1}{|H^0(T')|} \sum_{\tau \in H^1(T')} f(\tau). \tag{70}$$

The proof is clean and bijective.

The left-hand side of (70) counts orders of discriminant D in the split algebra $K \times T$. These can be straightforwardly parametrized as

$$\mathcal{O}_K + 0 \times \mathfrak{a},$$

where $\mathfrak{a}$ is a multiplicatively closed lattice in T, that is, an invertible ideal in some quadratic order $\mathcal{O} \subseteq T$. (Here we use that, in a quadratic algebra, any lattice $\mathfrak{a}$ is an invertible ideal with respect to its endomorphism ring $\operatorname{End} \mathfrak{a}$. This fails for higher-degree algebras, which we will encounter later.)

The sum on the right-hand side of (70) counts all cubic orders of discriminant $-3D$. Any cubic order C of discriminant $-3D$ can be assigned an ideal in T as follows. Let L be the fraction algebra of C. By Theorem 5.4, we have the description

$$L = K + \{\xi \sqrt[3]{\delta} + \bar{\xi} \sqrt[3]{\bar{\delta}} \mid \xi \in T'\}$$

for some $\delta \in T'^{N=1} / \left(T'^{N=1}\right)^3$; and so, since 3 is invertible in $\mathcal{O}_K$,

$$C = \mathcal{O}_K + \{\xi \sqrt[3]{\delta} + \bar{\xi} \sqrt[3]{\bar{\delta}} \mid \xi \in \mathfrak{c}\} \tag{71}$$

for some lattice $\mathfrak{c}$ in T'. Now by Theorem 6.11, we get that $(\mathcal{O}_D, \mathfrak{c}, \delta)$ is a *self-balanced ideal*, that is,

$$\delta \mathfrak{c}^3 \subseteq \mathcal{O}_D, \quad N(\mathfrak{c}) = (t) \text{ is principal}, \quad \text{and} \quad N(\delta) t^3 = 1, \tag{72}$$

Now $\mathfrak{c}$ need not be invertible in $\mathcal{O}_D$; but let $\mathcal{O} := \operatorname{End}\mathfrak{c}$. Note that $\mathcal{O} = \mathcal{O}_{D/\pi^{2i}}$ for some positive integer i. Then form the *shadow*

$$\mathfrak{a} = \frac{\delta \mathfrak{c}^3}{\pi^i}.$$

Since the norm is multiplicative on invertible ideals, the properties of $\mathfrak{c}$ in (72) can be recast as properties of $\mathfrak{a}$:

$$\mathfrak{a} \subseteq \operatorname{End}\mathfrak{a} \quad \text{and} \quad N_{\mathcal{O}_D}(\mathfrak{a}) = 1. \tag{73}$$

The first of these says that $\mathfrak{a}$ is multiplicatively closed, and the second that the ring $C = \mathcal{O}_K + 0 \times \mathfrak{a}$ corresponding to $\mathfrak{a}$ has discriminant D.

It remains to show that there are exactly $|H^0(T)|$ cubic orders C corresponding to each shadow $\mathfrak{a}$ satisfying (73), weighting each C by the number of isomorphic copies of C in its fraction algebra $L = KC$.

First, we simply count C up to isomorphism. This is the same as counting the self-balanced ideals $(\mathcal{O}_D, \mathfrak{c}, \delta)$ up to the equivalence relation

$$\mathfrak{c} \mapsto \lambda\mathfrak{c}, \quad \delta \mapsto \lambda^{-3}\delta \quad (\lambda \in T'^{\times}) \tag{74}$$

Note the slight subtlety in this step: we would like to define an isomorphism between the associated cubic algebras L_δ, $L_{\lambda^{-3}\delta}$ by

$$\xi\sqrt[3]{\delta} + \bar{\xi}\sqrt[3]{\bar{\delta}} \mapsto \lambda\xi\sqrt[3]{\lambda^{-3}\delta} + \bar{\lambda}\bar{\xi}\sqrt[3]{\bar{\lambda}^{-3}\bar{\delta}},$$

which works, but only after potentially rescaling the cube roots on the right-hand side by a suitable 3rd root of unity in K so that their product is $N(\lambda)t = N(\lambda)\sqrt[3]{\delta}\sqrt[3]{\bar{\delta}}$.

Let $\mathfrak{a} = \alpha\mathcal{O}$ be the given shadow, where $\mathcal{O} = \mathcal{O}_{D/\pi^{2i}}$ is its ring of invertibility. Clearly $\mathfrak{c}$ must be invertible with regard to $\mathcal{O}$. The possible $(\mathfrak{c}, \delta)$ may be found by fixing $\mathfrak{c} = \mathcal{O}$ and taking $\delta = \pi^i\alpha\varepsilon$ where $\varepsilon \in \mathcal{O}^\times$ is constrained by the requirement that $N(\delta)$ be a cube. If, without loss of generality, we scale α so that $N(\pi^i\alpha)$ is a cube, then the admissible values are $\{\varepsilon \in \mathcal{O}^\times : N(\varepsilon) \in (K^\times)^3\}$. Now

in the equivalence relation 74, the multipliers λ preserving $\mathfrak{c} = \mathcal{O}$ are $\lambda \in \mathcal{O}^\times$, so we must consider ε up to $\left(\mathcal{O}^\times\right)^3$. Since $N : \mathcal{O}^\times/\left(\mathcal{O}^\times\right)^3 \to \mathcal{O}_K^\times/\left(\mathcal{O}_K^\times\right)^3$ is surjective, the number of distinct ε, which is the number of nonisomorphic C, is simply

$$\frac{\left|\mathcal{O}^\times/\left(\mathcal{O}^\times\right)^3\right|}{\left|\mathcal{O}_K^\times/\left(\mathcal{O}_K^\times\right)^3\right|}.$$

Next, we weight each C by the number of isomorphic copies of C in $L = KC$. The automorphisms of C are given by

$$\xi\sqrt[3]{\delta} + \bar{\xi}\sqrt[3]{\bar{\delta}} \mapsto \omega\xi\sqrt[3]{\delta} + \bar{\omega}\bar{\xi}\sqrt[3]{\bar{\delta}}$$

where $\omega \in \mathcal{O}_{T'}$ satisfies $\omega^3 = \omega\bar{\omega} = 1$. But choices $\omega \in \mathcal{O}$ fix C, so we must quotient out by those, and the number of isomorphic copies is

$$\frac{\left|\mathcal{O}_{T'}^{N=1}[3]\right|}{\left|\mathcal{O}^{N=1}[3]\right|} = \frac{\left|\mathcal{O}_{T'}^\times[3]\right|}{\left|\mathcal{O}^\times[3]\right|},$$

and the total number of cubic orders we seek is the product

$$\frac{\left|\mathcal{O}^\times/\left(\mathcal{O}^\times\right)^3\right|}{\left|\mathcal{O}_K^\times/\left(\mathcal{O}_K^\times\right)^3\right|} \cdot \frac{\left|\mathcal{O}_{T'}^\times[3]\right|}{\left|\mathcal{O}^\times[3]\right|}. \tag{75}$$

To maneuver this into the required form, first note that

$$\frac{\left|\mathcal{O}^\times/\left(\mathcal{O}^\times\right)^3\right|}{\left|\mathcal{O}^\times[3]\right|} = \frac{\left|\mathcal{O}_{T'}^\times/\left(\mathcal{O}_{T'}^\times\right)^3\right|}{\left|\mathcal{O}_{T'}^\times[3]\right|}$$

by the Snake Lemma, since $\mathcal{O}_{T'}^\times/\mathcal{O}^\times$ is finite; so (75) takes the form

$$\frac{\left|\mathcal{O}_{T'}^\times/\left(\mathcal{O}_{T'}^\times\right)^3\right|}{\left|\mathcal{O}_K^\times/\left(\mathcal{O}_K^\times\right)^3\right|},$$

which we can now compute directly to equal

$$\left|\mathcal{O}_{T'}^{N=1}/\left(\mathcal{O}_{T'}^{N=1}\right)^3\right| = \frac{T',N=1/\left(T',N=1\right)^3}{|H^1(T')|} = \frac{|H^1(T)|}{|H^1(T')|} = |H^0(T)|.$$

■

11.2 A computational proof

We now turn our attention to the wild case of Theorem 11.2. We present two proofs, one computational, one more conceptual.

11.2.1 Trace ideals of maximal orders

Our first step is to compute $\mathrm{tr}(\mathcal{O}_L)$ for the maximal orders of all cubic extensions L. The answer is delightfully simple.

Proposition 11.9. *Let L/K be a cubic étale algebra over a 3-adic field. The trace ideal of the maximal order of L is*

$$\mathrm{tr}(\mathcal{O}_L) = (3) + \mathfrak{m}_K^{e-\ell(L)}$$

where $\ell(L)$ is the level.

Remark 11.10. Hyodo ([27], equation (1–4); see also Xia and Zhukov [61]) proves a theorem like this one for an invariant he calls the *depth* of a ramified extension. The depth is in fact closely related to the level and offset.

Proof. We first dispose of the case that L is not totally ramified, that is, has splitting type 111, 12, 3, or 1^21, by noting that in all these cases $\mathrm{tr}(\mathcal{O}_L) = (1)$ and $\ell(L) = e$.

Now let $L = K[\pi_L]$ be a totally ramified extension. We have $\mathrm{tr}(\mathcal{O}_L) = (3, \mathrm{tr}\,\pi_L, \mathrm{tr}\,\pi_L^2)$. There are two cases.

⟨1⟩ In this case we assume $v_K(\mathrm{tr}\,\pi_L) \geq v_K(\mathrm{tr}\,\pi_L^2)$, including the case that both are infinite. In this case it is possible to adjust π_L by a multiple of π_L^2 so as to make the trace vanish. Therefore we

may assume that $\operatorname{tr}\pi_L = 0$, so the Eisenstein minimal polynomial of π_L is a depressed cubic,

$$\phi(x) = x^3 + ux + v,$$

with $v_K(u) \geq 1$ and $v_K(v) = 1$. We have $\operatorname{tr}(x^2) = 2u$, so $\operatorname{tr}(\mathcal{O}_K) = (3, u)$.

$$\operatorname{disc}(L) = \operatorname{disc}\phi = 4u^3 - 27v^2.$$

Now $v_K(27v^2) = 3e + 2$ is not a multiple of 3, so the two terms have unequal valuation. If $v_K(u) \leq e$, then $4u^3$ dominates so L has level $\ell = e - v_K(u)$ and offset $\theta = 0$; and the trace ideal is $(u) = \mathfrak{m}_K^\ell$. If $v_K(u) > e$, then $-27v^2$ dominates so $v_K(\operatorname{disc} L) = 3e + 2$. This is the case $L = K[\sqrt[3]{\pi_K}]$ of a uniformizer radical extension. The level is -1, the offset is -1 and the trace ideal is (3).

⟨2⟩ In this case we assume $v_K(\operatorname{tr}\pi_L) < v_K(\operatorname{tr}\pi_L^2)$. Note that $v_K(\operatorname{tr}\pi_K\pi_L) \leq v_K(\operatorname{tr}\pi_L^2)$, so it is possible to adjust π_L^2 by a multiple of $\pi_K\pi_L$ to produce an element ρ such that $\operatorname{tr}\rho = 0$ and $v_L(\rho) = 2$. The minimal polynomial of ρ is a depressed cubic

$$\phi(x) = x^3 + ux + v,$$

with $v_K(u) \geq 1$ and $v_K(v) = 2$. Now ρ does not generate all of $\mathcal{O}_L$; instead, an $\mathcal{O}_K$-basis of $\mathcal{O}_L$ is $(1, \rho^2/\pi_K, \rho)$ so $\operatorname{tr}(\mathcal{O}_L) = (3, u/\pi_K)$.

$$\operatorname{disc}(L) = \frac{\operatorname{disc}\phi}{\pi_K^2} = \frac{4u^3 - 27v^2}{\pi_K^2}.$$

Now $v_K(27v^2) = 3e + 4$ is not a multiple of 3, so the two terms in the numerator have unequal valuation. If $v_K(u) \leq e + 1$, then $4u^3$ dominates so L has level $\ell = e - v_K(u) + 1$ and offset $\theta = 1$; and the trace ideal is $(u/\pi_K) = \mathfrak{m}_K^\ell$. If $v_K(u) > e + 1$, then $-27v^2$ dominates and we have a uniformizer radical extension again. ■

The foregoing proof has a corollary on the structure of totally ramified cubic extensions which will be important to us.

Corollary 11.11. *Let L/K be a totally ramified extension.*

(a) If $\theta(L) = 0$, then L has a traceless uniformizer.

(b) If $\theta(L) = 1$, then L has a traceless element of valuation 2.

Proof. Simply note that Case $\langle 1 \rangle$ occurs only when $\theta = 0$ or -1, and Case $\langle 2 \rangle$ occurs only when $\theta = 1$ or -1. ■

Problem 11.12. *Find an analogue of Proposition 11.9 for $\mathcal{GA}(\mathbb{Z}/p\mathbb{Z})$-extensions of p-adic fields, $p \geq 5$.*

11.2.2 The subring zeta function

If L/K is a cubic 3-adic algebra and $0 \leq t \leq e$, let

$$g(L,t) = \sum_{\substack{\text{orders } \mathcal{O} \subseteq L \\ \text{tr}(\mathcal{O}) \subseteq \mathfrak{m}_K^t}} z^{v_K(\text{disc}\,\mathcal{O})/2} \in \mathbb{Z}[[z^{1/2}]]$$

be the generating function of $\mathfrak{m}_K^t$-traced orders in L. This is related to the *subring zeta function* (see Section 12.3). The factor of $1/2$ in the exponent is used (quite arbitrarily) to make a factor of z correspond to passing to a subring of index $\mathfrak{m}_K$. Note that $g(L,t) \in z^{1/2}\mathbb{Z}[[z]]$ or $\mathbb{Z}[[z]]$ according as T is ramified or not.

Note that if $t \leq e - \ell(L)$, then every order in L is automatically $\mathfrak{m}_K^t$-traced, so $g(L,t) = g(L,0)$ is simply the generating function for all orders that was computed by Datskovsky and Wright.

We will proceed to compute $g(L,t)$ for all L and t. We begin by tabulating the possible splitting

types for a cubic algebra L:

$\sigma(L)$	$\ell(L)$	$\theta(L)$	$v_K(\operatorname{Disc} L)$
111	e	0	0
12	e	0	0
3	e	0	0
1^21	e	1	1
1^3	$0 \le \ell < e$	0 or 1	$3(e-\ell)+\theta$
1^3	-1	-1	$3e+2$

Lemma 11.13. *We have*

$$g(L,t) = z^{v_K(\operatorname{disc}\mathcal{O}_L)/2} \cdot s^{\sigma,\theta}(n)$$

for a certain power series $s^{\sigma,\theta}(n) \in \mathbb{Z}[[z]]$ that depends only on three parameters: the splitting type $\sigma = \sigma(L)$, the offset $\theta = \theta(L)$ (which is redundant unless $\sigma = 1^3$), and the trace deficit *$n = t - e + \ell(L)$.*

In due course, we will prove this theorem and determine the series $s^{\sigma,\theta}(n)$ by directly counting the rings involved. For now, we assume it and proceed to deduce Theorem 11.2, which, in this notation, says:

Theorem 11.14 (Local cubic O-N). *Considering $g(L,t)$ as a function of L, its Fourier dual is given by*

$$\hat{g}(L,t) = q^t z^{3t-\frac{3e}{2}} g(L, e-t).$$

Proof. The proof proceeds by writing $g(L,t)$ as a linear combination of characteristic functions of level spaces. Let $g(T,\ell,t) = g(L,t)$ for any L of resolvent torsor T and level ℓ, where

$$e \ge \ell \ge \ell_{\min} = \begin{cases} -1 & \text{if } T' \text{ is split} \\ 0 & \text{otherwise.} \end{cases}$$

By Theorem 7.1(d), such L exists, and by Lemma 11.13, the series $g(T, L, t)$ is independent of which L of this level we choose, with one exception: if $T \cong K \times K$ is split and $\ell = 0$, then L could have splitting type 111 or 3. We resolve the ambiguity as follows: give $g(K \times K, 0, t)$ the value of $g(L, t)$ when $\sigma(L) = 3$, and introduce a symbol $g(K \times K, -1, t)$ with the value $g(K \times K \times K, t)$ for splitting type 111. Correspondingly, define the level space

$$\mathcal{L}_{e+1} = \{0\},$$

in spite of the fact that cubic algebras of splitting types 3 and 111 both have level e. Then in all cases, if we set

$$\ell_{\max} = \begin{cases} e+1 & \text{if } T \text{ is split} \\ e & \text{otherwise} \end{cases}$$

then we have

$$g(L,t) = \sum_{\ell_{\min} \le \ell \le \ell_{\max}} \mathbf{1}_{L \in \mathcal{L}_\ell \setminus \mathcal{L}_{\ell+1}} g(T, \ell, t) = \sum_{\ell_{\min} \le \ell \le \ell_{\max}} \mathbf{1}_{L \in \mathcal{L}_\ell} (g(T, \ell, t) - g(T, \ell - 1, t))$$

where

$$g(T, \ell_{\min} - 1, t) = 0 \tag{76}$$

Now $\hat{\mathbf{1}}_{\mathcal{L}_\ell} = c_\ell \mathbf{1}_{\mathcal{L}_{e-\ell}}$, where

$$c_\ell = \frac{|\mathcal{L}_\ell|}{|H^0(T)|} = \begin{cases} \frac{1}{3} & \ell = e+1 = \ell_{\max} \\ q^{e-\ell} & 0 \le \ell \le e \\ 3q^e & \ell = -1 = \ell_{\min}. \end{cases}$$

Thus it suffices to prove that

$$c_\ell (g(T, \ell, t) - g(T, \ell - 1, t)) = q^t z^{3t - \frac{3e}{2}} (g(T', e - \ell, t) - g(T', e - \ell - 1, t)) \tag{77}$$

for $\ell_{\min} \le \ell \le \ell_{\max}$. It is easy to verify that flipping $T \mapsto T'$, $\ell \mapsto e - \ell$, $t \mapsto e - t$ transforms (77) to an equivalent equation, so we assume that $\ell > 0$ and $\ell + t \ge e$, which cuts down the number of cases.

We now enumerate the cases of (77), which by Lemma 11.13, depend on the splitting types and offsets of the fields L appearing. Recall that when the level ℓ ($0 \le \ell \le e$) and resolvent torsor T of a cubic algebra L are known, the offset can be determined by the congruence

$$3\ell + \theta = v_K(\operatorname{disc} L) \equiv v_K(\beta_T) \mod 2$$

where β_T is a Kummer element for T (here we simply have $v_K(\beta_T) \equiv v_K(\operatorname{disc} L) \mod 2$). Now since $\beta_T \beta_{T'} = -3$ (up to squares), we have

$$v_K(\beta_T) + v_K(\beta'_T) \equiv e \mod 2.$$

From this, we find that each offset in (77) determines the other three, even without knowing T, and there are only six cases:

$\sigma(T)$	ℓ	$\sigma(L_{T,\ell})$	$\sigma(L_{T,\ell+1})$	$\sigma(L_{T',e-\ell})$	$\sigma(L_{T',e-\ell+1})$
any	$0 < \ell < e$	$1^3(\theta = 0)$	$1^3(\theta = 1)$	$1^3(\theta = 0)$	$1^3(\theta = 1)$
any	$0 < \ell < e$	$1^3(\theta = 1)$	$1^3(\theta = 0)$	$1^3(\theta = 1)$	$1^3(\theta = 0)$
1^2	e	$1^2 1$	$1^3(\theta = 0)$	$1^3(\theta = 1)$	—
2	e	12	$1^3(\theta = 1)$	$1^3(\theta = 0)$	—
11	e	3	$1^3(\theta = 1)$	$1^3(\theta = 0)$	$1^3(\theta = -1)$
11	e	111	3	$1^3(\theta = -1)$	—

The dashes for $\ell = \ell_{\min}$ indicate that the corresponding term was declared zero in (76). We now write each term of (77) in terms of $s^{\sigma,\theta}(n)$ using Lemma 11.13. Thanks to our assumptions that $\ell > 0$ and $\ell + t \ge e$, the terms on the right side involve only $s^{\sigma,\theta}(n)$ for $n < 0$. In this case, we can replace n by 0 because all orders in L automatically satisfy the trace condition. The corresponding

generating function was computed by Datskovsky and Wright and will soon be recovered by us (see (94))

$$s_0 = s^{1^3,\theta}(0) = \frac{1}{(1-z)(1-qz^3)},$$

independent of θ. The theorem is now reduced to the following lemma. ■

Lemma 11.15. *For $t \geq 0$,*

$$s^{1^3,\theta=0}(n) - z^2 s^{1^3,\theta=1}(n-1) = q^n z^{3n}(1-z^2)s_0 \tag{78}$$

$$s^{1^3,\theta=1}(n) - z s^{1^3,\theta=0}(n-1) = q^n z^{3n}(1-z)s_0 \tag{79}$$

$$s^{3}(n) - z^2 s^{1^3,\theta=1}(n-1) = q^n z^{3n}(1-z)s_0 \tag{80}$$

$$s^{12}(n) - z^2 s^{1^3,\theta=1}(n-1) = q^n z^{3n} s_0 \tag{81}$$

$$s^{1^21}(n) - z s^{1^3,\theta=0}(n-1) = q^n z^{3n} s_0 \tag{82}$$

$$s^{111}(n) - s^3(n) = 3q^n z^{3n+1} s_0. \tag{83}$$

This lemma can be viewed as a set of coupled difference equations for computing the $s^{\sigma,\theta}(t)$.

11.2.3 Counting traced cubic orders: the proofs of Lemma 11.13 and Lemma 11.15

It now remains to count the $\mathfrak{m}_K^t$-traced orders in each cubic algebra L. These are sublattices of $\mathcal{O}_L$ containing 1 and satisfying (a) the *ring condition,* that is, closure under multiplication, and (b) the *trace condition* that each of their elements has trace in $\mathfrak{m}_K^t$. We first simplify these two conditions.

If $\mathcal{O} \subseteq \mathcal{O}_L$ is a sublattice containing 1, the quotient $\mathcal{O}_L/\mathcal{O} \cong (\mathcal{O}_L/\mathcal{O}_K)/(\mathcal{O}/\mathcal{O}_K)$ is a finite group generated as an $\mathcal{O}_K$-module by two elements. We may write

$$\mathcal{O}_L/\mathcal{O} = (\mathcal{O}_K/\mathfrak{m}_K^i)\xi \oplus (\mathcal{O}_K/\mathfrak{m}_K^j)\eta, \tag{84}$$

where ξ and η are generators such that $\mathcal{O}_L$ and $\mathcal{O}$ have $\mathcal{O}_K$-bases $(1,\xi,\eta)$ and $(1,\pi_K^i\xi,\pi_K^j\eta)$. By symmetry we may assume that $i \geq j$. By varying the basis $(1,\xi,\eta)$, we get all lattices $\mathcal{O}$ of "index (i,j)" in the sense that (84) holds. (This is an example of a *reduced basis*, which we will use more

systematically in the quartic case.) Note that

$$\mathcal{O} = \mathcal{O}_K + \mathfrak{m}_K^i \mathcal{O}_L + \mathfrak{m}_K^j \eta, \tag{85}$$

from which it is easy to see that two bases $(1, \xi, \eta)$ and $(1, \xi', \eta')$ yield the same $\mathcal{O}$ if and only if

$$\eta \equiv u\eta' \mod \mathfrak{m}_K^{j-i}\mathcal{O}_L, \quad \text{some } u \in (\mathcal{O}_K/\mathfrak{m}_K^{i-j})^\times. \tag{86}$$

Note that ξ is irrelevant. Also note that when $i = j$ there is a single lattice, the *content ring* $\mathcal{O}_K + \mathfrak{m}_K^i \mathcal{O}_L$.

Having constructed all lattices of index (i, j), we test whether they are rings using Theorem 6.9(c): $\mathcal{O}$ is a ring if and only if its index form is integral. Let the index form of L be

$$\Phi_L(x\xi + y\eta) = (ax^3 + bx^2y + cxy^2 + dy^3)(\xi \wedge \eta).$$

Then

$$\Phi_L(x\pi_K^i\xi + y\pi_K^j\eta) = (a\pi_K^{2i-j} + b\pi_K^i + c\pi_K^j + d\pi_K^{2j-i})(\pi_K^i\xi \wedge \pi_K^j\eta). \tag{87}$$

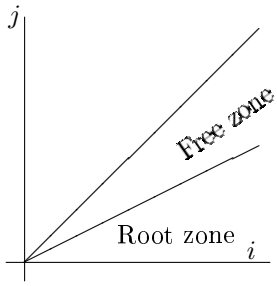


Figure 1: Two zones for the indices (i, j) for a candidate subring of $\mathcal{O}_L$

From this we can deduce that there are two kinds of pairs (i, j). If $j \le i \le 2j$, then every lattice with indices (i, j) is a ring: we say that (i, j) is in the *free zone*. If $i > 2j$, the ring condition is that

$\pi_K^{i-2j} | d$, that is,

$$\Phi_{\mathcal{O}_L}(\eta) \equiv 0 \mod \mathfrak{m}_K^{i-2j}. \tag{88}$$

Because η must in this sense be a root of Φ, we call this range of (i,j) values the *root zone*. Note that if L has splitting type (3), then Φ has no roots even mod $\mathfrak{m}_K$ and hence no orders in the root zone. For the remaining splitting types, the root-zone orders can be subdivided according to which root of Φ—which "1" in the splitting type—η reduces to mod $\mathfrak{m}_K$.

Finally we must test our orders for the trace condition $\operatorname{tr} \mathcal{O} \subseteq \mathfrak{m}_K^{e-\ell+n}$, where $\ell = e - v_K(\operatorname{tr} \mathcal{O}_L) = \max\{\ell(L), 0\}$. We may assume that $0 \leq n \leq \ell$. The trace ideal of an order (85) can be computed by

$$\operatorname{tr} \mathcal{O} = \operatorname{tr}(\mathcal{O}_K + \mathfrak{m}_K^i \mathcal{O}_L + \mathfrak{m}_K^j \eta) = (3) + \mathfrak{m}_K^{\ell+i} + \mathfrak{m}_K^j \operatorname{tr} \eta.$$

Now if $n > i$, the trace condition is impossible; if $n \leq j$, it is automatic; and if $j < n \leq i$, it is contingent on η: the condition is

$$\frac{\operatorname{tr} \eta}{\pi_K^\ell} \equiv 0 \mod \mathfrak{m}_K^{n-j}. \tag{89}$$

The ring condition (88) is cubic in η, while the trace condition (89) is linear. We will presently see how they interact.

11.2.4 Traced orders in the free zone

In this subsubsection we evaluate

$$s^{\mathrm{FZ}}(n) = \sum_{\substack{\mathcal{O} \subset \mathcal{O}_L \text{ free-zone orders,} \\ \operatorname{tr}(\mathcal{O}) \subseteq \mathfrak{m}_K^n \operatorname{tr}(\mathcal{O}_L)}} z^{v_K([\mathcal{O}_L : \mathcal{O}])}.$$

In the free zone, we know that the lattices of index (i,j) are parametrized by elements $\eta \in \mathcal{O}_L / \mathcal{O}_K$ not divisible by $\mathfrak{m}_K$ up to the equivalence relation (86), and all are orders. We get $q^{i-j-1}(q+1)$ orders if $i > j$, just 1 if $i = j$; and all of these satisfy the trace condition if $n \leq j$. It remains to test them on the trace condition (89) under the hypothesis that $j < n \leq i$.

It is not hard to see that $\mathcal{O}_L$ has a basis $(1, \xi_0, \eta_0)$ where $\operatorname{tr}(\xi_0) = 0$. Then η_0 can be taken to

generate $\mathrm{tr}(\mathcal{O}_L) = \mathfrak{m}_K^{e-\ell}$. Write $\eta = x\xi_0 + y\eta_0$ (the $\mathcal{O}_K$-component being irrelevant). The trace condition becomes $\mathfrak{m}_K^{n-j}|x$. In particular, x is not a unit so y must be, and we can scale so that $y = 1$; then there are q^{i-n} choices for x (which is defined modulo $\mathfrak{m}_K^{i-j}$).

Summing, the generating function for the free zone is

$$s^{\mathrm{FZ}}(n) = \sum_{j<n\le i\le 2j} q^{i-n} z^{i+j} + \sum_{n\le j<i\le 2j} (q+1) q^{i-j-1} z^{i+j} + \sum_{n\le j=i} z^{i+j}. \tag{90}$$

11.2.5 Traced orders in the root zone

In this subsubsection we fix a root $\bar{\eta}_0$ of the index form Φ of $\mathcal{O}_L$ modulo $\mathfrak{m}_K$. We evaluate the generating function of $\bar{\eta}_0$-orders, that is, orders whose corresponding basis element η reduces to $\bar{\eta}_0$ modulo $\mathfrak{m}_K$:

$$s^{\mathrm{RZ},\bar{\eta}_0}(n) = \sum_{\substack{\mathcal{O}\subset\mathcal{O}_L \ \bar{\eta}_0\text{-orders},\\ \mathrm{tr}(\mathcal{O})\subseteq\mathfrak{m}_K^n \mathrm{tr}(\mathcal{O}_L)}} z^{v_K([\mathcal{O}_L:\mathcal{O}])}$$

In each of the various cases that we will encounter, we will choose a basis $(1, \xi_0, \eta_0)$ such that η_0 reduces to $\bar{\eta}_0$ mod $\mathcal{O}_K + \mathfrak{m}_K\mathcal{O}_L$. Then the lattices belonging to this root are parametrized by elements $\eta = x\xi_0 + y\eta_0$ where $\mathfrak{m}_K|x$; so $\mathfrak{m}_K \nmid y$ and we can scale so that $y = 1$. Consequently we can take $\eta = x'\pi_K\xi_0 + \eta_0$ where x' runs over the residue classes mod $\mathfrak{m}_K^{i-j-1}$.

The first case is that of the *simple* root, the "1" with no exponent that appears in the splitting types 111, 12, and 1^21. In this case Hensel's lemma tells us that $\bar{\eta}_0$ can be lifted to an element η_0 with $\Phi(\eta_0) = 0$, and we can identify it explicitly: $L = K \times T$ splits and $\eta_0 = (1; 0)$. Note that $\mathrm{tr}(\eta_0) = 1$ and $\ell = e$. We can complete to a basis $(1, \xi_0, \eta_0)$ with $\mathrm{tr}(\xi_0) = 0$. The index form of L has the form

$$\Phi(x\xi_0 + y\eta_0) = (ax^3 + bx^2y + cxy^2)(\xi_0 \wedge \eta_0)$$

where $\mathfrak{m}_K \nmid c$, since the root is simple. When plugging in a value $\eta = x'\pi_K\xi_0 + \eta_0$ with $y = 1$, the cxy^2 term will dominate so the ring condition is $\mathfrak{m}_K^{i-2j-1}|x$: we get q^j rings. But $\mathrm{tr}(\eta) = 1$ so the trace condition cannot be fulfilled unless $n \le j$, in which case it is vacuous. Thus we get a root

subring generating function

$$s^{\mathrm{SR}}(n) = \sum_{\substack{j \geq n \\ i \geq 2j}} q^j z^{i+j}. \tag{91}$$

Now assume that $\bar{\eta}_0$ is the *multiple* root of one of the splitting types $1^2 1$ and 1^3: that is, in a basis $(1, \xi_0, \eta_0)$ with η_0 lifting $\bar{\eta}_0$, the index form is

$$\Phi_L(x\xi_0 + y\eta_0) = (ax^3 + bx^2 y + cxy^2 + dy^3)(\xi_0 \wedge \eta_0)$$

with $\mathfrak{m}_K | c$ and $\mathfrak{m}_K | d$. A now-standard trick shows that $\mathfrak{m}_K^2 \nmid d$, that is, $v_K(d) = 1$: if not, then applying the formula (87) with $i = 0$ and $j = -1$ would show that $(1, \xi_0, (\eta_0 + u)/\pi_K)$ is a basis of a ring for some $u \in \mathcal{O}_K$: that is, $\mathcal{O}_L$ would not be the maximal order in L. So $\mathfrak{m}_K^2 \nmid d$, and the root $\bar{\eta}_0$ mod $\mathfrak{m}_K$ has *no* lift to mod $\mathfrak{m}_K^2$. This shows that the only rings belonging to this root occur for $i = 2j + 1$, the very edge of the root zone, where the ring condition (88) is mod $\mathfrak{m}_K$ only (and is therefore automatically satisfied). There are $q^{i-j-1} = q^j$ rings.

The trace condition can be expressed in terms of the index form using the fact, previously mentioned, that

$$\mathrm{tr}(\xi_0) = -b \quad \text{and} \quad \mathrm{tr}(\eta_0) = c.$$

Thus $\mathrm{tr}(\eta) = \mathrm{tr}(x\pi_K \xi_0 + \eta_0) = c - \pi_K bx$. We may assume that $\ell = e - \min\{v_K(b), v_K(c)\} > 0$, as when $\ell = 0$ we have $n = 0$ and no trace condition. There are two cases.

⟨1⟩ If $v_K(b) \geq v_K(c)$, then $v_K(\mathrm{tr}(\eta)) = v_K(c) = e - \ell$ no matter what x we pick, and so the trace condition is unsatisfiable for all $n > j$.

⟨2⟩ But if $v_K(b) < v_K(c)$, then the equation $c - \pi_K bx = 0$ has a solution x_0, and the solutions to the trace condition

$$\frac{c - \pi_K bx}{\pi_K^{e-\ell}} \equiv 0 \mod \mathfrak{m}_K^{n-j}$$

are $x = x_0 + u$ for $v_K(u) \geq n - j - 1$ (since $v_K(b) = e - \ell$). There are $q^{i-n} = q^{2j+1-n}$ solutions.

We must now determine for which algebras L Cases ⟨1⟩ and ⟨2⟩ occur. For splitting type 1^3,

if we take our basis $(1, \xi_0, \eta_0) = (1, \pi_L, \pi_L^2)$, they match up exactly with Cases $\langle 1 \rangle$ and $\langle 2 \rangle$ in the proof of Proposition 11.9 and therefore correspond to the offsets $\theta = 0$ and $\theta = 1$, respectively. For splitting type $1^2 1$, we have $\mathfrak{m}_K \nmid b$ (since otherwise Φ would have a triple root) and again Case $\langle 2 \rangle$ occurs. Since $\theta = 1$ in this case too, we can divide up the generating functions by θ-value rather than splitting type:

$$s^{\mathrm{MR},\theta=0}(n) = \sum_{j \geq n} q^j z^{3j+1} \tag{92}$$

$$s^{\mathrm{MR},\theta=1}(n) = \sum_{j \geq n} q^j z^{3j+1} + \sum_{\frac{n-1}{2} \leq j < n} q^{2j+1-n} z^{3j+1}. \tag{93}$$

We have left out the case $\theta = -1$ of the uniformizer radical extensions. For these, $n = 0$, so the trace condition is vacuous and either (92) or (93) yields the correct generating function

$$s^{\mathrm{MR}}(0) = \sum_{j \geq 0} q^j z^{3j+1}. \tag{94}$$

11.2.6 Putting it together

The subring generating functions $s^{\sigma,\theta}(n)$ are now derived by summing the free-zone and root-zone contributions:

$$\begin{aligned} s^{111}(n) &= s^{\mathrm{FZ}}(n) + 3s^{\mathrm{SR}}(n) \\ s^{12}(n) &= s^{\mathrm{FZ}}(n) + s^{\mathrm{SR}}(n) \\ s^{3}(n) &= s^{\mathrm{FZ}}(n) \\ s^{1^2 1}(n) &= s^{\mathrm{FZ}}(n) + s^{\mathrm{SR}}(n) + s^{\mathrm{MR},\theta=1}(n) \\ s^{1^3,\theta}(n) &= s^{\mathrm{FZ}}(n) + s^{\mathrm{MR},\theta}(n). \end{aligned} \tag{95}$$

The proof of Lemma 11.13 is now complete.

Proof of Lemma 11.15. It is possible to prove Lemma 11.15 in an automated fashion by summing the doubly geometric series (90), (91), (92), and (93), solving the linear recurrences (78)–(83), and checking that the resulting rational functions agree for both even and odd n. We here present a

more illuminating method, which does not attempt to sum all the series but simply manipulates their terms—that is, it is very nearly a bijective proof.

We begin with a simplification of the generating functions $s^{1^3,\theta=0}$ and $s^{1^3,\theta=1}$.

Lemma 11.16.

$$s^{1^3,\theta=0}(n) = \sum_{\substack{a\geq 0 \\ b\geq \max\{3a,\frac{3a+3n}{2}\}}} q^a z^b \tag{96}$$

$$s^{1^3,\theta=1}(n) = \sum_{\substack{a\geq 0 \\ b\geq \max\{3a,\frac{3a+3n-1}{2}\}}} q^a z^b \tag{97}$$

Proof. We have

$$\begin{aligned} s^{1^3,\theta=0}(n) &= s^{\mathrm{FZ}}(n) + s^{\mathrm{MR},\theta=0}(n) \\ &= \sum_{j<n\leq i\leq 2j} q^{i-n}z^{i+j} + \sum_{n\leq j<i\leq 2j} (q+1)q^{i-j-1}z^{i+j} + \sum_{n\leq j=i} z^{i+j} + \sum_{j\geq n} q^j z^{3j+1}. \end{aligned}$$

Splitting the two summands in the $(q+1)$ factor and combining the former with the third sum,

$$s^{1^3,\theta=0}(n) = \sum_{j<n\leq i\leq 2j} q^{i-n}z^{i+j} + \sum_{n\leq j<i\leq 2j} q^{i-j}z^{i+j} + \sum_{n\leq j<i\leq 2j} q^{i-j-1}z^{i+j} + \sum_{j\geq n} q^j z^{3j+1}.$$

Reindexing the third sum by $i \mapsto i+1$,

$$\begin{aligned} s^{1^3,\theta=0}(n) &= \sum_{j<n\leq i\leq 2j} q^{i-n}z^{i+j} + \sum_{n\leq j<i\leq 2j} q^{i-j}z^{i+j} + \sum_{n\leq j\leq i\leq 2j+1} q^{i-j}z^{i+j+1} + \sum_{j\geq n} q^j z^{3j+1} \\ &= \sum_{j<n\leq i\leq 2j} q^{i-n}z^{i+j} + \sum_{n\leq j<i\leq 2j+1} q^{i-j}z^{i+j} + \sum_{n\leq j\leq i\leq 2j+1} q^{i-j}z^{i+j+1}. \end{aligned}$$

It is now not hard to check that the last two sums together include every term $q^a z^b$ with $a \geq 0$ and $b \geq \max\{3a, a+2n\}$ exactly once. As for the first sum, it includes every term with $a \geq 0$ and $\frac{3a+3n}{2} \leq b \leq a+2n$ exactly once. So we have (96).

To prove (97), it suffices to tack on the additional root-zone terms

$$s^{\mathrm{MR},\theta=1}(n) - s^{\mathrm{MR},\theta=0}(n) = \sum_{\frac{n-1}{2} \le j < n} q^{2j+1-n} z^{3j+1} = \sum_{\substack{0 \le a < n \\ b = \frac{3a+n-1}{2}}} q^a z^b. \qquad \blacksquare$$

In other words, $s^{1^3,\theta}(n)$ can be viewed as a sum of terms $q^a z^b$ for integer points (a, b) in a certain region $\mathcal{R}$:

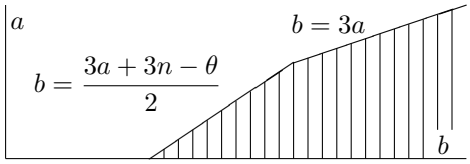


Figure 2: Terms $q^a z^b$ appearing in the count of traced orders of a totally ramified cubic field

In proving (78) and (79), we observe that changing n and θ moves only the left side of the region $\mathcal{R}$, while multiplication by powers of z moves the whole region to the right. The differences appearing in (78) and (79) have the pleasant property that the composite of these two transformations causes the left sides to coincide, causing cancellation everywhere but along the top side $b = 3a$. In symbols:

$$\begin{aligned} s^{1^3,\theta=0}(n) - z^2 s^{1^3,\theta=1}(n-1) &= \sum_{\substack{a \ge 0 \\ b \ge \max\{3a, \frac{3a+3n}{2}\}}} q^a z^b - \sum_{\substack{a \ge 0 \\ b \ge \max\{3a+2, \frac{3a+3n}{2}\}}} q^a z^b \\ &= \sum_{\substack{a \ge n \\ 3a \le b \le 3a+1}} q^a z^b \\ &= (1+z) \sum_{a \ge n} q^a z^{3a} \\ &= \frac{(1+z) q^n z^{3n}}{1 - qz^3} \\ &= q^n z^{3n} (1 - z^2) s^{1^3}(0). \end{aligned}$$

This proves (78), and the proof of (79) is analogous.

As for equations (80)–(83), the linear combination (78) − (80) reduces to a formula for $s^{\mathrm{MR},\theta=0}$,

$$s^{\mathrm{MR},\theta=0}(n) = q^n z^{3n+1} (1 - z) s^{1^3}(0),$$

while the linear combinations (81) − (80), (79) − (82), and (83) all reduce to a formula for s^{SR}:

$$s^{\mathrm{SR}}(n) = q^n z^{3n+1} s^{1^3}(0).$$

These formulas are easily derived from the series formulations (92) and (91). ■

Also easily derived from the foregoing is a formula for the number of traced orders in a given cubic algebra, in other words, for the coefficient of a single power z^b in one of the series $g(L,t)$:

Theorem 11.17 (the traced subring zeta function). *Let L be a cubic algebra over a 3-adic field K with discriminant $\operatorname{disc} L = \mathfrak{m}_K^{d_0}$. Let d and t be integers satisfying the necessary restrictions*

$$d \geq d_0, \quad d \equiv d_0 \mod 2, \quad 0 \leq t \leq e_K.$$

Then the number $g(L,d,t)$ of $\mathfrak{m}_K^t$-traced orders of discriminant $\mathfrak{m}_K^d$ in L is a linear combination of the three functions

$$g^{1^3}(d_0,d,t) = \frac{q^r-1}{q-1}, \quad r = \begin{cases} 0, & d < 3t \\ \left\lfloor \frac{d}{3} \right\rfloor - t + 1, & 3t \leq d \leq 6t - d_0 \\ \left\lfloor \frac{d-d_0}{6} \right\rfloor + 1, & d \geq 6t - d_0 \end{cases}$$

$$g^3(d_0 = 0,d,t) = \frac{q^r-1}{q-1}, \quad r = \begin{cases} 0, & d < 3t \\ \left\lfloor \frac{d}{3} \right\rfloor - t + 1, & 3t \leq d \leq 6t \\ \frac{d}{2} - 2\left\lceil \frac{d}{6} \right\rceil + 1, & d \geq 6t \end{cases}$$

$$g^{\mathrm{SR}}(d_0 = 0 \text{ or } 1,d,t) = \frac{q^r-q^t}{q-1}, \quad r = \begin{cases} t, & d < 6t \\ \left\lfloor \frac{d}{6} \right\rfloor - t + 1, & d \geq 6t \end{cases}$$

in a manner dependent on the splitting type of L:

- $\sigma(L) = 1^3$*:* $g = g^{1^3}$

- $\sigma(L) = 1^2 1$: $g = g^{1^3} + g^{\mathrm{SR}}$
- $\sigma(L) = 3$: $g = g^3$
- $\sigma(L) = 12$: $g = g^3 + g^{\mathrm{SR}}$
- $\sigma(L) = 111$: $g = g^3 + g^{3\mathrm{SR}}$.

Remark 11.18. When $t = 0$ (and here we need no longer assume that $\operatorname{char} k_K = 3$), we recover the formulas for orders in a cubic field computed by Datskovsky and Wright and written more explicitly by Nakagawa and the author.

11.3 A bijective proof of the wild case

Ideally we would desire a bijective proof of global reflection identities such as Theorem 11.3. This is still beyond reach. However, using the machinery of Galois cohomology and Poitou-Tate duality, we reduced this theorem to a local result, Theorem 11.14. In this section we will prove this theorem using a bijective method.

It is not obvious what "bijective" means when trying to prove that two local weightings are Fourier transforms of each other. Recall that in Theorem 7.1, we constructed *level spaces* $H^1(T) \supseteq \mathcal{L}_0 \supsetneq \mathcal{L}_1 \supsetneq \cdots \supsetneq \mathcal{L}_e$ with the property that, for i,

$$\mathcal{L}_i^{\perp} = \mathcal{L}_{e-i}. \tag{98}$$

As in the preceding proof, we extend this notation slightly. If $\mathcal{L}_e \neq \{0\}$, which happens exactly when $T \cong K \times K$ is split, then let $\mathcal{L}_{e+1} = \{0\}$; and dually, if $\mathcal{L}_0 \neq H^1(T)$, which happens exactly when T' is split, then let $\mathcal{L}_{-1} = H^1(T)$. Then $\mathcal{L}_e \setminus \mathcal{L}_{e+1}$ consists of the unramified field extension of K, and $\mathcal{L}_{-1} \setminus \mathcal{L}_0$ consists of the *uniformizer radical extensions (UREs)* $K[\sqrt[3]{\pi}]$, the cubic extensions of maximal discriminant-valuation $3e + 2$. We have

$$\widehat{\mathbf{1}_{\mathcal{L}_{e+1}}} = \frac{1}{3}\mathbf{1}_{\mathcal{L}_{-1}} \quad \text{and} \quad \widehat{\mathbf{1}_{\mathcal{L}_{-1}}} = 3q^e \mathbf{1}_{\mathcal{L}_{e+1}}.$$

We also let

$$\ell_{\min} = \begin{cases} -1 & T' \cong K \times K \\ 0 & \text{otherwise,} \end{cases} \qquad \mathcal{L}_{\min} = \mathcal{L}_{\ell_{\min}} = H^1(T),$$

$$\ell_{\max} = \begin{cases} e+1 & T \cong K \times K \\ e & \text{otherwise,} \end{cases} \qquad \mathcal{L}_{\max} = \mathcal{L}_{\ell_{\max}} = \{0\}.$$

The level spaces $\mathcal{L}_i$ and their associated characteristic functions L_i will be central to our proof. Our strategy is as follows: we group all cubic rings whose resolvent torsor is T into *families* $\mathcal{F}$ with the following properties:

- All rings in a family have the same discriminant and trace ideal.
- All rings in a family $\mathcal{F}$ are contained in étale algebras L belonging to some level space $\mathcal{L}_i$; this $\mathcal{L}_i$ is called the *support* $\mathrm{supp}(\mathcal{F})$ of the family.
- Each $L \in \mathcal{L}_i$ has the same number of orders in the family; this number is called the *thickness* $\mathrm{th}(\mathcal{F})$ of the family.

The proof of Theorem 11.14 will then consist in exhibiting an involution between the families of support $\mathcal{L}_i$ and $\mathcal{L}_{e-i}$ which affects their thicknesses, discriminants, and trace ideals in such a manner that they contribute equally to both sides of the theorem. The remainder of this section will be spent in carrying this out.

Lemma 11.19. *Let T/K be a quadratic torsor and let $n_T = v_K(\mathrm{disc}\, T) \in \{0, 1\}$.*

Then the cubic orders whose resolvent torsor is T can be partitioned into families $\mathcal{F}_{n,k}$ indexed by the pairs of integers (n, k) satisfying the conditions

$$0 \le k \le \left\lfloor \frac{n}{3} \right\rfloor, \quad n \equiv n_T \mod 2,$$

with the following properties:

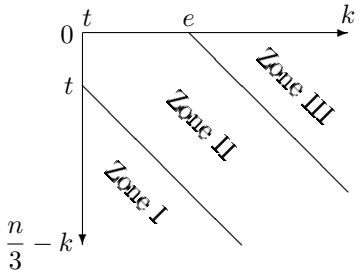
1. *The rings in $\mathcal{F}_{n,k}$ have discriminant ideal (π^n) and trace ideal $(\pi^{\min\{k,e\}})$.*

2. *The support and thickness of each $\mathcal{F}_{n,k}$ depend on which of three zones the pair (n,k) belongs to, as follows:*

Zone	(n,k)	$\mathrm{supp}(\mathcal{F}_{n,k})$	$\mathrm{th}(\mathcal{F}_{n,k})$
I	$0 \le k < \frac{n}{6}$	$\mathcal{L}_{\max}$	$\lvert H^0(T)\rvert$
II	$\frac{n}{6} \le k \le \left\lfloor \frac{n}{3} \right\rfloor - \frac{n}{6} + \frac{e}{2}$	$\mathcal{L}_{e-2k+\lfloor \frac{n}{3} \rfloor}$	$q^{\lfloor \frac{n}{3} \rfloor - k}$
III	$\left\lfloor \frac{n}{3} \right\rfloor - \frac{n}{6} + \frac{e}{2} < k \le \left\lfloor \frac{n}{3} \right\rfloor$	$\mathcal{L}_{\min}$	$q^{\lfloor \frac{n}{3} \rfloor - k}$

(99)

The relative positions of these zones follow a pattern like that in quadratic O-N, up to $O(1)$ discrepancies in the indices:



Proof of Theorem 11.14. Once Lemma 11.19 is proved, we can prove Theorem 11.14 quite simply by sending the family $\mathcal{F} = \mathcal{F}_{n,k}$ to $\mathcal{F}' = \mathcal{F}_{n',k'}$, where

$$n' = n + 3e - 6t$$
$$k' = \left\lfloor \frac{n}{3} \right\rfloor - k + e - t.$$

If the original $\mathcal{F}$ satisfied the bounds $t \le k \le \lfloor \frac{n}{3} \rfloor$, then it is easy to see that $t' \le k' \le \lfloor \frac{n}{3} \rfloor$ where $t' = e - t$, and likewise $n \equiv n_T \bmod 2$ implies $n' \equiv n_{T'}$. Thus $\mathcal{F}'$ is a family of rings of resolvent torsor T' whose trace ideal is contained in (π^{e-t}). It is not hard to see that $\mathcal{F}'$ lies in zone III, II,

or I according as $\mathcal{F}$ lies in zone I, II, or III. We leave it to the reader to check the needed identities

$$\begin{aligned} \operatorname{supp}(\mathcal{F}') &= \operatorname{supp}(\mathcal{F})^{\perp} \\ \operatorname{th}(\mathcal{F}') &= \frac{|\operatorname{supp}(\mathcal{F})|}{|H^0(T)|} \cdot \operatorname{th}(\mathcal{F}). \end{aligned}$$

■

Remark 11.20. Zone I, which is supported on $\mathcal{L}_{\max} = \{0\}$, consists precisely of those rings whose structure uses in an essential way that L is *split,* that is, has more than one field factor. Zone II has the approximate shape of a band of constant width,

$$\frac{n}{6} \leq k \leq \frac{n}{6} + \frac{e}{2};$$

but the dependency on the value of n modulo 3 attests to a waviness of the boundary between zones II and III that cannot be avoided.

Proof of Lemma 11.19. We now begin to enumerate all the orders in every cubic K-algebra L and arranging them into families. Let $\operatorname{disc} \mathcal{O}_L = (\pi^{n_0})$ and $\operatorname{tr}(\mathcal{O}_L) = (\pi^{k_0})$, and let $\theta = n_0 - 3k_0$. As our investigations of the structure of cubic fields have found, we have $\theta \in \{0, 1, 2\}$, the case $\theta = 2$ corresponding to the URE.

Let $[1, \xi_0, \eta_0]$ be a basis for $\mathcal{O}_L$. We can arrange so that η_0 is traceless and $\operatorname{tr}(\xi_0)$ is a generator for the trace ideal $\operatorname{tr}(\mathcal{O}_K)$. Any order $C \subseteq L$ then has a unique basis of the form

$$[1, \quad \xi = \pi^i \xi_0 + u\eta_0, \quad \eta = \pi^j \eta_0] \tag{100}$$

where i and j are nonnegative integers and u ranges over a system of coset representatives in $\mathcal{O}_K / \pi^j \mathcal{O}_K$. (Note the departure from the reduced basis used in the preceding subsection.) Such a C has discriminant valuation

$$n = v(\operatorname{disc} C) = n_0 + 2i + 2j$$

and trace ideal

$$(3, \mathrm{tr}(\pi^i \xi_0)) = \pi^{\min\{e, k_0+i\}}.$$

Let $k = k_0 + i$. With one exception, namely when L is a URE (which case we will handle later), we will place such a ring C into the family $\mathcal{F}_{n,k}$. We must now compute the sizes of the families we have thus constructed.

Whether or not a lattice C with a basis (100) is actually a ring is determined by the integrality of its *index form*. The following lemma reduces the number of coefficients to be checked from four to two.

Lemma 11.21. *Let $\xi, \eta \in \mathcal{O}_L$ be integral elements of a nondegenerate cubic algebra L over the field of fractions K of a Dedekind domain $\mathcal{O}_K$ such that the sublattice $C = \mathcal{O}_K \langle 1, \xi, \eta \rangle$ is of full rank. If the outer coefficients*

$$\Phi_C(\xi) = \frac{\Phi_{\mathcal{O}_L}(\xi)}{\pi^{[\mathcal{O}_L : C]}} \quad \textit{and} \quad \Phi_C(\eta) = \frac{\Phi_{\mathcal{O}_L}(\eta)}{[\mathcal{O}_L : C]}$$

of the index form of C are integral, then the entire index form of C is integral and C is a ring.

Proof. If the whole index form of C is integral, then there is a ring $C' = \langle 1, \xi', \eta' \rangle$ with the same index form (with respect to its basis) as C. Using the identity of index forms for L over K, we can embed C' into L with $\xi' = \xi + u$, $\eta' = \eta + v$ for some $u, v \in K$. But since ξ', ξ, η', η are integral elements and $\mathcal{O}_K$ is integrally closed, we have $u, v \in \mathcal{O}_K$ so $C' = C$.

So it suffices to prove that the index form is integral. This is a local statement, so we may assume that $\mathcal{O}_K$ is a DVR. Passing to a finite extension, we may assume that $L \cong K \times K \times K$ is totally split. Let

$$\xi = (a_1; a_2; a_3) \quad \text{and} \quad \eta = (b_1; b_2; b_3).$$

Then

$$D = [\mathcal{O}_L : C] = \det \begin{bmatrix} 1 & 1 & 1 \\ a_1 & a_2 & a_3 \\ b_1 & b_2 & b_3 \end{bmatrix}$$

We are given that the outer coefficients

$$c_0 = \frac{1}{D}(a_1 - a_2)(a_2 - a_3)(a_3 - a_1) \quad \text{and} \quad c_3 = \frac{1}{D}(b_1 - b_2)(b_2 - b_3)(b_3 - b_1)$$

of the index form of C are integral. We wish to prove that the same applies to the two middle coefficients. By symmetry, we can consider just the x^2y-coefficient

$$c_1 = \frac{1}{D}\left[\sum_{i=1}^{3}(a_i - a_{i+1})(a_{i+1} - a_{i+2})(b_{i+2} - b_i)\right].$$

(Here, and for the rest of the proof, indices are modulo 3.) It is easy to verify that

$$c_1 = -a_1 + 2a_2 - a_3 + \frac{3}{D}(a_1 - a_2)(a_2 - a_3)(b_3 - b_1).$$

So it is enough to show that

$$d_1 = \frac{1}{D}(a_1 - a_2)(a_2 - a_3)(b_3 - b_1)$$

is integral, or more generally any of the three

$$d_i = \frac{1}{D}(a_i - a_{i+1})(a_{i+1} - a_{i+2})(b_{i+2} - b_i).$$

But we see that

$$a_0^2 a_3 = d_1 d_2 d_3.$$

Since a_0 and a_3 have nonnegative valuation, the three d_i cannot all have negative valuation, completing the proof. ■

Remark 11.22. The hypothesis that L be nondegenerate is likely nonessential.

We can now resume the proof of Lemma 11.19. Let the index form of $\mathcal{O}_L$ be

$$\Phi_{\mathcal{O}_L}(x\xi_0 + y\eta_0) = ax^3 + bx^2y + cxy^2 + dy^3.$$

Of the coefficients of the index form of C, we focus on the outer coefficients,

$$\Phi_C(\xi) = \frac{a\pi^{3i} + b\pi^{2i}u + c\pi^i u^2 + du^3}{\pi^{i+j}} \quad \text{and} \quad \Phi_C(\eta) = d\pi^{2j-i}.$$

The latter coefficient is the simpler one, depending only on i and j. Due to the tracelessness of η_0, we have $3|c$. We must then have $\pi^2 \nmid d$, or else $\mathcal{O}_L$ would be nonmaximal, and the discriminant analysis of Proposition 11.9 shows that $v_K(d) = \theta$. Thus the condition $\Phi_C(\eta) \in \mathcal{O}_K$ comes out to $2j - i + \theta \geq 0$, which simplifies to $n \geq 3k$.

(Incidentally, when $k \leq e$, the relation $n \geq 3k$ expresses an important relation between the trace ideal of a ring and its discriminant, generalizing the observation that an integer-matrix cubic form has discriminant divisible by 27.)

There thus remains the ξ-condition $\Phi_C(\xi) \in \mathcal{O}_K$, which informally states that ξ is a root of $\Phi_{\mathcal{O}_L}$ modulo π^{i+j}. Now $\Phi_{\mathcal{O}_L}$ is a homogeneous binary form, and it is natural to consider its roots on the projective lines $\mathbb{P}^1(\mathcal{O}_K/\pi^m)$; the factorization over the field $\mathcal{O}_K/\mathfrak{m}$, for instance, gives the splitting type $\sigma(\mathcal{O}_L)$. However, in our situation there is a distinguished point on this projective line, at least for $m < e - k_0$, namely the traceless point η_0: and the line is thereby subdivided into an affine line and a portion at infinity. The point at infinity mod $\mathfrak{m}$ is a root of $\Phi_{\mathcal{O}_L}$ if and only if $\theta > 0$. This is the motivation for the calculations to be undertaken now.

Suppose first that we are in zone I, that is, $n > 6k$, which translates into $j > 2i + \theta$. Then the $\Phi_C(\xi)$ condition

$$\pi^{j-2i} \mid a + bu\pi^{-i} + cu^2\pi^{-2i} + du^3\pi^{-3i}$$

is clearly dominated by a non-integral last term unless u is of the form $\pi^i u'$, in which case it simplifies

to

$$\pi^{j-2i} \mid a + bu' + cu'^2 + du'^3.$$

In other words, $\xi_0 + u'\eta_0$ must be a root of $\Phi_{\mathcal{O}_L}$ modulo $\mathfrak{m}^{j-2i}$. The condition $j - 2i > \theta$ rules out any contribution from a multiple root modulo $\mathfrak{m}$, which never lifts to mod $\mathfrak{m}^2$ (or else $\mathcal{O}_L$ would be nonmaximal). So the only roots that contribute are the *simple* roots occurring if L has splitting type 111, 12, or 1^21. There are $|H^0(T)|$ simple roots, and none of them are traceless (to be explicit, they are at $(1;0)$ for each decomposition $L \cong K \times T$ into a linear and a quadratic algebra). By Hensel's lemma, each simple root has a unique lift to any modulus. So the solutions u' form a union of $|H^0(T)|$ congruence classes modulo $\mathfrak{m}^{j-2i}$. Since $u' = u/\pi^i$ is defined modulo $\mathfrak{m}^{j-i}$, there are

$$|H^0(T)| \cdot q^i = |H^0(T)| \cdot q^k$$

rings for each pair (i, j). This completes the construction of the families $\mathcal{F}_{n,k}$ in zone I.

Now suppose that (n, k) is in zone II or III, still assuming that L is *not* a URE: we have

$$3k \leq n \leq 6k$$

or, and the (i, j) coordinates,

$$i \leq 2j + \theta \quad \text{and} \quad j \leq 2i + \frac{n_0}{2} - \theta. \tag{101}$$

We claim that there are rings for this pair (i, j) if and only if $L \in \mathcal{L}_{e-2k+\lfloor \frac{n}{3} \rfloor}$, which may be also written as $k_0 \leq 2k - \frac{n-2}{3}$ or in (i, j) coordinates as

$$j \leq 2i + 1 - \theta. \tag{102}$$

Assume first that $k_0 > 0$, that is, L has splitting type 1^3. Then the structure of L, and the fact that ξ is a *depth element* (a generator of the trace ideal) imply that $v_L(\xi) = 2 - \theta$, and hence that

$v_K(a) = 1 - \theta$. Now it is easy to show that

$$v(\Phi_{\mathcal{O}_L}(\xi)) = v(a\pi^{3i} + bu\pi^{2i} + cu^2\pi^i + du^3) = \min\{3i + 1 - \theta, 3v(u) + \theta\}$$

because the sum is dominated by its first term if $\pi^{i+1-\theta}|u$ and by its last term otherwise. So a necessary condition for there to be rings is that $i + j \leq 3i + 1 - \theta$, which is equivalent to (102). If this condition holds, then the ξ-condition simply becomes

$$v(u) \geq \frac{i + j - \theta}{3} \tag{103}$$

and we get

$$q^{j - \lceil \frac{i+j-\theta}{3} \rceil} = q^{\lfloor \frac{2j+\theta-i}{3} \rfloor} = q^{\lfloor \frac{n}{3} - k \rfloor}$$

solutions.

If L has one of the other splitting types, then our task is simplified by the facts that $k_0 = 0$ and $n_0 = \theta \in \{0, 1\}$. Note that the second inequality of (101) implies (102), so we are only trying to prove that there *are* solutions in this case. If (103) does *not* hold, then the du^3 term dominates in $\Phi_{\mathcal{O}_L}(\xi)$ and we do not get a solution. If (103) holds, we leave it to the reader to check the inequalities that imply (even without knowing anything about a, b, and c) that π^{i+j} divides each term of $\Phi_{\mathcal{O}_L}(\xi)$. So we get the same number of solutions as in the preceding case.

Lastly, we must address the exceptional case that $L = K[\sqrt[3]{\pi}]$ is a URE. We take $\xi = \sqrt[3]{\pi}$ and $\eta = (\sqrt[3]{\pi})^2$, which are both traceless; and we have the explicit index form

$$\Phi_{\mathcal{O}_L}(x\xi + y\eta) = x^3 - \pi y^3.$$

This resembles the index form for a ramified L with $\theta = 1$, and analogously to that case, we compute that rings appear only for the pairs (i, j) with

$$i \leq 2j + 1 \quad \text{and} \quad j \leq 2i, \tag{104}$$

each such (i,j) yielding $q^{\left\lfloor \frac{2j+\theta-i}{3} \right\rfloor}$ solutions. Now we come to the least satisfying part of the bijection. In the absence of a distinguishing k (since all these rings are (3)-traced), we we simply have to place these rings into the families $\mathcal{F}_{n,k}$ of zone III so that the discriminant valuations and thicknesses match up. There is a unique choice:

$$\begin{aligned} n &= n_0 + 2i + 2j = 3e + 2i + 2j + 2 \\ k &= \left\lfloor \frac{n}{3} \right\rfloor - \left\lfloor \frac{2j+1-i}{3} \right\rfloor. \end{aligned}$$

We leave it to the reader that this establishes a bijection between the pairs (i,j) in the region (104) with the pairs (n,k) in zone III. The discriminant and thickness are correct by construction, completing the proof. ■

Remark 11.23. This lemma also yields a second proof of the number of t-traced rings of discriminant $\mathfrak{m}_K^n$ in a cubic algebra (Theorem 11.17).

Remark 11.24. The method of the above proof can also be adapted to the tame case.

12 Non-natural weightings

Now that we know that the integral models $V_{\mathfrak{t}}$, $V_{3\mathfrak{t}^{-1}}$ of binary cubic forms are naturally dual, we can further look for duals for *non-natural* weightings. This has applications to counting cubic rings satisfying local conditions. We restrict ourselves to primes not dividing 3∞.

For simplicity we work over $\mathbb{Z}$, though the techniques extend. Denote by M_D the group $\mathbb{Z}/3\mathbb{Z}$ with Galois action given by the quadratic character corresponding to $\mathbb{Q}(\sqrt{D})$. Denote by $V(R)$ the space of binary cubic forms over a ring R.

As in Section 8, if $W : V(\mathcal{O}_{\mathbb{A}_\mathbb{Q}}) \to \mathbb{C}$ is a locally constant weighting invariant under $\mathrm{GL}_2(\mathcal{O}_{\mathbb{A}_\mathbb{Q}})$, we denote by $h(D,W)$ the number of $\mathrm{GL}_2\mathbb{Z}$-classes of binary cubic forms over $\mathbb{Z}$ of discriminant D, each form Φ weighted by

$$\frac{W(\Phi)}{|\mathrm{Stab}_{\mathrm{GL}_2\mathbb{Z}}\,\Phi|}.$$

If $W = \prod_p W_p$ is a product of local weightings, then our local-to-global reflection engine (Theorems 8.12 and 8.13) produces identities relating different $h(D, W)$, if we can find a dual for each W_p.

12.1 Local weightings given by splitting types

Let $\sigma \in \{111, 12, 3, 1^21, 1^3, 0\}$ be one of the six *splitting types* a binary cubic form can have at a prime. Let

$$T(\sigma) = T_p(\sigma) : V(\mathbb{Z}_p) \to \{0, 1\}$$

be the selector that takes the value 1 on binary cubic forms of splitting type σ. Then the associated weighted local orbit counter

$$g_D\left(T_p(\sigma)\right) : H^1\left(\mathbb{Q}_p, M_D\right) \to \mathbb{N}$$

attaches to each cubic algebra L of discriminant $K(\sqrt{D})$ its number of orders of discriminant D and splitting type σ.

There is another construction of interest to us. If $a \in \mathbb{Q}$, then the varieties

$$V_{\mathbb{Z}}(D = D_0) \quad \text{and} \quad V_{\mathbb{Z}}(D = a^2 D_0) \tag{105}$$

do not in general look alike. However, their base-changes to $\mathbb{Q}$ are isomorphic, being related by any $g \in \mathrm{GL}_2(\mathbb{Q})$ of determinant a. Hence the two varieties (105) can be viewed as two integral models for $V_{\mathbb{Q}}(D = D_0)$. Coupled with Theorem 8.13, this viewpoint is very flexible. We denote by Z_p the transformation that applies

$$\begin{bmatrix} 1/p & \\ & 1 \end{bmatrix}$$

to the vectors of an integral model of $V_{\mathbb{Q}}$ and conjugates $\mathcal{G}$ accordingly. Observe that

$$g_D\left(T_p(\sigma) Z_p^n\right) = g_{Dp^{-2n}}\left(T_p(\sigma)\right),$$

and similarly for global class numbers. It is not hard to see that $h(D, W)$ is meaningful for any W

in the $\mathbb{Q}$-algebra generated by the $T_p(\sigma)$'s and the Z_p's for all p.

Over $\mathbb{Z}_p$, we still have Z_p, and we sometimes omit the subscript, as every Z_ℓ with $\ell \neq p$ has no effect on the integral model. We define $Z = Z_\pi$ for integral models over a general local field similarly.

Lemma 12.1. *Let K be a local field,* $\operatorname{char} k_K \neq 3$*, and let $D \in \mathcal{O}_K \backslash \{0\}$. Then the weightings*

$$T(1^3)Z \quad \textit{and} \quad 2 \cdot T(111) - T(3)$$

are dual with duality constant 1*; that is, the associated local orbit counters satisfy*

$$\hat{g}_{-3\pi^2 D}(1^3) = 2g_D(111) - g_D(3). \tag{106}$$

Proof. The right-hand side of (106) can be written as

$$|H^0(M_D)| \cdot \mathbf{1}_0 - \mathbf{1}_{H^1_{\mathrm{ur}}},$$

so it suffices to show that the left-hand side is the Fourier transform of this, namely

$$1 - \mathbf{1}_{H^1_{\mathrm{ur}}} = \mathbf{1}_{H^1_{\mathrm{ram}}}.$$

Look at binary cubic forms $f(x, y)$ of splitting type 1^3 and discriminant $-3\pi^2 D$. Changing coordinates, we can assume

$$f(x, y) = ax^3 + bx^2y + cxy^2 + dy^3 \equiv x^3 \mod \pi.$$

Then note that $\operatorname{disc} f \equiv -27a^2d^2 \equiv -27d^2 \bmod \pi^3$, so the only way that f can have discriminant $-3\pi^2 D$ is if $\pi^2 \nmid d$. Then f is an Eisenstein polynomial, the index form of a maximal order in a totally ramified extension L. Hence the weighting counting such f is $\mathbf{1}_{H^1_{\mathrm{ram}}}$, as desired. ∎

Plugging this, together with the natural duality of Theorem 11.2 at the other primes, into Theorem 8.12 yields results such as the following:

Theorem 12.2. *Let $p \in \mathbb{Z}$ be a prime, $p \neq 3$. For all integers D such that $p \nmid D$,*

$$\frac{1}{c_\infty} h_3(-27p^2D, T_p(1^3)) = 2h(D, T_p(111)) - h(D, T_p(3)) \tag{107}$$

$$c_\infty h(p^2D, T_p(1^3)) = 2h_3(-27D, T_p(111)) - h_3(-27D, T_p(3)) \tag{108}$$

where $c_\infty = 3$ for $D > 0$, $c_\infty = 1$ for $D < 0$.

12.2 Discriminant reduction

This can be used to improve a step that often occurs in arithmetic statistics, namely the production of *discriminant-reducing* identities that express the number of forms with certain non-squarefree discriminant in terms of lower discriminants.

For N a positive integer, let $h(D, R_N)$ be the number of classes of binary cubic forms of discriminant D, each weighted not only by the reciprocal of its number of automorphisms but also by its *number of roots* in $\mathbb{P}^1(\mathbb{Z}/N\mathbb{Z})$. Equivalently, consider the natural congruence subgroup

$$\mathrm{G}\Gamma^0(N) = \left\{ \begin{bmatrix} a & b \\ c & d \end{bmatrix} \in \mathrm{GL}_2(\mathbb{Z}) : b \equiv 0 \mod N \right\},$$

and let $h(D, R_N)$ be the number of $\mathrm{G}\Gamma^0(N)$-orbits of cubic $111N$-forms (integral forms with a marked root) of discriminant D over $\mathbb{Z}$, each weighted by the reciprocal of its stabilizer in $\mathrm{G}\Gamma^0(N)$. (If $N > 1$, it is easy to prove that these stabilizers are trivial.) If $3 \nmid N$, denote by $h_3(D, R_p)$ the analogous weighted count of $133N$-forms. For a prime $N = p$, we have

$$h(D, R_p) = 3h\left(D, T_p(111)\right) + h\left(D, T_p(12)\right) + 2h\left(D, T_p(1^21)\right) + h\left(D, T_p(111)\right) + (p+1)h\left(D, T_p(0)\right).$$

This enables us to state succinctly the following theorem.

Theorem 12.3 (discriminant reduction). *Let $p \neq 3$ be a prime, and D an integer divisible by p^2. Then*

$$h(D) = h\left(\frac{D}{p^2}, R_p\right) + h\left(\frac{D}{p^4}\right) - h\left(\frac{D}{p^4}, R_p\right) + \frac{1}{c_\infty}\left(2h_3\left(\frac{-27D}{p^2}, T_p(111)\right) - h_3\left(\frac{-27D}{p^2}, T_p(3)\right)\right),$$

where $c_\infty = 3$ for $D > 0$, $c_\infty = 1$ for $D < 0$.

Proof. The cubic rings C counted by the left-hand side can be divided into maximal and nonmaximal at p. If C is maximal at p, then $C \otimes_{\mathbb{Z}} \mathbb{Z}_p$ is the ring of integers of a totally tamely ramified cubic extension of $\mathbb{Q}_p$ and $p^2 \parallel D$. By Theorem 12.2, such rings are counted by the last term.

If C is nonmaximal at p, then C sits with p-power index inside an overring C'. By considering $C' + pC$, we can take an inclusion $C \subset C'$ of one of the following forms:

- C has index p in a $C' = C_1$ of discriminant D/p^2. Here the index form of C_1 must have a marked root modulo p so that the transformation

$$\Phi_{C_1}(x, y) = ax^3 + bx^2y + cxy^2 + dy^3 \longmapsto \Phi_C(x, y) = p^2ax^3 + pbx^2y + cxy^2 + \frac{d}{p}y^3$$

  keeps the form integral. This accounts for the term $h(D/p^2, R_p)$.

- C has index p^2 in a $C' = C_2$ of discriminant D/p^4 with $C_2/C \cong (\mathbb{Z}/p\mathbb{Z})^2$. This requires that the index form of C have *content* divisible by p; we have

$$\Phi_C = \frac{1}{p}C_2.$$

  This accounts for the term $h(D/p^4)$.

Observe that C_2 is unique if it exists. A choice of C_1 corresponds to a choice of multiple root of Φ_C, which is unique if Φ_C is nonzero modulo p. Thus, the only chance of overcounting occurs when a C admits both a C_2 and one or more C_1's. The C_1's are all the subrings of index p in C_2 and thus correspond to the roots of Φ_{C_2} modulo p. So we subtract 1 (more precisely, $1/|\operatorname{Aut} C_2|$) for each

root of a form Φ_{C_2} counted in the term $h(D/p^4)$. That is, we subtract $h(D/p^4, R_p)$, yielding the claimed total. ■

More generally, we can reduce at multiple primes at once. Let $T_p^{\max} : V(\mathcal{O}_{\mathbb{A}_\mathbb{Q}}) \to \mathbb{Z}$ be the selector for rings maximal at p.

Theorem 12.4 (discriminant reduction). *Let $q = p_1 \cdots p_r$ be a squarefree integer, $3 \nmid q$. If D is a nonzero integer divisible by q^2, then for any $t < q$,*

$$h(D) = \sum_{\substack{q=q_1q_2q_3 \\ q_1 \le t}} h\left(\frac{D}{q_2^2q_3^4}, \prod_{p|q_1} T_p^{\max} \prod_{p|q_2} R_p \prod_{p|q_3}(1-R_p)\right) + \\ + \frac{1}{c_\infty} \sum_{\substack{q=q_1q_2q_3 \\ q_1 > t}} h_3\left(\frac{-27D}{q_1^2q_3^2}, \prod_{p|q_1} \mathbf{1}_{p^2\|D}(R_p - 1) \prod_{p|q_3} \mathbf{1}_{p^2\|D}(1-R_p)\right)$$

and

$$h_3(-27D) = \sum_{\substack{q=q_1q_2q_3 \\ q_1 \le t}} h_3\left(\frac{-27D}{q_2^2q_3^4}, \prod_{p|q_1} T_p^{\max} \prod_{p|q_2} R_p \prod_{p|q_3}(1-R_p)\right) + \\ + c_\infty \sum_{\substack{q=q_1q_2q_3 \\ q_1 > t}} h_3\left(\frac{D}{q_1^2q_3^2}, \prod_{p|q_1} \mathbf{1}_{p^2\|D}(R_p - 1) \prod_{p|q_3} \mathbf{1}_{p^2\|D}(1-R_p)\right).$$

Remark 12.5. If we take $t = \sqrt{q}$, we find that all discriminants appearing are at most $-27D/q$.

Proof. Since a ring of discriminant D is maximal or nonmaximal at each of the primes dividing q, we have

$$h(D) = \sum_{q_1 q_2' = q} h\left(D, \prod_{p|q_1} T_p^{\max}(1^3) \prod_{p|q_2'} T_p^{\text{nonmax}}\right),$$

where $T_p^{\max}(1^3) = T_p^{\max} \cdot T_p(1^3)$ and $T_p^{\text{nonmax}} = 1 - T_p^{\max}$ (as is natural). We transform each term in one of two ways, depending on whether $q_1 \le t$.

If $q_1 \le t$, we simply replace each T_p^{nonmax} by $Z_p R_p + Z_p^2(1-R_p)$ by the method of the preceding

theorem, which respects local conditions at other primes. We get a sum

$$\begin{aligned}
&h\left(D, \prod_{p|q_1} T_p^{\max}(1^3) \prod_{p|q_2'} T_p^{\text{nonmax}}\right) \\
&= h\left(D, \prod_{p|q_1} T_p^{\max}(1^3) \prod_{p|q_2'} (Z_p R_p + Z_p^2(1-R_p))\right) \\
&= \sum_{q_2'=q_2q_3} h\left(\frac{D}{q_2^2 q_3^4}, \prod_{p|q_1} T_p^{\max} \prod_{p|q_2} R_p \prod_{p|q_3} (1-R_p)\right).
\end{aligned}$$

If $q_1 > t$, we reflect. A dual of $T_p^{\max}$, when restricted to discriminants D that are divisible by p^2, is $\mathbf{1}_{p^2\|D} Z_p(R_p - 1)$ by Lemma 12.1. Hence a dual of $T_p^{\text{nonmax}} = 1 - T_p^{\max}$ on the same discriminants is $1 + \mathbf{1}_{p^2\|D} Z_p(1-R_p)$. Applying the reflection theorem,

$$\begin{aligned}
&h\left(D, \prod_{p|q_1} T_p^{\max}(1^3) \prod_{p|q_2'} T_p^{\text{nonmax}}\right) \\
&= \frac{1}{c_\infty} h_3\left(-27D, \prod_{p|q_1} \mathbf{1}_{p^2\|D} Z_p(R_p - 1) \cdot \prod_{p|q_2'} \left(1 + \mathbf{1}_{p^2\|D} Z_p(1-R_p)\right)\right) \\
&= \frac{1}{c_\infty} \sum_{q_2'=q_2q_3} h_3\left(\frac{-27D}{q_1^2 q_3^2}, \prod_{p|q_1} \mathbf{1}_{p^2\|D}(R_p - 1) \prod_{p|q_3} \mathbf{1}_{p^2\|D}(1-R_p)\right).
\end{aligned}$$

Summing over q_1 yields the first identity. The second is proved in the same way. ■

12.3 Subring zeta functions

Fix a local field K. Instead of restricting ourselves to local weightings taking values in $\mathbb{N}$ or $\mathbb{C}$, consider the following (generalized) local weighting:

$$\begin{aligned}
\eta_D : H^1(K, M_D) &\to \mathbb{Z}((Z)) \\
L &\mapsto \sum_{k \in \mathbb{Z}} g_{\pi^{2k} D}(L) \cdot Z^k.
\end{aligned}$$

Note that the sum is a Laurent series since the discriminant $\pi^{2k}D$ is nonintegral for k sufficiently negative. This η_D is, up to renormalizing, (a local factor of) the *subring zeta function* that plays

a central role in the study of Shintani zeta functions in works such as Datskovsky and Wright [18] and Nakagawa [38]. In like manner we can define

$$\eta_D(\sigma, L) = \sum_{k \in \mathbb{Z}} g_{\pi^{2k} D}(\sigma, L) \cdot Z^k \in \mathbb{Z}(\!(Z)\!),$$

a partial subring zeta function that picks out the subrings of splitting type σ. We can even define

$$\eta_D(\sigma Z^n) = \eta_{\pi^{-2n} D}(\sigma) = Z^n \cdot \eta_D(\sigma),$$

which explains the use of the same symbol Z for the discriminant-shift operator and the formal variable in the subring zeta function.

A formula for the subring zeta function $\eta_{\operatorname{disc} L}(L)$, without splitting-type selector, is computed by Datskovsky and Wright [18] and put into a more explicit form by Nakagawa:

Theorem 12.6 (Datskovsky–Wright; Nakagawa)**.** *The subring zeta function $\eta_{\operatorname{disc} L}(L)(Z = p^{-s})$ is given by*

$$\eta_{\operatorname{disc} L}(L) = \frac{F}{(1 - Z)(1 - qZ^3)}$$

where F is a polynomial depending on the splitting type $\sigma(\mathcal{O}_L)$ as follows.

σ_χ	F
111	$(1 + Z)^2$
12	$1 + Z^2$
3	$1 - Z + Z^2$
$1^2 1$	$1 + Z$
1^3	1

(109)

Proof. Although Datskovsky–Wright [18] and Nakagawa ([38], Lemma 3.2; see Lemma 3.6 for the simplification method) work only with cubic extensions of $\mathbb{Q}$, their method applies to this case. Alternatively, it follows immediately from Theorem 11.17. ∎

Remark 12.7. When working over the field $K = \mathbb{Q}$, the local subring zeta functions at each prime p form an Euler product expansion of the Dirichlet series

$$\frac{\zeta_L(s)}{\zeta_L(2s)}\zeta(2s)\zeta(3s-1),$$

where ζ and ζ_L are the Riemann and Dedekind zeta functions, respectively. In principle, Theorem 11.17 allow us to write each Shintani zeta function $\xi_{K,\sigma,\mathfrak{t}}$ in Definition 11.5 as an infinite sum of Euler products, one factor for each cubic étale algebra L/K, as was done for $\mathfrak{t} = (1)$ by Datskovsky and Wright ([18]; see also [56]).

We turn to the computation of $\eta_{\operatorname{disc} L}(\sigma, L)$, in which subrings are filtered by splitting type. Happily the answers are not too hard to deduce from Theorem 12.6. The easiest cases are $\sigma = 111$, 12, and 3, which only occur in maximal orders: thus for these three values of σ,

$$\eta_{\operatorname{disc} L}(\sigma, L) = \begin{cases} 1 & \text{if } \sigma(\mathcal{O}_L) = \sigma \\ 0 & \text{otherwise.} \end{cases}$$

Next we compute $\eta_{\operatorname{disc} L}(1^2 1, L)$.

Lemma 12.8.

$$\eta_{\operatorname{disc} L}(1^2 1, L) = \frac{G}{1-Z}$$

where G is a polynomial depending on the splitting type σ_χ as follows.

σ_χ	G
111	$3Z$
12	Z
3	0
$1^2 1$	1
1^3	0

(110)

Proof. A ring C of splitting type 1^21 has its corresponding cubic form (in suitable coordinates) congruent to a multiple of xy^2 modulo p. Write

$$\Phi_C(x,y) = pax^3 + pbx^2y + cxy^2 + pdy^3$$

where $p \nmid c$. The ring C is non-maximal iff $p|a$, in which it is of index p in a unique overring C' whose cubic form

$$\Phi_{C'}(x,y) = \frac{a}{p}x^3 + bx^2y + pcxy^2 + p^2dy^3$$

has a distinguished *simple* root, here at $[0:1]$. Conversely, a ring with a distinguished simple root has one subring of index p and splitting type 1^21. Now the only non-maximal rings whose cubic forms have a simple root are themselves of splitting type 1^21: thus the number of these is constant at index $p, p^2, \ldots$. The value of the constant is the number of simple roots of the maximal order. Thus we have the desired claim. ■

As for the subrings of splitting type 0, they are $\mathcal{O}_K + \pi C$ for each subring C, and so

$$\eta_D(0,L) = \eta_{D/\pi^2}(L) = Z\eta_D(L)$$

for all D and L. Finally, $\eta_D(1^3, L)$ can be computed by subtracting off all the other splitting types from $\eta_D(L)$. We do not need the explicit value in this case.

Before computing the Fourier transforms of the $\eta_D(\sigma, L)$, it is helpful to compute them for some simpler local weightings.

Lemma 12.9. *Let $p \neq 3$ be a prime. For $\sigma \in \{111, 12, 3, 1^21, 1^3\}$ and $D \in K^\times$, let $t_D(\sigma) : H^1(M_D) \to \mathbb{N}$ be the local weighting given by*

$$t_D(L) := \begin{cases} 1 & \sigma(L) = \sigma \\ 0 & \textit{otherwise.} \end{cases}$$

Let T_D be the $\mathbb{Q}$-linear span of the $t_D(\sigma)$. Then the Fourier transform yields an isomorphism

$$\widehat{\ }: T_{-3D} \to T_D \tag{111}$$

given explicitly by

(a) $(t_{-3D}(111) + t_{-3D}(12) + t_{-3D}(3))\widehat{\ } = (t_{-3D}(111) + t_{-3D}(12) + t_{-3D}(3))$

(b) $t_{-3D}(1^21)\widehat{\ } = t_D(1^21)$

(c) $(2t_{-3D}(111) - t_{-3D}(3))\widehat{\ } = t_D(1^3)$

(d) $t_{-3D}(1^3)\widehat{\ } = 2t_D(111) - t_D(3)$

(e) $(t_{-3D}(12))\widehat{\ } = \begin{cases} t_D(12) & q \equiv 1 \mod 3 \\ t_D(111) + t_D(3) & q \equiv 2 \mod 3 \end{cases}$

where $q = |k_K|$.

Proof. We may assume that $D = D_0 \in \mathcal{O}_K$ is a fundamental discriminant. Parts (a) and (b) reduce to the self-orthogonality of $H^1_{D,\mathrm{ur}}$ for $D \in \mathcal{O}_K^\times$ and $D \in \pi\mathcal{O}_K^\times$, respectively. Parts (c) and (d) were proved after showing that both sides of Lemma 12.1 concern only $D \in \mathcal{O}_K^\times$. Finally, part (e) reduces to part (a), using the fact that $3 \in \mathcal{O}_K^\times$ is a square if and only if $q \equiv 1 \mod 3$. ∎

Theorem 12.10. *The weightings η_D, $\eta_D(111)$, $\eta_D(12)$, $\eta_D(3)$, $\eta_D(1^21)$ span $T_D(\!(Z)\!) := T_D \otimes_{\mathbb{Q}} \mathbb{Q}(\!(Z)\!)$. Their Fourier transforms are given by*

(a) $\hat{\eta}_{-3D} = \eta_D$;

(b) *If $q \equiv 1$ mod 3, then*

$$(\eta_{-3D}(111) + \eta_{-3D}(3))\widehat{\ } = \eta_D(111) + \eta_D(3) \quad \textit{and} \quad \widehat{\eta}_{-3D}(12) = \eta_D(12);$$

(c) *If $q \equiv 2$ mod 3, then*

$$(\eta_{-3D}(111) + \eta_{-3D}(3))\widehat{\ } = \eta_D(12) \quad \textit{and} \quad \widehat{\eta}_{-3D}(12) = \eta_D(111) + \eta_D(3);$$

(*d*) $(2\eta_{-3D}(111) - \eta_{-3D}(3))\widehat{\ } = \frac{1}{Z}\big[(1-Z)(1-qZ^3)\eta_D + (Z-1)(\eta_D(111)+\eta_D(12)+\eta_D(3)) + Z^2(2\eta_D(111)-\eta_D(3)) - (1+Z)^2\eta_D(1^21)\big]$;

(*e*) $\hat{\eta}_{-3D}(1^21) = \frac{1}{1+Z}\big[(1-Z)(1-qZ^3)\eta_D+(Z-1)(\eta_D(111)+\eta_D(12)+\eta_D(3))+Z(Z-1)(2\eta_D(111)-\eta_D(3)) - Z(1+Z)\eta_D(1^21)\big]$.

Proof. We may assume that $D = D_0 \in \mathcal{O}_K$ is a fundamental discriminant. We need the following result, which is useful in its own right:

Lemma 12.11. *Let $D = \operatorname{disc}\mathcal{O}_L$ be the discriminant of a maximal cubic order over a local field K,* $\operatorname{char} k_K \neq 3$. *Write $D = \pi^{2k}D_0$ where D_0 is the associated fundamental discriminant. Then*

$$k = \begin{cases} 1 & \sigma(\mathcal{O}_L) = 1^3 \\ 0 & \textit{otherwise.} \end{cases}$$

Proof. If L is unramified, then $\pi \nmid D$ and $k = 0$. If $\sigma(L) = 1^21$, then

$$D = \operatorname{disc} L = \operatorname{disc}(K \times K(\sqrt{D_0})) = D_0.$$

So we are left with the case that $\sigma(L) = 1^3$. Note that L/K is tamely ramified so $D = \pi^2 D'$, $\pi \nmid D'$. We need to prove that D' is a discriminant, which is only nontrivial when $\operatorname{char} k_K = 2$. Let $f(x) = ax^3 + \pi bx^2 + \pi cx + \pi d$ be an Eisenstein polynomial for L. Then

$$D' = \pi^2b^2c^2 - 4\pi ac^3 - 4\pi^2b^3d - 27a^2d^2 + 18\pi abcd \equiv (ad - \pi bc)^2 \mod 4,$$

so $D' = D_0$. ∎

This allows us to change the scaling in Lemma 12.8 (on $\eta_D(1^21)$) and Theorem 12.6 (on η_D) from $\eta_{\operatorname{disc} L}$ to η_D, multiplying the weighting by Z in the case that $\sigma(\mathcal{O}_L) = 1^3$. Also, trivially

$\eta_D(\sigma) = t_D(\sigma)$ for unramified σ. So we have five equations

$$\begin{aligned}
\eta_D(111) &= t_D(111) \\
\eta_D(12) &= t_D(12) \\
\eta_D(3) &= t_D(3) \\
\eta_D(1^21) &= \frac{3t_D(111) + t_D(12) + t_D(1^21)}{1 - Z} \\
\eta_D &= \frac{(1+Z)^2 t_D(111) + (1+Z^2)t_D(12) + (1 - Z + Z^2)t_D(3) + (1+Z)t_D(1^21) + Zt_D(1^3)}{(1-Z)(1-qZ^3)}.
\end{aligned}$$

We see that there is an invertible transition matrix between the sets

$$\{t_D(111), t_D(12), t_D(3), t_D(1^21), t_D\} \quad \text{and} \quad \{\eta_D(111), \eta_D(12), \eta_D(3), \eta_D(1^21), \eta_D\}$$

is invertible (we cannot call these "bases," because $t_D(\sigma)$ can vanish for certain D). Accordingly, we can rewrite Lemma 12.9 in terms of the η's and get the identities claimed in the theorem. ■

Problem 12.12. *Can the rich structure found in this section be carried out, to some extent, when* $\operatorname{char} k_K = 3$*? For instance,* $\hat{V}(\mathbb{F}_3)$*, the space of integral* 1331*-forms modulo* 3993*-forms, has six* $\mathrm{GL}_2(\mathbb{F}_3)$*-orbits, the analogues of splitting types, and it is natural to wonder whether the Fourier transform relates them to the six splitting types on* $V(\mathbb{F}_3)$*.*

12.4 Invariant lattices at 2

The foregoing investigation also allows us to extend the work of Ohno and Taniguchi [45] on extending O-N to counting binary cubic forms satisfying certain congruence conditions at 2. Assume that $q = 2$.

Recall from Section 11 the five primitive invariant lattices $\Lambda_i \subseteq V(\mathcal{O}_K)$ of binary cubic forms:

$$\Lambda_1 = \{f(x,y) = ax^3 + bx^2y + cxy^2 + dy^3 : a,b,c,d \in \mathcal{O}_K\}$$

$$\Lambda_2 = \{f \in \Lambda_1 : \sigma(f) \in \{0, 12\}\}$$

$$\Lambda_3 = \{f \in \Lambda_1 : \sigma(f) \in \{0, 111, 3\}\}$$

$$\Lambda_4 = \{f \in \Lambda_1 : \sigma(f) \in \{0, 111, 12, 1^3\}\}$$

$$\Lambda_5 = \{f \in \Lambda_1 : \sigma(f) \in \{0, 111\}\}$$

Let

$$\lambda_i(D) : H^1(K, M_D) \to \mathbb{Z}((Z))$$

$$L \mapsto \sum_{k \in \mathbb{Z}} g_{\pi^{2k}D}(\Lambda_i, L) \cdot Z^k$$

be the analogue of the subring zeta function counting only those rings whose corresponding form is in Λ_i. Each $\lambda_i(D)$ is a linear combination of the appropriate $\eta_{\sigma,D}$, and the transition matrix is again invertible. (No reason is known, beyond pure coincidence, why the number of invariant lattices over $\mathbb{Z}_2$ should equal 5, the number of independent $\eta_{\sigma,D}$.) So we get:

Corollary 12.13 (**Local O-N for general invariant lattices;** cf. [45], Theorems 1.2, 1.3 and 1.4)**.** *Let K be an unramified extension of $\mathbb{Q}_2$. The Fourier dual of each $\lambda_i(-27D)$ lies again in the*

span of the $\lambda_i(D)$, explicitly:

$$\hat{\lambda}_1(-27D) = \lambda_1(D)$$

$$\hat{\lambda}_2(-27D) = \lambda_3(D)$$

$$\hat{\lambda}_3(-27D) = \lambda_2(D)$$

$$\hat{\lambda}_4(-27D) = \frac{1}{3Z}\big[(-8Z^3+6Z^2-Z)\lambda_1(D) + (2Z-1)\lambda_2(D) + (-8Z^2+4Z)\lambda_3(D) + (-4Z^2+1)\lambda_4(D) + (16Z^2-1)\lambda_5(D)\big]$$

$$\hat{\lambda}_5(-27D) = \frac{1}{3Z}\big[(-2Z^3+3Z^2-Z)\lambda_1(D) + (2Z-1)\lambda_2(D) + (-2Z^2+Z)\lambda_3(D) + (-Z^2+1)\lambda_4(D) + (4Z^2-1)\lambda_5(D)\big]$$

Proof. The $\lambda_i(D)$ are simply the $\eta_D(\sigma)$ in disguise: for instance,

$$\lambda_2(D) = \eta_D(0) + \eta_D(12),$$

and so on. Rewriting the results of Theorem 12.10 in terms of the λ_i and plugging in $q = 2$ proves the theorem. ■

The five equalities in this corollary can be viewed as local reflection theorems in the sense of Theorem 8.13, relating different integral models of the same composed variety on each side.

We can now get global results in great generality.

Theorem 12.14 (O-N for general invariant lattices). *Let K be a number field. Let $\mathfrak{a}$ be an ideal of K, and let Λ be a $\mathcal{G}_a = \mathrm{SL}(\mathcal{O}_K \oplus \mathfrak{a})$-invariant lattice of full rank in the space $V(K)$ of binary cubic forms. Let $\mathfrak{t}$ be the trace ideal of Λ, that is, the unique $\mathfrak{t} \mid 3$ such that $\Lambda_\mathfrak{p} \cong \mathcal{V}_{(1,\mathfrak{t})}(\mathfrak{p})$ at every prime $\mathfrak{p} \mid 3$ (after identifying $\mathcal{G}_\mathfrak{a}$ with SL_2, which we can do after localization). For $D \in K^\times$, denote by $h_\Lambda(D)$ the number of $\mathcal{G}_a$-orbits of binary cubic forms of discriminant D, each orbit weighted by the reciprocal of its stabilizer.*

Then:

1. *If Λ is of type Λ_1, Λ_2, or Λ_3 at every prime whose residue field is $\mathbb{F}_2$, then there is a lattice Λ^* invariant under $\mathcal{G}_{\mathfrak{at}^{-3}}$ such that we have the global reflection theorem: for each $D \in K^\times$,*

$$h_\Lambda(D) = \frac{3^{\#\{v|\infty : D \in (K_v^\times)^2\}}}{N_{\mathcal{O}_K/\mathbb{Z}}(\mathfrak{t})} h_{\Lambda^*}(-27D). \tag{112}$$

2. *In general, there is a family $\Lambda_1^*, \ldots, \Lambda_m^*$ of lattices, all equal away from 2, each Λ_j^* invariant under a group $\mathcal{G}_{\mathfrak{as}_j\mathfrak{t}^{-3}}, \ldots$ where $\mathfrak{s}_j$ is an ideal having nonzero valuation only at primes dividing 2, and a global reflection theorem of the shape*

$$h_\Lambda(D) = \frac{3^{\#\{v|\infty : D \in (K_v^\times)^2\}}}{N_{\mathcal{O}_K/\mathbb{Z}}(\mathfrak{t})} \sum_{j=1}^{m} c_j h_{\Lambda_j^*}(-27D),$$

where the $c_i \in \mathbb{Q}$ depend only on Λ.

Proof. Theorem 11.1 limits the lattices we must consider. If Λ is of type Λ_1 at each prime dividing 2, we have $\Lambda = \mathfrak{c}\mathcal{V}_{\mathfrak{a},\mathfrak{t}}(\mathcal{O}_K)$. But since

$$\mathfrak{c} \oplus \mathfrak{c} \cong 1 \oplus \mathfrak{c}^2,$$

there is an isomorphism of integral models

$$(\mathfrak{c}\mathcal{V}_{\mathfrak{a},\mathfrak{t}}, \mathcal{G}_\mathfrak{a}) \cong \left(\mathcal{V}_{\mathfrak{ac}^{-2},\mathfrak{t}}, \mathcal{G}_{\mathfrak{ac}^{-2}}\right).$$

So we can take

$$\Lambda^* = \mathfrak{c}\mathcal{V}_{\mathfrak{at}^{-3},3\mathfrak{t}^{-1}},$$

and the desired reflection theorem follows from Theorem 11.3.

The remaining cases can be solved with a bit of fiddling at 2. Let $\bar{\Lambda} \supseteq \Lambda$ be the lattice that sits over Λ at each $\mathfrak{p} \mid 2$ as Λ_1 sits over the relevant Λ_i, $1 \le i \le 5$, and let $\bar{\Lambda}^*$ be the corresponding reflection lattice. All Λ_i^* will look like Λ^* away from 2.

Locally at each $\mathfrak{p} \mid 2$, we construct a collection of $\Lambda_{j,\mathfrak{p}}^*$, $1 \le j \le m_\mathfrak{p}$ as follows: for each term

$Z^k\lambda_i(D)$ in Corollary 12.13, take the lattice

$$\Lambda^*_{j,\mathfrak{p}} = \begin{bmatrix} \pi^k & & \\ & & \\ & & 1 \end{bmatrix} \Lambda_i,$$

for which $\mathcal{G}_{\pi^{-1}}$-orbits of discriminant D correspond to SL_2-orbits of discriminant D/π^{2k} in Λ_i. Then Corollary 12.13 appears as a local reflection theorem

$$\hat{g}_{\Lambda_\mathfrak{p}}(D) = \sum_{j=1}^{m_\mathfrak{p}} c_{j,\mathfrak{p}} \cdot g_{\Lambda^*_{j,\mathfrak{p}}}(D).$$

for the integral models $\Lambda_\mathfrak{p}$ and $\Lambda^*_{j,\mathfrak{p}}$. (Strictly speaking, these are not truly integral models, inasmuch as the SL_2-invariance of $\Lambda_2, \ldots, \Lambda_5$ is not given by an algebraic integrality; but we get the same local and global class numbers by going up to a lattice of type Λ_1 and imposing non-natural weights to pick out the appropriate splitting types.)

We then apply Theorem 8.13 to these local reflection theorems and, as usual, the ones relating $\bar{\Lambda}$ and $\bar{\Lambda}^*$ away from 2. The resulting reflection theorem involves the global integral models given by gluing the $\Lambda^*_{j,\mathfrak{p}}$ at each $\mathfrak{p} \mid 2$ in all possible ways. When Λ is of type $\Lambda_1, \Lambda_2, \Lambda_3$ at each $\mathfrak{p} \mid 2$, there is only one Λ^*, and $\mathfrak{s}$, which arises from the Z-operators in Corollary 12.13, disappears. ■

12.5 Binary cubic forms over $\mathbb{Z}[1/N]$

For N a squarefree integer, it is natural to ask what happens if we invert finitely many primes and count binary cubic forms of discriminant $D \neq 0$ over $\mathbb{Z}[1/N]$, up to the action of the relevant group $\mathrm{SL}_2(\mathbb{Z}[1/N])$. There are still only finitely many for each degree, owing to Hermite's theorem on the finiteness of the number of number fields with prescribed degree and set of ramified primes.

Note that D matters only up to multiplication by the squares in $\mathbb{Z}[1/N]^\times$; hence we can restrict our attention to $D \in \mathbb{Z}$ that are *fundamental* at each prime $p \mid N$. (If $p \neq 2$, this means that $p^2 \nmid D$. If $p = 2$, this means that $D \equiv 1 \mod 4$ or $D \equiv 8, 12 \mod 16$. However, we allow D to be non-fundamental at primes not dividing N.)

We do not have O-N for forms over $\mathbb{Z}[1/N]$ in the same formulation as over $\mathbb{Z}$. Nevertheless, the other side of the reflection theorem is noticeably not too complicated.

Theorem 12.15. *Let N be a squarefree integer.*

For $0 \neq D \in \mathbb{Z}[1/N]$, let $h_{\mathbb{Z}[1/N]}(D)$ be the number of $\mathrm{SL}_2(\mathbb{Z}[1/N])$-orbits of integral binary cubic forms over $\mathbb{Z}[1/N]$, each weighted by the reciprocal of its stabilizer in $\mathrm{SL}_2(\mathbb{Z}[1/N])$. If $3 \nmid N$, define $h_{3,\mathbb{Z}[1/N]}(D)$ to be the same count, counting only 1331-forms (that is, forms whose middle two coefficients belong to the ideal $3\mathbb{Z}[1/N] \subsetneq \mathbb{Z}[1/N]$).

Now let D be a discriminant that is fundamental at all primes dividing N. For each $p \mid N\infty$, let

$$c_{D,p} = \begin{cases} 3 & \text{if } D \in \left(\mathbb{Z}_p^\times\right)^2 \\ 1 & \text{if } D \text{ is a non-square unit modulo } p, \\ 1/2 & \text{if } p \mid D. \end{cases}$$

and let

$$c_{D,N\infty} = \prod_{p \mid N\infty} c_{D,p}.$$

Then:

(a) If $3 \nmid N$, then

$$h_{\mathbb{Z}[1/N]}(D) = \frac{c_{-27D,N\infty}}{3} \cdot h_3(-27D, R_N)$$
$$h_{3,\mathbb{Z}[1/N]}(-27D) = c_{D,N\infty} \cdot h(D, R_N).$$

(b) If $3 \mid N$, then

$$h_{\mathbb{Z}[1/N]}(-27D) = 3c_{D,N\infty} \cdot h_3(D, R_N).$$

Proof. We take the same composed variety (V, Γ) of binary cubic forms as before. However, we take integral models $(\mathcal{V}^{(i)}, G^{(i)})$ that are not even over the same ring of integers $\mathcal{O}_{\mathbb{Q}}^{(i)}$!

On the left-hand side, we take the scheme $\mathcal{V}^{(1)}$ of binary cubic $111N$- or $133N$-forms of discrim-

inant D or $-27D$. This does not admit an algebraic action of $\mathrm{SL}_2\mathbb{Z}$, but it *does* admit an algebraic action of $G^{(1)} = \mathrm{G}\Gamma^0(N)$.

On the right-hand side, we take the scheme $\mathcal{V}^{(2)}$ of binary cubic forms over $\mathbb{Z}[1/N]$ of discriminant D, or 1331-forms as appropriate, with the natural action of $G^{(2)} = \mathrm{SL}_2$ over $\mathbb{Z}[1/N]$.

It is evident that the global class numbers of these integral models match the quantities studied in the theorem. The checking of most of the conditions of Theorem 8.12 is routine, so we content ourselves with checking the local duality.

When $p \nmid N$, the integral model is identical to that used for O-N, so we already have the needed duality with an appropriate duality constant $c_{D,p}$ or $c_{-27D,p}$. This includes the infinite prime, at which the duality constant $c_{D,\infty}$ tracks the sign of D as in O-N.

When $p \mid N$, the computation of the local class numbers is not difficult:

- As to $\mathcal{V}^{(1)}$, we look for forms of discriminant D with a marked root modulo p. We first observe that forms corresponding to nonzero cohomology classes are not counted, because they either have splitting type
  - (3), and have no roots modulo p, or
  - (1^3), and have discriminant non-fundamental at p, by Lemma 12.11.

  So $g^{(1)} : H^1(\mathbb{Z}_p, M') \to \mathbb{N}$ is a scalar multiple of $\mathbf{1}_0$, nonzero because the split ring $\mathbb{Z}_p \times \mathbb{Z}_p[(D + \sqrt{D})/2]$ has an index form with a root.

- As to $\mathcal{V}^{(2)}$, since the completion of $\mathbb{Z}[1/N]$ at p is $\mathbb{Q}_p$, the local orbit counter counts cosets in $\mathrm{SL}_2(\mathbb{Q}_p)\backslash\mathrm{SL}_2(\mathbb{Q}_p)$ that keep a certain form f "integral" over $\mathbb{Q}_p$. There is obviously only one such coset, regardless of the cohomology class of f, so $g^{(2)} : H^1(\mathbb{Z}_p, M) \to \mathbb{N}$ is identically 1.

It remains only to compute the duality constant.

- If $\mathbb{Q}_p[\sqrt{D}]$ is split, then there are three roots of $f(x, y) = xy(x + y)$ to mark, but they all wind up equivalent. So $g^{(1)} = \mathbf{1}_0$, but because of the $|H^0| = 3$ in the scaling of the Fourier transform, we need to insert a factor of $c_{D,p} = 3$.

- If $\mathbb{Q}_p[\sqrt{D}]$ is inert, there is only one root to mark, and $|H^0| = 1$, so $c_{D,p} = 1$.
- If $\mathbb{Q}_p[\sqrt{D}]$ is ramified, then we can mark either the single or the double root modulo p. These are non-equivalent $\mathrm{G}\Gamma^0(p)(\mathbb{Z}_p)$-orbits inside the same $\mathrm{SL}_2(\mathbb{Q}_p)$-orbit, so $g^{(1)} = 2 \cdot \mathbf{1}_0$ and $|H^0| = 1$, so $c_{D,p} = 1/2$. (If we modified the theorem by counting $111N$-forms whose third coefficient c is coprime to N, another family stable under $\mathrm{G}\Gamma^0(N)$, then we would be forced to mark the simple root, and this factor of $1/2$ would disappear.)

Multiplying the duality constants obtained completes the proof. ■

Problem 12.16. *Does the integral model of $111N$-forms of non-fundamental discriminant D have a natural dual? The first step in answering this is to check whether the Fourier transform of its local orbit counter takes nonnegative values.*

Part VI

Reflection theorems: quartic rings and related objects

13 Reflection for 2-adic quartic orders, and applications

Analogously to the cubic case, the reflection theorem that we state and prove is going to swap $\mathfrak{t}$-traced and $2\mathfrak{t}^{-1}$-traced orders. It is not the most general reflection theorem that one can try to state: see Section 24 below.

Fix a nondegenerate cubic ring C over a Dedekind domain $\mathcal{O}_K$. We can also fix a basis

$$C = \mathcal{O}_K \oplus \mathcal{O}_K\xi \oplus \mathfrak{a}\eta,$$

making the index form $\Phi_C(x\xi + y\eta)$ a cubic in the $\mathcal{V}_{\mathfrak{a},1}$ of Theorem 11.3. However, none of our work

will depend on this basis.

We can then look at the scheme $\mathcal{V}_{\mathfrak{t},C}$ of pairs of ternary quadratic forms

$$(\mathcal{A},\mathcal{B}) : \mathcal{O}_K \times \mathcal{O}_K \times \mathfrak{a} \rightrightarrows \mathcal{O}_K \times \mathfrak{a},$$

that is, pairs of 3×3 symmetric matrices with entries in the ideals

$$\left(\begin{bmatrix} (1) & 2^{-1}\mathfrak{t} & 2^{-1}\mathfrak{t}\mathfrak{a}^{-1} \\ & (1) & 2^{-1}\mathfrak{t}\mathfrak{a}^{-1} \\ & & \mathfrak{a}^{-2} \end{bmatrix}, \begin{bmatrix} \mathfrak{a} & 2^{-1}\mathfrak{t}\mathfrak{a} & 2^{-1}\mathfrak{t} \\ & \mathfrak{a} & 2^{-1}\mathfrak{t} \\ & & \mathfrak{a}^{-1} \end{bmatrix} \right)$$

satisfying the four equations

$$\det(\mathcal{A}x + \mathcal{B}y) = \Phi_C(x,y)$$

asserting that $(\mathcal{A},\mathcal{B})$ parametrizes a quartic ring L that is $\mathfrak{t}$-traced with reduced resolvent C. This $\mathcal{V}_{\mathfrak{t},C}$, together with the natural action of the group $\mathcal{G} = \mathrm{GL}(\mathcal{O}_K \times \mathcal{O}_K \times \mathfrak{a})$, is an integral form of the composed variety (V, GL_3) of pairs of ternary quadratic forms over K. We assert that the integral models

$$\mathcal{V}_{\mathfrak{t},C} \quad \text{and} \quad \mathcal{V}_{2\mathfrak{t}^{-1},C}$$

are naturally dual at all finite places.

Notation 13.1. Here and in the sequel, we use the label "Theorem*" to denote a theorem proved with the following caveats:

(1) Resolvents that are wildly ramified at a 2-adic place are excluded.

(2) In general, the theorem depends on a Monte Carlo verification of a rational algebraic identity (as we will explain). However:

(3) The results for $K/\mathbb{Q}_2$ unramified (e.g. the cases over $\mathbb{Z}$) are known unconditionally.

(4) The results for the reduced resolvent being maximal ($C_{\mathfrak{t}} = \mathcal{O}_R$) are also known unconditionally.

Theorem* 13.2 ("Local Quartic O-N"). *Let K be a nonarchimedean local field and C an order in an étale algebra R that is not wildly ramified over K. For τ a divisor of 2, let $\mathcal{V}_{\tau,C}$ be the integral model parametrizing (τ)-traced orders with reduced resolvent C. Then $\mathcal{V}_{\tau,C}$ and $\mathcal{V}_{2\tau^{-1},C}$ are naturally dual with duality constant $q^{2v_K(\tau)}$; in order words, the associated local orbit counters*

$$g_{\mathfrak{t},C} : H^1(K, M_R) \to \mathbb{N}$$

satisfy the local reflection theorem

$$\hat{g}_{\mathfrak{t},C} = |\mathcal{O}_K/\tau\mathcal{O}_K|^2 \cdot g_{2\mathfrak{t}^{-1},C}.$$

At the infinite places, we no longer have natural duality. (We did not have this problem in the cubic case because $H^1(\mathbb{R}, M)$ is trivial for $|M|$ odd.)

Therefore, call a quartic algebra L/K over a number field *nowhere totally complexified (ntc)* if there is no real place $\mathfrak{p}$ of K such that $L_\mathfrak{p} \cong \mathbb{C} \times \mathbb{C}$. This is equivalent to the cohomology element $\sigma_L \in H^1(K, (\mathbb{Z}/2\mathbb{Z})^2)$ being trivial at all infinite places. Then the local specifications $\mathbf{1}_{\{0\}}$ for ntc quartic algebras and 1 for all quartic algebras are mutually dual, provided that one inserts the correct scale factor.

Theorem* 13.3 ("Quartic O-N"). *Let K be a number field. Let C be an order in a cubic K-algebra R, and let $\mathfrak{t} \subseteq \mathcal{O}_K$ be an ideal such that $\mathfrak{t} \mid (2)$. Let $h(C, \mathfrak{t})$ count the number of $\mathfrak{t}$-traced quartic rings with reduced resolvent C, respectively, each weighted by the reciprocal of its number of resolvent-preserving automorphisms. Let $h^{\mathrm{ntc}}(C, \mathfrak{t})$ count the subset of the foregoing that are ntc, weighted in the same way. Then*

$$h(C, \mathfrak{t}) = \frac{N(\mathfrak{t})^2}{2^{r_\infty}} \cdot h^{\mathrm{ntc}}(C, 2\mathfrak{t}^{-1}),$$

where r_∞ is the number of real places of K over which R is not totally real plus twice the number of complex places of K.

Proof. We apply Theorem 8.12 to the composed varieties $\mathcal{V}^{(1)} = \mathcal{V}_{\mathfrak{t},C}$ and $\mathcal{V}^{(2)} = \mathcal{V}_{2\mathfrak{t}^{-1},C}$ just defined, with the following local weightings $w_v^{(i)}$:

- At finite $v \nmid 2$, we take $w_v^{(i)} = 1$, which are mutually dual with duality constant 1 by Theorem 14.6.
- At $v = \mathfrak{p}|2$, we take $w_v^{(i)} = 1$, which are mutually dual with duality constant

$$N(\mathfrak{p})^{2v_{\mathfrak{p}}(\mathfrak{t})}$$

by Theorem* 13.2.

- At complex v, we take $w_v^{(i)} = 1$, which are mutually dual with duality constant

$$\hat{f}_v = \frac{1}{|H^0(K_v, M_R)|} = \frac{1}{4}.$$

- At real v for which $R_v \cong \mathbb{R} \times \mathbb{C}$, we take $w_v^{(i)} = 1$, which are mutually dual with duality constant

$$\hat{f}_v = \frac{1}{|H^0(K_v, M_R)|} = \frac{1}{2}.$$

- At real v for which $R_v \cong \mathbb{R} \times \mathbb{R} \times \mathbb{R}$, we take $w_v^{(1)} = 1$ and $w_v^{(2)} = \mathbf{1}_0$, the selector for rings that are not totally complex at v. The corresponding duality constant is

$$\frac{\left|H^1(K_v, M_R)\right|}{|H^0(K_v, M_R)|} = \frac{4}{4} = 1.$$

The product of all duality constants is thus

$$\prod_{\mathfrak{p}|2} N(\mathfrak{p})^{2v_{\mathfrak{p}}(\mathfrak{t})} \cdot \prod_{K_v \cong \mathbb{C}} \frac{1}{4} \cdot \prod_{R_v \cong \mathbb{R}\times\mathbb{C}} \frac{1}{2} = \frac{N(\mathfrak{t})^2}{2^{r_\infty}},$$

as desired. ∎

Although we have been counting quartic rings by resolvent, the corresponding result where we

count by discriminant follows quickly. We present the reflection theorem in two forms, one dealing with $2 \times 3 \times 3$ symmetric boxes, the other with quartic rings (which are in bijection only in the case of rings of content 1):

Theorem 13.4. *Let K be a number field. Denote by $\mathcal{V}_{\mathfrak{t},\mathfrak{a}}(\mathcal{O}_K)$ the space of pairs of ternary quadratic forms*

$$(\mathcal{A}, \mathcal{B}) : \mathcal{O}_K \times \mathcal{O}_K \times \mathfrak{a} \rightrightarrows \mathcal{O}_K \times \mathfrak{a},$$

that are $\mathfrak{t}$-traced in the sense that the entries belong to the ideals

$$\left(\begin{bmatrix} (1) & 2^{-1}\mathfrak{t} & 2^{-1}\mathfrak{t}\mathfrak{a}^{-1} \\ & (1) & 2^{-1}\mathfrak{t}\mathfrak{a}^{-1} \\ & & \mathfrak{a}^{-1} \end{bmatrix}, \begin{bmatrix} \mathfrak{a} & 2^{-1}\mathfrak{t}\mathfrak{a} & 2^{-1}\mathfrak{t} \\ & \mathfrak{a} & 2^{-1}\mathfrak{t} \\ & & (1) \end{bmatrix} \right).$$

It has a natural action of the group

$$\mathcal{G}_{\mathfrak{a}} = \mathrm{SL}(\mathcal{O}_K \oplus \mathcal{O}_K \oplus \mathfrak{a}) \times \mathrm{SL}(\mathcal{O}_K \oplus \mathfrak{a})$$

that preserves discriminant. Denote by $h_{\mathfrak{t}}(\mathcal{D})$ the number of $\mathcal{G}_{\mathfrak{t},\mathfrak{a}}$ orbits of pairs of ternary quadratic forms having discriminant $\mathcal{D} = (\mathfrak{a}, D)$, each orbit weighted by the reciprocal of the order of its stabilizer in $\mathcal{G}_{\mathfrak{a}}$. Denote by $h_{\mathfrak{t}}^{\mathrm{ntc}}(\mathcal{D})$ the number of such orbits (weighted in the same way) which are ntc, in the sense that at each real place of K, the conics $\mathcal{A}$ and $\mathcal{B}$ have a common point in $\mathbb{RP}^2$. Then for all discriminants $\mathcal{D}$ prime to 2,

$$h_{\mathfrak{t}}(\mathfrak{t}^8\mathcal{D}) = \frac{N(\mathfrak{t})^2}{2^{r_\infty}} \cdot h_{2\mathfrak{t}^{-1}}^{\mathrm{ntc}}(256\mathfrak{t}^{-8}\mathcal{D}),$$

where r_∞ is the number of real places of K at which $D < 0$ plus twice the number of complex places of K.

Proof. We sum the preceding theorem over all cubic rings C of discriminant $\mathcal{D}$, weighting each C by the reciprocal of the number of *orientation-preserving* automorphisms of C, which is the stabilizer of

the corresponding form in $\mathrm{SL}(\mathcal{O}_K \oplus \mathfrak{a})$. It is easy to see that each orbit is counted the number of times it appears in the theorem. Because the reduced discriminant is prime to 2 (a needed condition to avoid involving wildly ramified resolvents in the sum), we can state the theorem unconditionally. ■

Theorem 13.5. *Let K be a number field, and let $\mathcal{D} = (\mathfrak{a}, D)$ be a discriminant. Denote by $h_{\mathfrak{t}}^{\circ}(\mathcal{D})$ the number of $\mathfrak{t}$-traced quartic rings $\mathcal{O}$ over $\mathcal{O}_K$ having discriminant $\mathcal{D}$, each $\mathcal{O}$ weighted by $1/|\mathrm{Aut}_K(\mathcal{O})|$. Denote by $h_{\mathfrak{t}}^{\circ,\mathrm{ntc}}(\mathcal{D})$ the number of such that are ntc, weighted in the same way. Then for all discriminants $\mathcal{D}$ prime to 2,*

$$h_{\mathfrak{t}}^{\circ}(\mathfrak{t}^8\mathcal{D}) = \frac{N(\mathfrak{t})^2}{2^{r_\infty}} \cdot h_{2\mathfrak{t}^{-1}}^{\circ,\mathrm{ntc}}(256\mathfrak{t}^{-8}\mathcal{D}), \tag{113}$$

where r_∞ is the number of real places of K at which $D < 0$ plus twice the number of complex places of K.

Proof. In the previous theorem, we studied $h_{\mathfrak{t}}(\mathfrak{t}^8\mathcal{D})$, which can be interpreted as the number of quartic rings $\mathcal{O}$ equipped with a resolvent C and an *orientation,* that is, an identification $\Lambda^4\mathcal{O} \cong \mathfrak{a}$ for which the discriminant is $\mathfrak{t}^8\mathcal{D}$. Every quartic ring admits two orientations (there are $|\mathcal{O}_K^\times|$-many identifications $\Lambda^4\mathcal{O} \cong \mathfrak{a}$, but all but one and its negative yield a D scaled by a different square of a unit). So $\frac{1}{2}h_{\mathfrak{t}}(\mathfrak{t}^8\mathcal{D}\mathcal{D})$ is the number of resolvents $(\mathcal{O}, C, \Theta, \Phi)$ of discriminant $\mathfrak{t}^8\mathcal{D}$, up to isomorphism, each weighted by the reciprocal of its number of automorphisms.

Let $h_{\mathfrak{t}}^1(\mathfrak{t}^8\mathcal{D})$ be the number of quartic rings $\mathcal{O}$ of discriminant $(\mathfrak{a}, D)$ with $\mathfrak{t}$-traced content 1, weighted by $1/|\mathrm{Aut}\,\mathcal{O}|$. This is related to If $\mathcal{O}$ is an ntc quartic ring of discriminant $\mathfrak{t}^8\mathcal{D}$ having some $\mathfrak{t}$-traced content $\mathfrak{c}$, then $\mathcal{O} = \mathcal{O}_K + \mathfrak{c}\mathcal{O}'$, where $\mathcal{O}'$ has $\mathfrak{t}$-traced content 1, discriminant $(\mathfrak{a}\mathfrak{c}^{-3}\mathfrak{t}^8, D) = \mathfrak{c}^{-6}\mathfrak{t}^8\mathcal{D}$, and the same automorphism group as $\mathcal{O}$. Thus

$$\frac{1}{2}h_{\mathfrak{t}}(\mathfrak{t}^8\mathcal{D}) = \sum_{\mathfrak{c}^3 | D\mathfrak{a}^2} h_{\mathfrak{t}}^1(\mathfrak{t}^8\mathcal{D}\mathfrak{c}^{-6}).$$

On the other hand, the number of resolvents of $\mathcal{O}$ depends on the $\mathfrak{t}$-traced content $\mathfrak{c}$ (Proposition

6.17(b)): it is

$$\sigma_1(\mathfrak{c}) = \sum_{\mathfrak{d}|\mathfrak{c}} N_{K/\mathbb{Q}}(\mathfrak{d}).$$

These are resolvents *as maps out of* $\mathcal{O}$ (as pointed out in [42], end of Section 8), which is the correct manner of counting to make

$$h_{\mathfrak{t}}^{\circ}(\mathfrak{t}^8\mathcal{D}) = \sum_{\mathfrak{c}^3|D\mathfrak{a}^2} \sigma_1(\mathfrak{c}) h_{\mathfrak{t}}^1(\mathfrak{c}^{-6}\mathfrak{t}^8\mathcal{D}).$$

We can now write $h_{\mathfrak{t}}^{\circ}$ in terms of $h_{\mathfrak{t}}$:

$$\begin{aligned} h_{\mathfrak{t}}^{\circ}(\mathfrak{t}^8\mathcal{D}) &= \sum_{\mathfrak{c}^3|D\mathfrak{a}^2} \sigma_1(\mathfrak{c}) h_{\mathfrak{t}}^1(\mathfrak{c}^{-6}\mathfrak{t}^8\mathcal{D}) \\ &= \sum_{\mathfrak{c}^3|D\mathfrak{a}^2} \sum_{\mathfrak{b}|\mathfrak{c}} N(\mathfrak{b}) h_{\mathfrak{t}}^1(\mathfrak{c}^{-6}\mathfrak{t}^8\mathcal{D}) \\ &= \sum_{\mathfrak{b}^3|D\mathfrak{a}^2} \sum_{\mathfrak{c}'^3|D\mathfrak{a}^2\mathfrak{b}^{-3}} N(\mathfrak{b}) h_{\mathfrak{t}}^1(\mathfrak{b}^{-3}\mathfrak{c}'^{-6}\mathfrak{t}^8\mathcal{D}) \\ &= \frac{1}{2} \sum_{\mathfrak{b}^3|D\mathfrak{a}^2} N(\mathfrak{b}) h_{\mathfrak{t}}(\mathfrak{b}^{-3}\mathfrak{t}^8\mathcal{D}). \end{aligned}$$

Transforming both sides of (113) in this manner reduces it to Theorem 13.4. ■

13.1 Results on binary quartic forms

We can also derive a reflection theorem about binary quartic forms, which correspond (via a completely general construction for binary n-ic forms) to a certain subclass of quartic rings. This subclass was identified explicitly by Wood:

Theorem 13.6 ([59], Theorem 1.1)**.** *There is a natural, discriminant preserving bijection between the set of* $\mathrm{GL}_2(\mathbb{Z})$*-equivalence classes of binary quartic forms and the set of isomorphism classes of pairs* (Q, C) *where* Q *is a quartic ring and* C *is a monogenized cubic resolvent of* Q *(where isomorphisms are required to preserve the generator of* C *modulo* $\mathbb{Z}$*).*

Proof. Regarding pairs (Q, C) of quartic rings as pairs (A, B) of 3×3 symmetric matrices via

Bhargava's parametrization, we send a form $\Phi(x,y) = ax^4 + bx^3y + cx^2y^2 + dxy^3 + ey^4$ to

$$(A_0, B) = \left(\begin{bmatrix} & & 1/2 \\ & -1 & \\ 1/2 & & \end{bmatrix}, \begin{bmatrix} a & b/2 & \\ b/2 & c & d/2 \\ & d/2 & e \end{bmatrix} \right).$$

The distinguished generator arises because the resolvent form $g(x,y) = 4\det(A_0 x - By)$ is monic, since $\det A_0 = 1/4$. Further details will be found in [59]. ■

To apply this theorem, we need to know the number of automorphisms of the quartic ring corresponding to a given form:

Lemma 13.7. *In this bijection, the group of resolvent-preserving automorphisms of a quartic ring is in natural isomorphism with the stabilizer (in* $\mathrm{PGL}_2(\mathbb{Z})$*) of the corresponding form.*

Proof. The conclusion follows easily from the method of proof of the preceding theorem. By [59], Theorem 2.5, we can choose bases for Q and C so that the corresponding pair of ternary quadratic forms, has the form (A_0, B) above. A resolvent-preserving automorphism is a change of variables $h \in \mathrm{SL}_3(\mathbb{Z})$ that preserves both A_0 and B. By [59], Lemma 3.2, $h = \varepsilon_{A_0}(\tilde{h})$ lies in the image of the map

$$\varepsilon_{A_0} : \mathrm{GL}_2(\mathbb{Z}) \to \mathrm{SL}_3(\mathbb{Z})$$
$$\begin{bmatrix} a & b \\ c & d \end{bmatrix} \mapsto \frac{1}{ad-bc} \begin{bmatrix} a^2 & ab & b^2 \\ 2ac & ad+bc & 2bd \\ c^2 & cd & d^2 \end{bmatrix}$$

By [59], Theorem 3.1, h preserves B if and only if $\tilde{h}$ preserves the binary quartic form f. Moreover, it is easy to see that $\ker \varepsilon_{A_0} = \pm 1$. This constructs the desired isomorphism. ■

We fix a monic binary cubic form $g(x,y)$ and let $C = \mathbb{Z}[\xi]$ be the corresponding monogenized

cubic ring, with generator ξ. Then in the notation of Theorem* 13.3,

$$h\big(C,(1)\big) = \sum_{\substack{\text{quartic rings } Q \\ \text{with resolvent } C, \\ \text{up to } C\text{-isom}}} \frac{1}{|\mathrm{Aut}_C\, Q|} = \sum_{\substack{\text{binary quartics } f(x,y) \\ \text{with resolvent } g, \\ \text{up to } \mathrm{PGL}_2\mathbb{Z}}} \frac{1}{|\mathrm{Stab}_{\mathrm{PGL}_2\mathbb{Z}}|\, f}.$$

The quantity $h^{\mathrm{ntc}}\big(C,(2)\big)$ appearing on the opposite side of Theorem* 13.3 is not so straightforward to interpret. Here we are counting pairs (A,B) of integer symmetric matrices with $\det(Ax - By) = g$ (with a certain condition at ∞), so we need to classify integer symmetric matrices A with $\det A = 1$. There are, up to similarity, two:

Lemma 13.8. *Every integer symmetric matrix A with $\det A = 1$ is similar to*

$$A_1 = \begin{bmatrix} & & 1 \\ & -1 & \\ 1 & & \end{bmatrix} \quad \textit{or} \quad I = \begin{bmatrix} 1 & & \\ & 1 & \\ & & 1 \end{bmatrix}.$$

Proof. Let A be an integral symmetric matrix of determinant 1. Look at the corresponding conic $\mathcal{C}$ defined by $x^\top Ax = 0$. Note that for each rational prime $p \notin \{2,\infty\}$, we have $p \nmid 4 = \det \mathcal{C}$, so $\mathcal{C}$ has good reduction to $\mathbb{F}_p$: by the Chevalley-Warning theorem, $\mathcal{C}$ has an $\mathbb{F}_p$-point and hence a $\mathbb{Q}_p$-point. Then, by Hilbert reciprocity, there are only two possibilities for the isomorphism type of $\mathcal{C}$ over $\mathbb{Q}$:

- If $\mathcal{C}$ has an $\mathbb{R}$-point, then $\mathcal{C}$ also has a $\mathbb{Q}_2$-point and hence (by the Hasse principle) a $\mathbb{Q}$-point. By a $\mathrm{GL}_3\mathbb{Z}$-transformation, we set this point to $[1:0:0]$, the tangent line there to go through $[0:1:0]$, and then A must take the form

$$\begin{bmatrix} & & \pm 1 \\ & -1 & a \\ \pm 1 & a & b \end{bmatrix},$$

  which one easily sees is similar to A_1.

- If $\mathcal{C}$ has no $\mathbb{R}$-points, then A is positive (or negative) definite. It is well known that the only

positive definite integral unimodular matrix of any rank is the identity. ■

Hence $h^{\mathrm{ntc}}\big(C,(2)\big)$ decomposes into the pairs (A,B) of "type A_1" and of "type I" according to the value of A after an appropriate $\mathrm{SL}_3\mathbb{Z}$-transformation.

13.1.1 Type A_1

To understand pairs (A_1,B), we capitalize on the fact that $A_1 \sim A_0$ over $\mathbb{Q}$. Namely, the transformation

$$T = \begin{bmatrix} 1 & & \\ & 1 & \\ & & 2 \end{bmatrix}$$

satisfies $TA_0T^\top = A_1$. Let

$$(A_1,B) = \left(A_1, \begin{bmatrix} a & b & c' \\ b & c & d \\ c' & d & e \end{bmatrix} \right).$$

Then the pair

$$\left(T^{-1}A_1\left(T^{-1}\right)^\top, T^{-1}B\left(T^{-1}\right)^\top\right) = (A_0,B')$$

is determined up to $\mathrm{SO}(\mathbb{Q},A_0)$ by (A_1,B), and the form

$$f(x,y) = ax^4 + 2bx^3y + (c+c')x^2y^2 + dxy^3 + \frac{1}{4}ey^4$$

is determined up to $\mathrm{PSL}_2(\mathbb{Q})$. This is a form of a peculiar shape, the $(1,2,1,1,\frac{1}{4})$-*forms*. Since the Wood embedding is resolvent-preserving, we see that the resolvent of a $(1,2,1,1,\frac{1}{4})$-form is actually integral, which can also be deduced directly from the formula for the resolvent of a binary quartic.

The $(1,2,1,1,\frac{1}{4})$-forms do not naturally have an action by $\mathrm{PGL}_2\mathbb{Z}$, but rather by a group that we can reveal as $\mathrm{SO}(\mathbb{Z},A_1)$:

Lemma 13.9. *We have* $\mathrm{SO}(\mathbb{Q}, A_1) \cong \mathrm{PGL}_2(\mathbb{Q})$ *via the isomorphism*

$$\varepsilon_{A_1} : M = \begin{bmatrix} a & b \\ c & d \end{bmatrix} \mapsto T\varepsilon_{A_0}(M)T^{-1} = \frac{1}{ad-bc} \begin{bmatrix} a^2 & ab & \frac{1}{2}b^2 \\ 2ac & ad+bc & bd \\ 2c^2 & 2cd & d^2. \end{bmatrix}$$

Under this map, the subgroup corresponding to $\mathrm{SO}(\mathbb{Z}, A_1)$ *is* $G = \mathrm{G}\Gamma^0(2) \sqcup \tau\mathrm{G}\Gamma^0(2)$*, where*

$$\mathrm{G}\Gamma^0(2) = \left\{ \begin{bmatrix} a & b \\ c & d \end{bmatrix} \in \mathrm{PGL}_2(\mathbb{Z}) : b \equiv 0 \mod 2 \right\}$$

is a congruence subgroup, and

$$\tau = \begin{bmatrix} & 2 \\ 1 & \end{bmatrix},$$

Proof. The first statement follows easily from considering the action of an element of $\mathrm{SO}(\mathbb{Q}, A_1)$ on the locus of isotropic points for A_1, a conic in $\mathbb{P}^2$ that is rationally isomorphic to $\mathbb{P}^1$. Note that ε_{A_1} is compatible with the map ε_{A_0} found earlier:

$$\varepsilon_{A_1} = T\varepsilon_{A_0}T^{-1}. \tag{114}$$

As for the second statement, if

$$M = \begin{bmatrix} a & b \\ c & d \end{bmatrix} \in \mathrm{PGL}_2(\mathbb{Q})$$

is given such that $\varepsilon_{A_1}(M)$ is integral, we first multiply by τ if needed to make $v_2(\det M)$ even, and then scale M so that a, b, c, d are coprime integers. Then we argue that if a prime p were to divide $ad - bc$, it must divide each of a,b,c,d by the integrality of $\varepsilon_{A_1}(M)$, which is a contradiction. ∎

We have now mapped each SL_3-orbit of pairs of integral symmetric matrices of A_1-type to a G-orbit of binary quartic $(1, 2, 1, 1, \frac{1}{4})$-forms; indeed, it is not hard to show that G is in fact the subgroup of $\mathrm{PGL}_2(\mathbb{Q})$ that preserves the lattice of forms of this shape, and we have, by an argument

similar to Lemma 13.7,

$$h^{A_1\text{-type}}\big(C,(2)\big) = \sum_{\substack{\text{quartic rings } Q \\ \text{with resolvent } C \\ \text{of } A_1 \text{ type,} \\ \text{up to } C\text{-isom}}} \frac{1}{|\mathrm{Aut}_C\, Q|} = \sum_{\substack{(1,2,1,1,\frac{1}{4})\text{-forms } f(x,y) \\ \text{with resolvent } g, \\ \text{up to } G}} \frac{1}{|\mathrm{Stab}_G\, f|}.$$

13.1.2 Type I

Following the same method, we can write

$$h^{I\text{-type}}\big(C,(2)\big) = \sum_{\substack{\text{quartic rings } Q \\ \text{with resolvent } C \\ \text{of } A \text{ type,} \\ \text{up to } C\text{-isom}}} \frac{1}{|\mathrm{Aut}_C\, Q|} = \sum_{\substack{(I,B) \text{ with resolvent } g \\ \text{up to } \mathrm{SO}(\mathbb{Z},I)}} \frac{1}{|\mathrm{Stab}_{\mathrm{SO}(\mathbb{Z},I)}\, B|}.$$

At this point we make two striking observations:

- The resolvent condition $\det(xI - yB) = g$ is equivalent to B having *characteristic polynomial* $g(x,1)$, so we have connected counting quartic rings to another classical problem, namely counting symmetric matrices of given characteristic polynomial;
- Since $\mathrm{SO}(\mathbb{Z},I)$ is a finite group, isomorphic to $\mathcal{S}_4$ (in its representation as the group of rotations of a cube), there is no need to count *orbits* of symmetric matrices; the matrices themselves will be finite in number.

Thus

$$h^{I\text{-type}}\big(C,(2)\big) = \frac{1}{24}\left|\{B \in \mathrm{Mat}^{3\times 3}\,\mathbb{Z} : \mathrm{char\,poly}(B) = g(x,1)\}\right|.$$

13.1.3 Conditions at ∞

The interpretations of class numbers of quartic rings that we have here developed can be modified to take into account local conditions or weightings at a prime. Here we only consider the prime at infinity.

Over $\mathbb{R}$ there are only two nondegenerate cubic algebras, $\mathbb{R}\times\mathbb{C}$ and $\mathbb{R}\times\mathbb{R}\times\mathbb{R}$. If $C_g \otimes \mathbb{R} \cong \mathbb{R}\times\mathbb{C}$ (that is, g has only one real root), then there is only one quartic algebra with resolvent C_g up to C_g-isomorphism, so it does not make sense to impose local conditions at the infinite place. If, on the

other hand, $C_g \otimes \mathbb{R} \cong \mathbb{R} \times \mathbb{R} \times \mathbb{R}$, then the three factors of $\mathbb{R}$ are non-interchangeable, being labeled by the three real roots of g, and there are four non-C_g-isomorphic quartic algebras with resolvent C_g (one isomorphic to $\mathbb{R} \times \mathbb{R} \times \mathbb{R} \times \mathbb{R}$ and three to $\mathbb{C} \times \mathbb{C}$), parametrized by the four Kummer elements $\delta \in C_g^{N=1}/(C_g^{N=1})^2$. The following is not hard to verify:

Lemma 13.10. *Let g be a monic binary cubic form over $\mathbb{R}$ whose dehomogenization has three real roots $\xi_1 < \xi_2 < \xi_3$. Identify the corresponding $\mathbb{R}$-algebra C_g with $\mathbb{R} \times \mathbb{R} \times \mathbb{R}$ with the coordinates ordered so that $\xi \mapsto (\xi_1, \xi_2, \xi_3)$. Let $L/\mathbb{R}$ be a quartic algebra with resolvent C_g. The corresponding pair (A, B) of real symmetric matrices is related to the sign of the corresponding Kummer element $\delta \in C_g^{N=1}/(C_g^{N=1})^2$ in the following way:*

- *If $\operatorname{sgn}\delta = (+,+,+)$, then (A,B) is of type A_1 and yields an indefinite binary quartic form with four real roots.*
- *If $\operatorname{sgn}\delta = (+,-,-)$, then (A,B) is of type A_1 and yields a positive definite binary quartic form.*
- *If $\operatorname{sgn}\delta = (-,-,+)$, then (A,B) is of type A_1 and yields a negative definite binary quartic form.*
- *If $\operatorname{sgn}\delta = (-,+,-)$, then (A,B) is of type I.*

13.1.4 Statements of results

We leave it to the reader to furnish the modifications of the condition at ∞ in the proof of Theorem* 13.3 to yield the following identities. Because $\mathbb{Z}$ is unramified at 2, we can prove them unconditionally, but only for tamely ramified resolvent at present.

Theorem 13.11 (**Quartic O-N for binary quartic forms**). *Let g be a monic integral binary cubic form whose splitting field is unramified at 2. Denote by $h(g)$ the number of integral binary quartic forms of resolvent g, up to $\mathrm{PGL}_2(\mathbb{Z})$-equivalence and weighted by inverse of $\mathrm{PGL}_2(\mathbb{Z})$-stabilizer. Denote by $h_4(g)$ the number of binary quartic $(1,2,1,1,\frac{1}{4})$-forms of resolvent g, up to G-equivalence*

and weighted by inverse of G-stabilizer. Denote by $s(g)$ the number of integral 3×3 symmetric matrices of characteristic polynomial g. Then:

- *If* $\operatorname{disc} g < 0$, *then*

$$2h(g) = h_4(g).$$

- *If* $\operatorname{disc} g > 0$, *then*

$$\begin{aligned} h(g) &= 2h_4^{indef}(g) \\ h^{indef\ or\ pos\ def}(g) &= h_4^{indef\ or\ pos\ def}(g) \\ h^{indef\ or\ neg\ def}(g) &= h_4^{indef\ or\ neg\ def}(g) \\ 24\big(h^{indef}(g) - h^{def}(g)\big) &= s(g) \end{aligned}$$

where the superscripts instruct one to count only forms satisfying the indicated condition at infinity, with the same weighting.

Corollary 13.12. *Let g be a monic integral binary cubic form with three real roots whose splitting field is unramified at 2. Among integral binary quartics with resolvent g, at least half are indefinite when we weight by inverse size of $\mathrm{PGL}_2(\mathbb{Z})$-stabilizer, with equality exactly when g is not the characteristic polynomial of an integral 3×3 symmetric matrix.*

We state these unconditionally because they apply only to the number field $K = \mathbb{Q}$. We do not attempt to generalize to other number fields. While the quartic rings of types corresponding to soluble conics (A_0 and A_1 in our notation) continue to be connected to binary quartic forms, the number of insoluble types grows with the degree of K.

13.2 The conductor property of the resolvent ring

We conclude this part of the paper with a family of results which at first do not look at all like reflection theorems.

Let R be an étale algebra over a local field K, and let E/R be an abelian extension whose Artin

map $\psi_{E/R} : R^\times \to \mathrm{Gal}(E/R)$ vanishes on the base $K^\times$. Call an order $\mathcal{O} \subseteq R$ an *admissible ring* for E if $\psi(\mathcal{O}^\times) = 0$. Such rings exist (e.g. $\mathcal{O} = \mathcal{O}_K + \mathfrak{f}$ where $\mathfrak{f} \subseteq R$ is the conductor ideal) and are stable under passage to suborders. If there is a unique maximal admissible ring, we call it the *conductor ring* of the extension E/R.

In like manner, we define admissible and conductor rings for an abelian extension E/R over a global field K, if the Artin map $\psi_{E/R} : I(R, \mathfrak{m}) \to \mathrm{Gal}(E/R)$ vanishes on the ideals $I(K, \mathfrak{m})$ of the base. By Lemma 10.1, if $E/R/K$ are fields, $\mathcal{O}$ is an admissible ring of E if and only if E is contained in the ring class field of $\mathcal{O}$.

In general, an extension E/R can have multiple maximal admissible rings, and there is no reason for a conductor ring to exist.

Example 13.13. Let $p \geq 5$ be a prime. Take $K = \mathbb{Q}_p$, $R = \mathbb{Q}_p^4$ and let $\chi : K^\times \to \mathbb{F}_p^\times$ be any multiplicative homomorphism extending the natural projection from $\mathbb{Z}_p^\times$. Define $\psi : R^\times \to \mathbb{F}_p^\times$ by

$$\psi(a; b; c; d) = \chi\left(\frac{ab}{cd}\right).$$

This is the Artin map of a certain $\mathbb{F}_p^\times \cong \mathbb{Z}/(p-1)\mathbb{Z}$-torsor E/R. By construction, ψ vanishes on $\mathbb{Q}_p^\times$, and the orders

$$\mathcal{O}_1 = \{(a; b; c; d) \in \mathbb{Z}_p^4 : a \equiv c, b \equiv d \mod p\}$$
$$\mathcal{O}_2 = \{(a; b; c; d) \in \mathbb{Z}_p^4 : a \equiv d, b \equiv c \mod p\}$$

are admissible rings for ψ. However, no ring strictly containing either $\mathcal{O}_1$ or $\mathcal{O}_2$ (of which there are very few) is an admissible ring for ψ; in particular, $\mathcal{O}_1 \cup \mathcal{O}_2$ generates the whole $\mathcal{O}_R$, which is certainly not an admissible ring for ψ. Thus ψ has no conductor ring.

However, in two special cases the conductor ring not only exists but has a striking characterization: it is the *resolvent ring* of a certain maximal order. These cases are those of general cubic and quartic algebras.

Proposition 13.14. *Let L/K be a cubic étale algebra over a global or local field. Let T be its quadratic resolvent torsor and $E = LT$ its $\mathcal{S}_3$-closure. Then the quadratic resolvent ring $\mathcal{O} \subseteq T$ of L is the conductor ring of E/T.*

Proof. The global case reduces immediately to the local one. The Artin map $\phi_{E/T}$ vanishes on $K^\times$ by the Galois symmetry of the situation (the same argument is carried out in a global context in Nakagawa [38, p. 110]), so L/K has admissible rings. Now the orders in T are totally ordered: they are simply of the form $\mathcal{O} = \mathcal{O}_K + \pi^i \mathcal{O}_T$ for $i \geq 0$. It is evident that the conductor ring of E/T must be $\mathcal{O}_K + \mathfrak{f}_{E/T}\mathcal{O}_T$, which has discriminant

$$\operatorname{disc} T \cdot \mathfrak{f}_{E/T}^2 = \operatorname{disc} T \cdot \operatorname{disc}(E/T).$$

The proposition is now reduced to the identity

$$\operatorname{disc} L = \operatorname{disc} T \cdot \operatorname{disc}(E/T).$$

This is a form of the "Brauer relation" between the absolute discriminants of L, T, and E and follows quickly from an Artin-conductor argument: see [12], equation (2.7). ∎

The above proof is not very deep and does not use reflection theorems at all. Let it be noted that over $K = \mathbb{Q}$, a very similar result was proved, if not stated, by Hasse ([26], table on p. 568) and forms a foundation to Nakagawa's proof of Ohno-Nakagawa [38, Lemma 1.3].

However, the quartic analogue of this statement, which we state in an identical way, is much deeper. Note that, in addition to the cubic resolvent R, a quartic étale algebra L/K has a natural sextic resolvent S coming from the map $\mathcal{S}_4 \to \mathcal{S}_6$ that sends a permutation of $\{1,2,3,4\}$ to the corresponding permutation of its 2-element subsets. S is naturally a quadratic étale extension of R with the same Kummer element $\delta \in R^{N=1}/\left(R^{N=1}\right)^2$ that parametrized L in 5.4.

Theorem* 13.15 (Conductor rings). *Assume Theorem* 13.2. Let L/K be a quartic étale algebra over a global number field or a p-adic field. Let R and S be its cubic and sextic resolvent algebras,*

respectively. Then the cubic resolvent ring $S_0 \subseteq R$ of $\mathcal{O}_L$ is the conductor ring of S/R.

Proof. The global case reduces immediately to the local one. To see the vanishing of $\phi_{S/R}$ on $K^\times$, let $S = R(\sqrt{\delta})$ where $S_{R/K}(\delta) = 1$. Then for $a \in K^\times$,

$$\phi_{S/R}(a) = \langle \delta, a \rangle = \langle a, \delta \rangle = \phi_{R(\sqrt{a})/R}(\delta) = \phi_{K(\sqrt{a})/K}\left(S_{R/K}(\delta)\right) = 1.$$

The conjecture now has two parts:

(a) S_0 is an admissible ring for S/R;

(b) Any admissible ring for S/R is contained in S_0.

As mentioned, this result does not on the surface look like a reflection theorem. But we will prove both (a) and (b) using Theorem* 13.2.

Let $g(L, S, \mathfrak{t})$ denote the number of $\mathfrak{t}$-traced orders in L with reduced resolvent S. Then Theorem* 13.2 states that

$$\hat{g}(L, S, (2)) = c \cdot g(L, S, (1)) \tag{115}$$

for the appropriate positive constant $c = |\mathcal{O}_L/2\mathcal{O}_L|$. Now $g(L, S, (1))$ is the number of orders in L of resolvent S. In particular, it is 1 if $S = S_0$ and 0 if $S \not\subseteq S_0$. On the other hand, $g(L', S, (2))$ can be interpreted as the number of ideals $I \subseteq R$ such that (S, I, δ') is balanced, and overall

$$\begin{aligned}
\hat{g}(L, S, (2)) &= \frac{1}{|H^0(M_R)|} \sum_{\delta' \in H^1(M_R)} \langle \delta, \delta' \rangle \, g(L_{\delta'}, S, (2)) \\
&= \frac{1}{|H^0(M_R)|} \sum_{\substack{\delta' \in H^1(M_R) \\ (S,I,\delta') \text{ balanced}}} \langle \delta, \delta' \rangle \\
&= \frac{1}{|H^0(M_R)|} \sum_{\substack{\delta' \in H^1(M_R) \\ (S,I,\delta') \text{ balanced}}} \phi_{S/R}(\delta'). \qquad (116)
\end{aligned}$$

(117)

Assume for the sake of contradiction that $S = S_0$ is not an admissible ring for S/R. Then there

exists $\varepsilon \in S^\times$ such that $\phi_{S/R}(\varepsilon) = -1$. The rearrangement of terms $(S, I, \delta') \mapsto (S, I, \varepsilon\delta')$ flips the sign of the sum, so $\hat{g}(L, S, (2)) = 0$, a contradiction, since $g(L, S, (1)) = 1$. This proves (a).

Now assume for the sake of contradiction that there is an admissible ring $S \not\subseteq S_0$. Choose such an S maximal for this property. Then divide the summands of (116) into two cases:

- If I is invertible in S, then $I = \alpha S$ for some α, and $\delta = \alpha^2\varepsilon$ for some $\varepsilon \in S^\times$. These terms contribute

$$\phi_{S/R}(\delta) = \phi_{S/R}(\varepsilon) = 1,$$

  since S is an admissible ring. There is at least one term of this type, namely $\delta = 1$, $I = S$.

- If I is not invertible in S, then $\operatorname{End} I^2 = S' \supsetneq S$. (If we had $\operatorname{End} I^2 = S$, then by Lemma 14.4, I^2 would be invertible in S and then I would also.) By maximality, S' is *not* an admissible ring for S/R and there is an $\varepsilon \in S'^\times$ such that $\phi_{S/R}(\varepsilon) = -1$. The rearrangement $(S, I, \delta') \mapsto (S, I, \varepsilon\delta')$ permutes the terms with the same S' and flips their signs. So the terms of this type contribute nil.

Overall, we get $\hat{g}(L, S, (2)) > 0$, a contradiction, since $g(L, S, (1)) = 0$. This proves (b). ■

14 Tame quartic rings with non-split resolvent, by multijection

In this section, we will adapt the methods of Section 11.1 to prove Theorem* 13.2 in the case that K is tame (not 2-adic) and $R \ncong K \times K \times K$.

14.1 Invertibility of ideals in orders

We begin with a technical inquiry that has interest in its own right. It is well known that every $\mathbb{Z}$-lattice $\mathfrak{a}$ in a quadratic field is invertible with respect to *some* order, namely its endomorphism ring $\operatorname{End}\mathfrak{a}$. In a cubic or higher-degree field this is not so. However, the following two lemmas will help us understand the structure of orders and ideals in such a setting.

Lemma 14.1. *Let K be a local field, and let $\mathcal{O}$ be an order in a finite-rank étale algebra L over K. Then there is a decomposition*

$$L = L_1 \times \cdots \times L_s,$$

each L_i being the product of some field factors of L, with the following properties:

$$\mathcal{O} = \mathcal{O}_1 \times \cdots \times \mathcal{O}_s$$

is the product of orders in the L_i, and each $\mathcal{O}_i$ has only a single prime $\mathfrak{p}_i$ above the valuation ideal $\mathfrak{p}$, so that every element of $\mathcal{O}_i$ not lying in $\mathfrak{p}_i$ is a unit.

Proof. Let $L = K_1 \times \cdots \times K_r$ be the field factor decomposition of L. Each K_i is a local field; let $\mathfrak{p}_i$ be the pullback to L of the valuation ideal of K_i. Define an equivalence relation on the $\mathfrak{p}_i$ by

$$\mathfrak{p}_i \sim \mathfrak{p}_j \iff \mathfrak{p}_i \cap \mathcal{O} = \mathfrak{p}_j \cap \mathcal{O}.$$

Thus if $\mathfrak{p}_i \nsim \mathfrak{p}_j$, then there is an $\alpha \in \mathcal{O}$ such that either

$$\mathfrak{p}_i \nmid \alpha, \mathfrak{p}_j | \alpha \quad \text{or} \quad \mathfrak{p}_i | \alpha, \mathfrak{p}_j \nmid \alpha. \tag{118}$$

Suppose for the moment that it is the first. We first claim that we can take $\alpha \equiv 1 \bmod \mathfrak{p}_i$. Note that $\mathcal{O}_L/\mathfrak{p}_i$ is a finite field extension of $\mathcal{O}_K/\mathfrak{p}$, so α satisfies a polynomial congruence

$$\alpha^m + u_{m-1}\alpha^{m-1} + \cdots + u_0 \equiv 0 \mod \mathfrak{p}_i, \quad u_i \in \mathcal{O}_K, \quad u_0 \in \mathcal{O}_K^\times.$$

Then

$$\alpha' = -u_0^{-1}(\alpha^m + u_{m-1}\alpha^{m-1} + \cdots + u_1\alpha)$$

is 1 mod $\mathfrak{p}_i$ and 0 mod $\mathfrak{p}_j$. Also, note that we can switch α' with $1 - \alpha'$ to satisfy these congruences for any i and j, regardless of which condition in (118) held to begin with.

Fix i and multiply the resulting values of α', which are 1 mod $\mathfrak{p}_i$ (and hence 1 mod any $\mathfrak{p}_j \sim \mathfrak{p}_i$) but 0 mod $\mathfrak{p}_j$ for any chosen $\mathfrak{p}_j \nsim \mathfrak{p}_i$. We get a single α'' such that

$$\alpha'' \equiv \begin{cases} 1 \mod \mathfrak{p}_j, & \mathfrak{p}_j \sim \mathfrak{p}_i \\ 0 \mod \mathfrak{p}_j, & \mathfrak{p}_j \nsim \mathfrak{p}_i. \end{cases}$$

As a final step, we can iterate the polynomial

$$f(x) = x^2(3 - 2x),$$

which takes $\mathfrak{p}_i^m$ to $\mathfrak{p}_i^{2m}$ and $1 + \mathfrak{p}_i^m$ to $1 + \mathfrak{p}_i^{2m}$, and take the limit to derive that the idempotent $e = (e_j)_j \in \mathcal{O}_L$, defined by

$$e_j = \begin{cases} 1, & \mathfrak{p}_j \sim \mathfrak{p}_i \\ 0, & \mathfrak{p}_j \nsim \mathfrak{p}_i, \end{cases}$$

lies in $\mathcal{O}$ ($\mathcal{O}$ is closed in the $\mathfrak{p}$-adic topology). These e_j's form a set of orthogonal idempotents decomposing $\mathcal{O}$ into a direct product of $\mathcal{O}_i$, one for each $\sim$-equivalence class, that have the properties we seek. ■

Lemma 14.2. *Let K be a local field, and let $\mathcal{O}$ be an order in a finite-rank étale algebra L over K. Then a fractional ideal of $\mathcal{O}$ is invertible if and only if it is principal.*

Remark 14.3. This implies that a if $\mathcal{O}$ is an order in a finite-rank algebra over a Dedekind domain, then a fractional ideal of $\mathcal{O}$ is invertible if and only if it is locally principal, where here "locally" denotes localization at each prime of K. Thus our statement and proof differ slightly from the corresponding statement in Neukirch [39] (Theorem I.12.4), which is built by localization at the primes *of* $\mathcal{O}$ (and also assumes that $\mathcal{O}$ is a domain).

Proof. By the preceding lemma, an ideal of a product $\mathcal{O}_1 \times \cdots \times \mathcal{O}_s$ is just a product $\mathfrak{a}_1 \times \cdots \times \mathfrak{a}_s$, which is principal (resp. invertible) if and only if every $\mathfrak{a}_i$ is: hence we can assume that $s = 1$.

The reverse direction is trivial (principal fractional ideals are invertible), so let $\mathfrak{a}$ be an ideal of

$\mathcal{O}$ with inverse $\mathfrak{a}^{-1}$, $\mathfrak{a}\mathfrak{a}^{-1} = \mathcal{O}$. Since all ideals of $\mathcal{O}_L$ are principal, we can assume that $\mathfrak{a}\mathcal{O}_L = \mathcal{O}_L$ and hence $\mathfrak{a}^{-1}\mathcal{O}_L = \mathcal{O}_L$ as well. We can express

$$1 = \sum_i \alpha_i \beta_i, \quad \alpha_i \in \mathfrak{a}, \quad \beta_i \in \mathfrak{a}^{-1}.$$

Let $\mathfrak{p}_1, \ldots, \mathfrak{p}_r$ be the valuation ideals coming from the field factors of L. Since $1 \notin \mathfrak{p}_1$, some term $\alpha_i\beta_i$, say $\alpha_1\beta_1$, is nonzero mod $\mathfrak{p}_1$. But because $\mathfrak{p}_i \cap \mathcal{O} = \mathfrak{p}_1 \cap \mathcal{O}$ is the unique maximal ideal of $\mathcal{O}$ for all i, we have $\alpha_1\beta_1 \notin \mathfrak{p}_i$ for all i. This implies that α_1 and β_1 are units, whose product lies in $\mathcal{O}^\times$. Now since

$$\mathfrak{a} \supset \alpha_1\mathcal{O}, \quad \mathfrak{b} \supset \beta_1\mathcal{O}$$

and $\mathfrak{a}\mathfrak{b} = \mathcal{O}$, equality must hold. ■

Lemma 14.4. *If $\mathfrak{c} \subseteq R$ is a lattice in a cubic algebra over a local field K, then $\mathfrak{c}^2$ is invertible in its endomorphism ring* $\mathrm{End}(\mathfrak{c}^2)$.

Proof. First, $\mathfrak{c}\mathcal{O}_R$ is an invertible $\mathcal{O}_R$-ideal, which, since $\mathcal{O}_R$ is a product of PID's, we can scale to be $\mathcal{O}_R$.

We first claim that $\mathfrak{c}$ contains a unit, or else has a special form for which $\mathfrak{c}^2 = \mathcal{O}_R$ is clearly invertible. Let p be a uniformizer for $\mathcal{O}_K$ and $k = \mathcal{O}_K/p\mathcal{O}_K$ the residue field. The units of $\mathcal{O}_R$ are those elements whose projections to the cubic k-algebra $\overline{C_1} = C_1/pC_1$ are non-units (that is, zero divisors). The non-units of $\overline{C_1}$ are the union of at most three proper subspaces (the projections of the valuation ideals of each field factor). The projection $\bar{\mathfrak{c}}$ of $\mathfrak{c}$ down to $\overline{C_1}$ cannot lie in any of these subspaces since $\mathfrak{c}\mathcal{O}_R = C_1$. An easy theorem in linear algebra is that a vector space over a field k cannot be the union of fewer than $|k| + 1$ proper subspaces. We conclude that $\mathfrak{c}$ contains a unit except if $|k| = 2$ and $R = K \times K \times K$ has three field factors. In this case, the only $\bar{\mathfrak{c}} \subseteq \overline{C_1}$ instantiating this case is

$$\bar{\mathfrak{c}} = \{(a; b; c) \in \mathbb{F}_2^3 : a + b + c = 0\}.$$

It is evident that $\bar{\mathfrak{c}}^2$ is the whole of $\mathbb{F}_2^3$, whence by Nakayama's lemma, $\mathfrak{c}^2$ is the whole of $\mathcal{O}_R$.

Now we can assume that $\mathfrak{c}$ contains a unit, which we scale to equal 1. We claim that $\mathfrak{c}^3 = \mathfrak{c}^2$. By the theory of modules over a PID, we can find a basis $\{1, \alpha, \beta\}$ for $\mathcal{O}_K$ such that $\{1, p^i\alpha, p^j\beta\}$ is a basis for $\mathfrak{c}$ for some integers $i, j \geq 0$. Now by translation, we can assume that $\alpha\beta = t \in \mathcal{O}_K$. We then have

$$\mathfrak{c}^3 = \mathfrak{c}^2 + \langle \alpha^3, \alpha^2\beta, \alpha\beta^2, \beta^3 \rangle = \mathfrak{c}^2 + \langle \alpha^3, t\alpha, t\beta, \beta^3 \rangle$$

The elements $t\alpha$ and $t\beta$ are certainly already in $\mathfrak{c} \subseteq \mathfrak{c}^2$. As for α^3, since α is an integral element of R, its characteristic polynomial expresses α^3 as an $\mathcal{O}_K$-linear combination of α^2, α, and 1, all of which lie in $\mathfrak{c}^2$. So $\mathfrak{c}^3 = \mathfrak{c}^2$.

We conclude that $\mathfrak{c}^4 = \mathfrak{c}^3 = \mathfrak{c}^2$, so $\mathfrak{c}^2$ is closed under multiplication and hence is an order. In particular, it coincides with its endomorphism ring and in particular is invertible. ■

Remark 14.5. Although Lemma 14.4 is simple to state, we have not found it anywhere in the literature. In general, we suspect that if $\mathfrak{c}$ is a lattice in an algebra L of rank n, then $\mathfrak{c}^{n-1}$ and all higher powers of $\mathfrak{c}$ are invertible in their common endomorphism ring. This is not hard to prove if $\operatorname{char} k_K > n$. That the exponent $n-1$ is sharp is seen from the cute example

$$\mathfrak{c} = \mathbb{Z}_p + (0; 1; \ldots; n-1)\mathbb{Z}_p + p\mathbb{Z}_p^n \subseteq \mathbb{Z}_p^n.$$

The power $\mathfrak{c}^i$ consists of all sequences $(a_0; \ldots; a_{n-1}) \in \mathbb{Z}_p^n$ that are congruent modulo p to the values

$$(f(0); f(1); \ldots; f(n-1))$$

of a polynomial f of degree at most i with coefficients in k. If $p > n$, then this power stabilizes to the whole of $\mathbb{Z}_p^n$ only for $i \geq n-1$.

14.2 Self-duality of the count of quartic orders

Theorem 14.6 (Local quartic O-N in the tame, not totally split case). *Assume K is a local field of residue characteristic not 2. Let $C \subseteq R$ be a cubic étale order that is* not *totally split. Then*

the assignment f_C to each L of the number of orders $\mathcal{O} \subseteq L$ with resolvent C is self-dual.

Proof. As in the cubic case, the proof proceeds by reduction to the zero case (i.e. that $f(0) = \hat{f}(0)$).

Note that $M \cong M'$ as Galois modules (one can even make this canonical, using the unique alternating bilinear form on M). The fixity of this Galois module is easy to compute:

$$|H^0| = |H^0(K, R)| = \begin{cases} 1 & \text{if } R \text{ is a field} \\ 2 & \text{if } R \cong K \times K_2 \text{ for some quadratic field } K_2 \\ 4 & \text{if } R \cong K \times K \times K. \end{cases}$$

This can be written concisely as

$$|H^0| = \frac{|R^\times[2]|}{2}$$

(the latter formula will work especially well for our case).

Moreover, since the unramified cohomology is self-orthogonal, we have

$$|H^1| = |H^0|^2 = \frac{|R^\times[2]|^2}{4}.$$

Since we are excluding the case $R \cong K \times K \times K$, there are just two possibilities:

- If R is a field, then $|H^1| = 1$, and there is nothing to prove, as any function on H^1 is self-dual.
- If R is the product of two fields, then $|H^1| = 4$. Pick an $\mathbb{F}_2$-basis $\langle \sigma_1, \sigma_2 \rangle$. The Tate pairing is given by the unique alternating pairing on H^1. The space of functions on H^1 is four-dimensional, and a basis is

  $$\mathbf{1}_{\langle \sigma_1 \rangle}, \mathbf{1}_{\langle \sigma_2 \rangle}, \mathbf{1}_{\langle \sigma_1 + \sigma_2 \rangle}, \mathbf{1}_{\{0\}}.$$

  Note that the first three basis elements are self-dual, while the fourth differs from its dual even at 0. This proves that if f is a function on H^1 with $f(0) = \hat{f}(0)$, then $f = \hat{f}$.

So we have reduced local O-N to the following lemma: ■

Lemma 14.7. *Assume K is a local field of residue characteristic not 2. Let $C \subseteq R$ be an order in an étale algebra. Then the assignment g_C to each L of the number of orders $\mathcal{O} \subseteq L$ with resolvent C satisfies self-duality at 0:*

$$\hat{g}_C(0) = g_C(0).$$

Proof. As in the cubic case, the proof is by explicit multijection.

On the one hand,

$$|H^0| \cdot \hat{g}_C(0) = \sum_{\sigma} g_C(\sigma)$$

counts all quartic orders with cubic resolvent C, and using Theorem 6.18, these can be parametrized by self-balanced ideals $(C, \mathfrak{c}, \delta)$, where δ ranges over a set of representatives for $R^{N=1}/\left(R^{N=1}\right)^2$. On the other hand, $g_C(0)$ is the number of orders with resolvent C in $K \times R$. Write such an order as $\mathcal{O} = \mathcal{O}_K + 0 \times \mathfrak{a}$, where $\mathfrak{a} \subseteq R$ is a lattice. The condition that $\mathcal{O}$ be a ring is (by Theorem 6.13) subsumed by the resolvent conditions, namely that

(i) $N_C(\mathfrak{a}) = 1$,

(ii) $\Phi_{4,3}(0; \alpha) = \alpha' \alpha'' \in C$ for all $\alpha \in \mathfrak{a}$.

Our aim is to associate $|H^0|$ values of $(\mathfrak{c}, \delta)$ to each value of $\mathfrak{c}$.

The multijection is as follows. First, $\mathfrak{c}$ may not be invertible. Let $C_1 = \operatorname{End} \mathfrak{c}^2$ and $\mathfrak{c}_1 = \mathfrak{c}C_1$, an invertible and thus a principal C_1-ideal. Let

$$\mathfrak{a}_1 = \frac{[C_1 : C]}{\delta[\mathfrak{c}_1 : \mathfrak{c}]} \left(\mathfrak{c}_1^2\right)^{-1}. \tag{119}$$

Finally, since $\mathfrak{c}_1$ and $\mathfrak{a}_1$ are both principal and thus scalar multiples of each other, we can take $\mathfrak{a}$ to be an ideal that sits inside $\mathfrak{a}_1$ as $\mathfrak{c}$ sits inside $\mathfrak{c}_1$: that is, if $\mathfrak{c}_1 = \gamma_0 C_1$ and $\mathfrak{a}_1 = \alpha_0 C_1$, then

$$\mathfrak{a} = \frac{\alpha_0}{\gamma_0} \mathfrak{c}.$$

Before checking that this $\mathfrak{a}$ yields a valid ring, we check how many-to-one our multijection is. First

note that $\mathfrak{a}$ determines $C_1 = \operatorname{End}\mathfrak{a}^2$ and $\mathfrak{a}_1 = \mathfrak{a}C_1$, and in particular the index $[\mathfrak{c}_1 : \mathfrak{c}] = [\mathfrak{a}_1 : \mathfrak{a}]$. Then, by (119), the "shadow" $\mathfrak{b} = \delta\mathfrak{c}^2 = \delta\mathfrak{c}_1^2$ is determined. Note that $\mathfrak{b}$ is an invertible C_1-ideal of norm $[C_1 : C]^2/[\mathfrak{a}_1 : \mathfrak{a}]^2$, a square. The pairs $(\mathfrak{c}_1, \delta)$ satisfying $\mathfrak{b} = \delta\mathfrak{c}_1$, where $\mathfrak{c}_1$ is an invertible C_1-ideal and δ is one of the representatives for $R^{N=1}/\left(R^{N=1}\right)^2$, are found to be $|H^0|$ in number by an argument identical to the cubic case. Finally, locating $\mathfrak{c}$ within $\mathfrak{c}_1$ involves the same choice as locating $\mathfrak{a}$ within $\mathfrak{a}_1$. So we have a string of many-to-one correspondences

$$(\mathfrak{c}, \delta) \xrightarrow{n \text{ to } 1} (\mathfrak{c}_1, \delta) \xrightarrow{|H^0| \text{ to } 1} \mathfrak{a}_1 \xleftarrow{n \text{ to } 1} \mathfrak{a}, \tag{120}$$

and thus overall there are $|H^0|$ times as many $(\mathfrak{c}, \delta)$ as $\mathfrak{a}$.

It remains to prove that the correspondence (120) preserves the resolvent and balancing conditions. As for the first condition, regarding the discriminant of the ring, we leave it to the reader to verify that

$$N_C(\mathfrak{a}) = \frac{1}{N(\delta)N_C(\mathfrak{c})^2}. \tag{121}$$

Now we may assume that both sides of (121) are 1. Since $\mathfrak{c}_1$ is principal, we may assume that $\mathfrak{c}_1 = C_1$, adjusting δ by a square if necessary. Then by the conditions of Theorem 6.18, $N(\delta)$ is a square t^2 and

$$\frac{1}{t} = N_C(\mathfrak{c}) = \frac{[C_1 : C]}{[\mathfrak{c}_1 : \mathfrak{c}]};$$

thus

$$\mathfrak{a}_1 = \frac{t}{\delta}C_1.$$

We first prove that if $\mathfrak{c}$ satisfies its resolvent condition, so does $\mathfrak{a}$. Any $\alpha \in \mathfrak{a} \subseteq \mathfrak{a}_1$ has the form $\alpha = \frac{t}{\delta}\beta$, $\beta \in C_1$, and then

$$\alpha'\alpha'' = \frac{t^2}{\delta'\delta''}\beta'\beta'' = \delta\beta'\beta'';$$

and we note that if $\beta \in C_1$, then $\beta'\beta'' \in C_1$ as well, by the relation

$$\beta'\beta'' = \underbrace{\beta\beta' + \beta\beta'' + \beta'\beta''}_{\in\mathcal{O}_K} - \beta(\underbrace{\beta + \beta' + \beta''}_{\in\mathcal{O}_K} - \beta). \tag{122}$$

Thus if $\mathfrak{c}$ satisfies the resolvent condition ($\delta\mathfrak{c}^2 \subseteq C$), then $\mathfrak{a}$ satisfies the resolvent condition ($\alpha'\alpha'' \in C$ for all $\alpha \in \mathfrak{a}$). To prove the converse, it suffices to show that

$$B = \{\beta'\beta'' : \beta \in \mathfrak{c}\}$$

spans C_1 over $\mathcal{O}_K$, where $\mathfrak{c} \subseteq C_1$ is a sublattice with $\mathfrak{c}^2 = C_1$.

We first claim that $\mathfrak{c}$ contains a unit. Let p be a uniformizer for $\mathcal{O}_K$ and $k = \mathcal{O}_K/p\mathcal{O}_K$ the residue field. In the cubic k-algebra $\overline{C_1} = C_1/pC_1$, the non-units are the union of at most three subspaces. The projection $\bar{\mathfrak{c}}$ of $\mathfrak{c}$ down to $\overline{C_1}$ cannot lie in any of these subspaces since $\mathfrak{c}^2 = C_1$, so, since $|k| \geq 3$, $\bar{\mathfrak{c}}$ must contain a unit, which lifts to a unit in $\mathfrak{c}$. There is no harm in rescaling $\mathfrak{c}$ so that $1 \in \mathfrak{c}$.

Now $1 \in B$. Also, for each $\beta \in \mathfrak{c}$,

$$\langle B\rangle \ni \beta'\beta'' - (\beta' + 1)(\beta'' + 1) + \operatorname{tr}\beta - 1 = \beta,$$

and thus

$$\langle B\rangle \ni \beta'\beta'' - (\beta\beta' + \beta\beta'' + \beta'\beta'') + \beta(\beta + \beta' + \beta'') = \beta^2.$$

But since $\operatorname{char} k \neq 2$, the elements β^2, for $\beta \in \mathfrak{c}$, generate $\mathfrak{c}^2 = C_1$, completing the proof. ■

For the totally split case, the method of proof of Theorem 14.6 fails, because $\dim H^1 = 4$ and $\hat{f}(0) = f(0)$ is no longer enough to imply $\hat{f} = f$. But when we count by discriminant instead of resolvent, it can be rescued, due to the following symmetry argument.

Theorem 14.8. *Fix a cubic algebra R over a local field K, and let $g_D : H^1 \to \mathbb{Z}$ count the number of orders in a quartic algebra $L \in H^1$ with discriminant D. That is, g_D is the sum of all the g_C's*

in Theorem 14.6 over $C \subseteq R$ of discriminant D. Then g_D is self-dual.

Proof. All cases are covered by Theorem 14.6 except for the totally split case $R \cong K \times K \times K$, where $\dim H^1 = 4$. We can write $H^1 = \langle \sigma_1, \tau_1, \sigma_2, \tau_2 \rangle$, where the σ's and τ's correspond to Kummer elements

$$\sigma_1 : (u, u, 1), \quad \tau_1 : (p, p, 1), \quad \sigma_2 : (1, u, u), \quad \tau_2 : (1, p, p),$$

where $p \in \mathcal{O}_K$ is a uniformizer and u is a non-square unit. The Tate pairing is given, by Theorem 5.7, by the μ_2-valued pairing

$$\langle \sigma_1, \tau_2 \rangle = \langle \sigma_1, \tau_2 \rangle = -1, \quad \langle \sigma_1, \sigma_2 \rangle = \langle \tau_1, \tau_2 \rangle = \langle \sigma_1, \tau_1 \rangle = \langle \sigma_2, \tau_2 \rangle = 1.$$

The group $\operatorname{Aut} R \cong \mathcal{S}_3$ acts on H^1, permuting $\sigma_1, \sigma_2, \sigma_1 + \sigma_2$ and $\tau_1, \tau_2, \tau_1 + \tau_2$ in the permutation manner. There are five orbits, represented by 0, σ_1, τ_1, $\sigma_1 + \tau_1$, and $\sigma_1 + \tau_2$. Note that g_D must be constant on each orbit, because its definition is S_3-invariant. The functions

$$\mathbf{1}_{\langle \sigma_1, \sigma_2 \rangle}, \mathbf{1}_{\langle \tau_1, \tau_2 \rangle}, \mathbf{1}_{\langle \sigma_1 + \tau_1, \sigma_2 + \tau_2 \rangle}, \sum_{\pi \in \operatorname{Aut} R} \mathbf{1}_{\pi(\langle \sigma_2, \sigma_1 + \tau_2 \rangle)}, \mathbf{1}_{\{0\}}$$

form a basis for the 5-dimensional space of $\mathcal{S}_3$-invariant functions on H^1. The first four are self-dual, while the last differs from its dual even at 0; so, since $g_D(0) = \hat{g}_D(0)$ by Lemma 14.7), the coefficient of the last basis element must be 0 and g_D is self-dual. ■

Part VII

Counting quartic rings with prescribed resolvent

15 Introduction

Here end the cases in which a conceptual, bijective argument has been found to suffice for proving local reflection for quartic rings. To win the remaining cases, we attack a problem that has interest in its own right: counting orders $\mathcal{O}$ in a quartic algebra L over a local field K whose cubic resolvent ring $C \subseteq R$ is fixed.

The index $[\mathcal{O}_L : \mathcal{O}]$ being fixed by the condition $\operatorname{Disc}\mathcal{O} = \operatorname{Disc} C$, we must analyze the resolvent condition $\Phi_{4,3}(\mathcal{O}/\mathcal{O}_K) \subseteq C/\mathcal{O}_K$, where $\Phi_{4,3} : L/K \to R/K$ is the resolvent map. Recall that, with respect to bases of $\mathcal{O}$ and C, $\Phi_{4,3}$ is given by a pair

$$(\mathcal{M}, \mathcal{N}) = ([M_{ij}], [N_{ij}])$$

of symmetric 3×3 matrices, and the resolvent condition can be viewed as the $\mathcal{O}_K$-integrality of the entries (properly scaled to account for the tracedness condition). By suitably choosing coordinates, we can ensure that only the integrality of the entries

$$M_{11}, \quad N_{11}, \quad M_{12}, \quad \text{and} \quad M_{22}$$

is in doubt. Of these, the condition on M_{11} is the most challenging. It amounts to a quadratic condition on the first basis vector ξ_1 of C, that is, a conic on some pixel (determined by the N_{11}-condition) in $\mathbb{P}^2(\mathcal{O}_K)$. The solubility of this conic over K is governed by the *Hilbert symbol,* which we analyze. It is very hard in general to tell if any K-points of the conic lie in the requisite pixel,

but if there is even one such K-point, then, using the rational parametrization of a conic with a basepoint, the volume of points in the pixel is easy to determine. Accordingly, our approach to solving the M_{11}-condition is a three-step one:

- Determine the sum of the solution volumes for ξ_1 over all quartic algebras L.
- Find restrictions on what L can yield a nonzero volume and what that volume can be, providing an upper bound (the *bounding step*).
- If the sums of these upper bounds agree, deducing that the bound is attained everywhere (the *summing step*).

The M_{12} and M_{22} conditions are essentially linear. We use the computer program LattE to sum the ring totals over all possible values of the discrete data and verify the local reflection theorem.

The case of wildly ramified resolvent (splitting type 1^21) is still in progress. Except for brief remarks, it has been omitted from this edition. Also omitted are the adaptations to be made when $\operatorname{char} k_K > 2$, where, in view of Theorem 14.6, only splitting type (111) need be considered. It involves only the black, brown, beige, and white zones; the conics are all very easy to solve and yield the same answers as the wild case upon substituting $e = 0$. So in the sequel, R **is a tamely ramified étale algebra over a 2-adic local field** K**.**

Corresponding to R, there is a Galois module M_R whose underlying group is $\mathcal{C}_2 \times \mathcal{C}_2$. We will work extensively with $H^1(K, M_R)$, which we abbreviate to H^1.

16 The group H^1 of quartic algebras with given resolvent

We fix a local field K and an separable closure $\bar{K}$. Let $\mathcal{O}_{\bar{K}}$ be the ring of integers in $\bar{K}$. (If the reader is uncomfortable with non-Noetherian rings, he can take $\bar{K}$ to be instead the compositum of all extensions of K of degree at most 4; the Galois cohomology and all proofs will be unaffected.)

By Theorem 5.4(c), we can identify H^1 naturally with

$$R^{N=1} / \left(R^{N=1}\right)^2.$$

Now there is a natural isomorphism

$$R^\times/(R^\times)^2 \cong K^\times/(K^\times)^2 \times R^{N=1}/\left(R^{N=1}\right)^2.$$

Thus for any $\alpha \in R^\times$, we can talk about the class $[\alpha]$ of α in H^1, that is, the class of $\alpha^3/N(\alpha)$.

Hence the structure of H^1 can be uncovered by taking a suitable Shafarevich basis of $R^\times/(R^\times)^2$ and removing a basis of $K^\times/(K^\times)^2$, which, by Lemma 7.13, maps in isometrically:

Lemma 16.1. *If R/K is a cubic étale extension, then H^1 is an $\mathbb{F}_2$-vector space of dimension $2\dim_{\mathbb{F}_2} H^0 + 2ef$. It has a basis of $\dim_{\mathbb{F}_2} H^0$ nonunits, $\dim_{\mathbb{F}_2} H^0$ intimate units, and $2ef$ generic units; the generic units can be chosen as follows:*

(*a*) *If R is unramified, we take $2ef$ units of the form $1 + x\pi^{2i+1}$, where $0 \le i < e$ and x ranges over f elements whose reductions mod π form an $\mathbb{F}_2$-basis of $k_R^{\mathrm{tr}=0}$ for each i.*

(*b*) *If R is totally tamely ramified, we take $2ef$ units of the form $1 + x\pi^{2i+1}$, where $0 \le i < 3e$ but $3 \nmid i$, and x ranges over an $\mathbb{F}_2$-basis of k_K for each i.*

In the unramified case, we define the *level space*

$$\mathcal{L}_i = \begin{cases} H^1 & i = -1 \\ \{[\alpha] \in H^1 : \alpha \equiv 1 \mod \pi^{2i}\} & 0 \le i \le e \\ \{[1]\} & i = e+1, \end{cases}$$

noting that $|\mathcal{L}_i| = |H^0| q^{2(e-i)}$ for $0 \le i \le e$ and that $\mathcal{L}_i^\perp = \mathcal{L}_{e-i}$ for all i by Lemma 7.19.

Likewise, in the ramified case, we define the *level space*

$$\mathcal{L}_i = \begin{cases} H^1 & i = -1 \\ \{[\alpha] \in H^1 : \alpha \equiv 1 \mod \pi^{i}\} & 0 \le i \le 2e \\ \{[1]\} & i = e+1, \end{cases}$$

noting that $|\mathcal{L}_i| = |H^0| q^{2e-i}$ for $0 \le i \le e$ and that $\mathcal{L}_i^\perp = \mathcal{L}_{2e-i}$ for all i by Lemma 7.19.

We will occasionally let

$$e' = \begin{cases} e, & R \text{ unramified} \\ 2e, & R \text{ ramified} \end{cases}$$

to shorten lemma statements.

We define the *level* $\ell(\alpha)$ of an element $[\alpha] \in H^1$ as the largest $i \ge 0$ for which $[\alpha] \in \mathcal{L}_i$. We have $\ell(1) = e' + 1$. By convention, if $[\alpha] \notin \mathcal{L}_0$, we set

$$\ell(\alpha) = -1/2$$

to shorten some future statements.

17 Reduced bases

Define a valuation on $\bar{K}^n$ by

$$v(x_1; \ldots; x_n) = \min\{v(x_1), \ldots, v(x_n)\}.$$

Let R be a rank-n étale algebra over a local field K. We can Minkowski-embed R into $\bar{K}^n$.

Definition 17.1. Let I be an $\mathcal{O}_K$-lattice in R, and let $\omega \in \bar{K}^n$ be a multiplier with the following property:

(∗) If ι, ι' are two coordinates of the same field factor of R, then $\omega^{(\iota)}$ and $\omega^{(\iota')}$ have the same valuation.

A basis $(\rho_1, \ldots, \rho_n)$ for ωI is called *reduced* if

(a) $v(\rho_1) \le \cdots \le v(\rho_n)$;

(b) If $\rho \in \omega R$ is decomposed as

$$\rho = \sum_i c_i \rho_i, \quad c_i \in K,$$

then for each i,

$$v(c_i\rho_i) \geq v(\rho).$$

This notion has the following properties:

Proposition 17.2. *Let ωI be as above.*

(a) *There exists a reduced basis $(\rho_1, \ldots, \rho_n)$ for ωI.*

(b) *If $(\rho'_1, \ldots, \rho'_n)$ is any other basis for ωI, sorted so that $v(\rho'_1) \leq \cdots \leq v(\rho'_n)$, then for each k,*

$$v(\rho'_k) \leq v(\rho_k).$$

In particular, if both bases are reduced, equality holds.

(c) *If $(\rho'_1, \ldots, \rho'_n)$ is another reduced basis for ωI, then*

$$\rho'_i = \sum_j c_{ij}\rho_j$$

for some change-of-basis matrix

$$[c_{ij}] \in \mathrm{GL}_n\mathcal{O}_K, \quad v\left(c_{ij}\right) \geq v(\rho_i) - v(\rho_j). \tag{123}$$

Conversely, any matrix $[c_{ij}]$ satisfying (123) *yields a new reduced basis $(\rho'_i)_i$.*

(d) *As $\mathcal{O}_{\bar{K}}$-modules,*

$$\left\langle \pi^{-v(\rho_i)}\rho_i : 1 \leq i \leq n \right\rangle = \left\langle \pi^{-v(\rho)}\rho : \rho \in \omega R^\times \right\rangle.$$

Proof. (a) Choose a basis $(\rho_1, \ldots, \rho_n)$ such that the sum of the valuations $v(\rho_1) + \cdots + v(\rho_n)$ is maximal. This can be done because there are only finitely many possible valuations of primitive vectors in ωI. Sort the ρ_i in increasing order of valuation. We claim $(\rho_i)_i$ is reduced. Let $\rho = \sum_i c_i\rho_i$ be given. Let a be the minimal valuation $v(c_i\rho_i)$ of a term, and suppose that

$a < v(\rho)$. Then we have a linear dependency

$$\sum_{v(c_i\rho_i)=a} c_i\rho_i \equiv 0 \mod \pi^a \mathfrak{m}_{\bar{K}}.$$

Choose j such that $v(c_j\rho_j) = a$ and $v(c_j)$ is minimal. Then

$$\rho_j' = \sum_{v(c_i\rho_i)=a} \frac{c_i}{c_j}\rho_j$$

is an element of ωI whose valuation exceeds $v(\rho_j)$. Since the coefficient of ρ_j in ρ_j' is 1, replacing ρ_j by ρ_j' does not change the span ωI but increases the valuation sum $\sum_i c_i\rho_i$, contradicting the choice of basis $(\rho_i)_i$.

(b) Since $(\rho_i)_i$ and $(\rho_i')_i$ are bases for the same module ωI, such a $[c_{ij}] \in \mathrm{GL}_n(\mathcal{O}_K)$ certainly exists. Applying the reducedness property to each decomposition

$$\rho_i' = \sum_j c_{ij}\rho_j$$

yields a bound

$$v(c_{ij}) \geq v(\rho_i') - v(\rho_j).$$

Suppose that $v(\rho_k) < v(\rho_k')$ for some k. Then for $j \leq k \leq i$,

$$v(\rho_j) \leq v(\rho_k) < v(\rho_k') \leq v(\rho_i'),$$

so c_{ij} has positive valuation. Thus, when the matrix $[c_{ij}]$ is reduced modulo π, it has an $(n-k+1)\times k$ block of 0's, large enough to make the determinant vanish, which is a contradiction.

(c) By the preceding part, $v(\rho_k') = v(\rho_k)$. So the associated matrix $[c_{ij}]$ must satisfy

$$v(c_{ij}) \geq v(\rho_i') - v(\rho_j) = v(\rho_i) - v(\rho_j). \tag{124}$$

Conversely, if $[c_{ij}]$ is an invertible matrix satisfying this inequality, we get a new basis ρ_i' with $v(\rho_i') \geq v(\rho_i)$. Equality must hold, and now since $\sum_k v(\rho_k')$ achieves the maximal value, $(\rho_k')_k$ is reduced by the proof of part (a).

(d) The $\subseteq$ direction is obvious. For the $\supseteq$ direction, let $\rho \in \omega R^\times$ be given. Since $(\rho_i)_i$ is reduced,

$$\rho = \sum_i c_i \rho_i, \quad v(c_i \rho_i) \geq v(\rho),$$

so

$$\pi^{-v(\rho)}\rho = \sum_i \left(\pi^{v(\rho_i)-v(\rho)} c_i\right) \pi^{-v(\rho_i)} \rho_i,$$

and the parenthesized coefficients belong to $\mathcal{O}_{\bar{K}}$, as desired. ■

We can find reduced bases with added structure.

Definition 17.3. Fix an ordering $R = R_1 \times \cdots \times R_r$ of the field factors of R. For $\rho \in \omega R$, let k be the minimal index such that $v(\rho^{(k)}) = v(\rho)$. We say that ρ is $R^{(k)}$*-led,* and we define the *leader* of ρ to be the normalization

$$\mathrm{ldr}(\rho) = \left(\frac{\rho}{\pi^u \omega}\right)^{(i)},$$

where u is the unique integer for which $\mathrm{ldr}(\rho)$ is a primitive vector in $\mathcal{O}_R$. We say that a reduced basis $(\rho_i)_i$ is *well-led* if the leaders $\mathrm{ldr}(\rho_i)$ consist of a reduced basis for $\mathcal{O}_R^{(k)}$ for each k.

Proposition 17.4. *Every ωI, as above, admits a well-led basis.*

Proof. Consider the element

$$\eta_\varepsilon = (\pi^\varepsilon; \pi^{2\varepsilon}; \ldots; \pi^{r\varepsilon})$$

where ε is a positive rational number, small enough that if $a_1 < a_2$ are two valuations of elements in ωI, then $r\varepsilon < a_2 - a_1$. By Proposition 17.2(a), there is a reduced basis $\rho_1\eta_\varepsilon, \ldots, \rho_n\eta_\varepsilon$ for $\omega\eta_\varepsilon I$. Each basis element $\rho_i\eta_\varepsilon$ has some valuation $u + k\varepsilon$, $u \in \mathbb{Q}$, $k \in \{1, \ldots, r\}$, indicating that ρ_i is $R^{(k)}$-led. Since replacing ε by 0 preserves non-strict inequalities among valuations in $\eta_\varepsilon \omega I$, the ρ_i form a reduced basis for ωI, which we claim is well-led.

Given $\alpha \in \mathcal{O}_{R^{(k)}}$ primitive, decompose $\omega\alpha = \sum_j c_j \rho_j$ as an element of ωR. We have

$$v(c_j \rho_j \eta_\varepsilon) \geq v(\alpha \eta_\varepsilon) = v(\alpha) + i\varepsilon,$$

and for a nonempty subset of j, equality must hold and, in particular, ρ_j must be $R^{(k)}$-led. Let L_k be the set of indices j for which ρ_j is $R^{(k)}$-led, and let $B_k = \{\mathrm{ldr}(\rho_j) : j \in L_k\}$. Now we have

$$\omega\alpha = \sum_{j \in L_k} c_j \rho_j^{(k)} + \omega\alpha'$$

with each term of valuation at least $v(\alpha)$, and where $\alpha' \in \mathcal{O}_R$ with $v(\alpha') > v(\alpha)$. We can rewrite this as

$$\alpha = \sum_{j \in L_k} c'_j \,\mathrm{ldr}(\rho_j) + \alpha'$$

where $c'_j = c_j \pi^u \in \mathcal{O}_K$. We can iteratively decompose α' the same way, and as its valuation goes to infinity, we get a decomposition

$$\alpha = \sum_{j \in L_k} c''_j \,\mathrm{ldr}(\rho_j). \tag{125}$$

So B_k generates $\mathcal{O}_{R^{(k)}}$, and in particular, $|L_k| \geq [R : R^{(k)}]$. However,

$$\sum_k [R : R^{(k)}] = n = \sum_k |L_k|.$$

So equality holds and each B_k is a basis for $\mathcal{O}_R$. Since the decomposition (125) has every term of valuation at least $v(\alpha)$, and α was any primitive vector, B_k is in fact reduced. ■

It is evident that reduced indices take a limited number of values modulo 1. Indeed, we have the following:

Corollary 17.5. *If $I \subseteq R$ is a lattice, then the multiset of valuations $\{a_i\}_i = \{v(\rho_i)\}_i$ mod 1 of reduced basis elements for ωI depends only on R and ω, not on I. It consists of $f_{R_i/K}$ copies of*

$$v(\omega^{(R_i)}) + \frac{j}{e_{R_i/K}}, \quad j = 0, 1, \ldots, e_{R_i/K} - 1,$$

where R_i ranges over the field factors of $R = R_1 \times \cdots \times R_r$.

Proof. Taking a well-led basis and passing to the leaders, we reduce to the case that $R = R_i$ is a field. Then ω has equal valuations in all coordinates, and we may assume that $\omega = 1$. Let $\rho_i = \pi_R^{e_{R/K} a_i} \xi_i$, where the $\xi_i \in \mathcal{O}_R^\times$ differ only by a unit from the normalizations used before. For each congruence class of a_i modulo 1, note that if the set of corresponding ξ_i is linearly dependent modulo π_R, then one of the ρ_i could be increased by an $\mathcal{O}_K$-linear combination of the others to increase its valuation, contradicting the hypothesis that our basis is reduced. So the ξ_i corresponding to each congruence class of a_i modulo 1 are linearly independent, and in fact must form a basis for k_R over k_K in order for there to be the full number $e_{R/K} f_{R/K}$ of ξ_i. This establishes the claimed multiset. ∎

A reduced basis for ωI does not always remain reduced when we extend the ground field K. To study this, we make the following definition.

Definition 17.6. An *extender basis* for ωI is a basis $(\rho_1, \ldots, \rho_n)$ for $\omega I \otimes_{\mathcal{O}_K} \mathcal{O}_{\bar{K}}$ such that the vectors

$$\xi_i = \pi^{-v(\rho_i)} \rho_i$$

form an $\mathcal{O}_{\bar{K}}$-basis for $\mathcal{O}_{\bar{K}}^n$. The valuations $a_i = v(\rho_i)$ are called the *extender indices* of the basis, and the ξ_i are called the *extender vectors*.

If it consists of $\rho_i \in \omega I$, an extender basis is easily seen to be reduced. Fortunately, in the cases of tamely ramified resolvent, this always holds:

Proposition 17.7. *If R/K is tamely ramified, then any reduced basis of ωI is an extender basis.*

Proof. In view of Proposition 17.2(d), it is enough to show that

$$\mathcal{O}_{\bar{K}} \left\langle \pi^{-v(\rho)} \rho : \rho \in \omega R^\times \right\rangle = \mathcal{O}_{\bar{K}}^n.$$

We immediately reduce to the case that R is a field, and then we may assume $\omega = 1$. It suffices to

prove that, for some reduced basis $\rho_1, \ldots, \rho_n$ of R,

$$\det \left[\pi^{-v(\rho_i)} \rho_i^{(j)} \right]_{i,j} \sim 1.$$

But that follows from the familiar formula for the discriminant of a tamely ramified extension. ■

17.1 The extender basis of a cubic resolvent ring

Let C be a candidate resolvent for $\mathfrak{t}$-traced quartic rings, and let $C_\mathfrak{t}$ be the corresponding reduced resolvent, that is, the unique ring such that $C = \mathcal{O}_K + \mathfrak{t}^2 C_\mathfrak{t}$. First, look at the reduced basis of $C_\mathfrak{t} \subset R$ as a lattice; and look at its extender basis, a basis of $\bar{C}_\mathfrak{t} = C_\mathfrak{t} \otimes_{\mathcal{O}_K} \mathcal{O}_{\bar{K}}^3$. Because $1 \in C_\mathfrak{t}$ is an element of minimal valuation, there are not so many cases:

- If R is tamely ramified, then the reduced basis

$$C_\mathfrak{t} = \left\langle 1, \pi^{b_1}\theta_1, \pi^{b_2}\theta_2 \right\rangle, \quad b_1 \le b_2$$

  is also an extender basis. If R is unramified, the b_i are of course integers; if R is tamely ramified, then by Proposition 17.4, we have

$$\{b_1, b_2\} \equiv \left\{ \frac{1}{3}, \frac{2}{3} \right\} \mod \mathbb{Z}. \tag{126}$$

Because θ_1 is coprimitive to 1, at most one pair of its three coordinates can be congruent modulo $\mathfrak{m}_{\bar{K}}$. We let $\bar{s} = \bar{s}_C$, the *idempotency index* of C. Note that $\bar{s}$ is infinite only when two coordinates of θ_1 are exactly equal. Since the θ_i are determined only up to finite precision, we can, and will, assume that $\bar{s}$ is finite.

Lemma 17.8. *If finite, the value of $\bar{s}$ is constrained as follows:*

- *If R is unramified, then $\bar{s}$ is an integer. For simplicity we let $s = \bar{s}$.*
- *If R has splitting type 1^3 (residue characteristic 2), then $\bar{s} = 0$.*

Proof. In the tame splitting types this is immediate, knowing that $b_0 = 1$ is an extender vector for C of minimal valuation. ■

Notation 17.9. If $\bar{s} > 0$, then there is a unique coordinate of $\bar{K}^3 \cong R \otimes \bar{K}$ at which ω_C has positive valuation. This defines a splitting $R \cong K \times Q$ into a linear and a quadratic (possibly split) factor. We denote the three coordinates of R by (K), $(Q1)$, $(Q2)$, where (K) is the distinguished one; thus we can write an element $\xi \in \bar{K}^3$ as

$$\xi = \left(\xi^{(K)}; \xi^{(Q1)}; \xi^{(Q2)}\right) = \left(\xi^{(K)}; \xi^{(Q)}\right)$$

where $\xi^{(Q)} = \left(\xi^{(Q1)}; \xi^{(Q2)}\right) \in \bar{K}^2 = Q \otimes_K \bar{K}$.

A common tool in understanding nonmaximal orders is their duals under the trace pairing. Hence it is fitting that we should understand the element $\omega_C \in \mathcal{O}_{\bar{K}}^3$, unique up to scaling, that satisfies the relations

$$\operatorname{tr} \omega_C = \operatorname{tr}(\theta_1 \omega_C) = 0;$$

that is, $\bar{K}\langle\omega\rangle = \bar{K}\langle 1, \theta_1\rangle^{\perp}$ under the trace pairing.

One explicit choice of ω_C is as follows: If $\tilde{\theta} = \pi^{b_1}\theta_1 = (\tilde{\theta}^{(1)}, \tilde{\theta}^{(2)}, \tilde{\theta}^{(3)}) \in C$ is the second reduced basis vector, then

$$\hat{\omega}_C = \left(\tilde{\theta}^{(2)} - \tilde{\theta}^{(3)}\right)\left(\tilde{\theta}^{(3)} - \tilde{\theta}^{(1)}\right)\left(\tilde{\theta}^{(1)} - \tilde{\theta}^{(2)}\right)\left(\tilde{\theta}^{(2)} - \tilde{\theta}^{(3)}; \tilde{\theta}^{(3)} - \tilde{\theta}^{(1)}; \tilde{\theta}^{(1)} - \tilde{\theta}^{(2)}\right).$$

The symmetry ensures that $\hat{\omega}_C \in R$. Note that $N(\hat{\omega}_C) = (\operatorname{disc}\tilde{\theta})^2$ is a square in $K^{\times}$. Note also that

$$\operatorname{tr}(\omega_C) = \operatorname{tr}(\theta_1 \omega_C) = 0.$$

Then

$$\vec{v}(\hat{\omega}_C) = (4b_1 + 2\bar{s}, 4b_1 + \bar{s}, 4b_1 + \bar{s}).$$

Two other rescalings of $\hat{\omega}_C$, chosen for primitivity rather than the property of lying in R, will also

be used:

$$\omega_C = \pi^{-4b_1-\bar{s}}\omega_C, \qquad \vec{v}(\omega_C) = (\bar{s}, 0, 0)$$

$$\bar{\omega}_C = \pi^{-4b_1-2\bar{s}}\omega_C, \qquad \vec{v}(\bar{\omega}_C) = (0, -\bar{s}, -\bar{s}).$$

They have the properties that ω_C and $\bar{\omega}_C^{-1}$ are primitive (that is, have valuation 0) in $\mathcal{O}_{\bar{K}}^{\oplus 3}$.

18 Resolvent conditions

Let $C, C_{\mathfrak{t}} \subseteq R$ be a resolvent cubic ring and its corresponding reduced resolvent, whose reduced bases are related by

$$C = \left\langle 1, \pi^{b_1+2t}\theta_1, \pi^{b_2+2t}\theta_2 \right\rangle \quad \text{and} \quad \bar{C}_{\mathfrak{t}} = \left\langle 1, \pi^{b_1}\theta_1, \pi^{b_2}\theta_2 \right\rangle, \quad 0 \le b_1 \le b_2,$$

where $t = v_K(\mathfrak{t})$. Let L be a quartic algebra with resolvent R. As we noted in the proof of Theorem 6.13, an order $\mathcal{O} \subseteq L$ is completely determined by the lattice $I \subseteq R$ such that $\mathcal{O}/\mathcal{O}_K = \kappa(I)$, where

$$\begin{aligned} \kappa : K &\to \bar{K}^4 \\ \xi &\mapsto \left(\mathrm{tr}_{\bar{K}^3/K}\, \xi\omega\sqrt{\delta}\right)_\omega \end{aligned}$$

is the map in Theorem 5.4(c). For reasons that will become clear below, we take the reduced and extender bases, not of I itself, but of

$$\sqrt{\pi^{\bar{s}}\delta\omega_C}I.$$

Let the reduced basis be

$$\sqrt{\pi^{\bar{s}}\delta\omega_C} \cdot I = \left\langle \pi^{a_1}\xi_1, \pi^{a_2}\xi_2, \pi^{a_3}\xi_3 \right\rangle.$$

and let the extender basis be

$$\sqrt{\pi^{\bar{s}}\delta\omega_C} \cdot \bar{I} = \left\langle \pi^{\bar{a}_1}\bar{\xi}_1, \pi^{\bar{a}_2}\bar{\xi}_2, \pi^{\bar{a}_3}\bar{\xi}_3 \right\rangle.$$

Both δ and ω_C satisfy property $(*)$ in Definition 17.1, so the foregoing theory applies. (In this edition, since R will always be tamely ramified, the overbars can be ignored.) We will take

$$a_i' = a_i + 2b_1 \quad \text{and} \quad \bar{a}_i' = \bar{a}_i + 2b_1,$$

the reduced and extender indices of $\sqrt{\delta\hat{\omega}_C}I$. Then we can write the resolvent conditions as follows:

Lemma 18.1. *With respect to the above setup, a lattice I yields a ring $\mathcal{O}$ with a $\mathfrak{t}$-traced resolvent to $\mathcal{C}$ if and only if the following conditions hold:*

- *Discriminant (Θ) condition:*

$$\bar{a}_1 + \bar{a}_2 + \bar{a}_3 = \bar{b}_1 + \bar{b}_2 + 2\bar{s} + 4t - 4e \tag{127}$$

- *Resolvent (Φ) conditions for $\bar{\theta}_2$-coefficients:*

$$\mathcal{M}_{ij}: \quad \operatorname{tr}(\bar{\xi}_i\bar{\xi}_j) \equiv 0 \mod \pi^{\bar{m}_{ij}}$$

where

$$\bar{m}_{ij} = \begin{cases} \bar{b}_2 + 2t - 2e - 2\bar{a}_i + \bar{s}, & i = j \\ \bar{b}_2 + 3t - 3e - \bar{a}_i - \bar{a}_j + \bar{s}, & i \neq j. \end{cases}$$

- *Resolvent (Φ) conditions for $\bar{\theta}_1$-coefficients:*

$$\mathcal{N}_{ij}: \quad \textit{All coordinates of } \ \bar{\omega}_C^{-1} \cdot \bar{\xi}_i\bar{\xi}_j \ \textit{ are congruent } \mod \pi^{\bar{n}_{ij}},$$

where

$$\bar{n}_{ij} = \begin{cases} \bar{b}_1 + 2t - 2e - 2\bar{a}_i + 2\bar{s}, & i = j \\ \bar{b}_1 + 3t - 3e - \bar{a}_i - \bar{a}_j + 2\bar{s}, & i \neq j. \end{cases}$$

Proof. The conditions that C is a $\mathfrak{t}$-traced resolvent for $\mathcal{O}$ are that all coefficients in the coordinate

representations of Θ, Θ^{-1}, and Φ have nonnegative valuation. In particular, it is equivalent to study when $\bar{C} = C \otimes_{\mathcal{O}_K} \mathcal{O}_{\bar{K}}$ is a resolvent of $\bar{\mathcal{O}} = \mathcal{O} \otimes_{\mathcal{O}_K} \mathcal{O}_{\bar{K}}$.

We have

$$\bar{C} = \left\langle 1, \pi^{2t+\bar{b}_1}\bar{\theta}_1, \pi^{2t+\bar{b}_2}\bar{\theta}_2 \right\rangle,$$

so

$$\Lambda^2(\bar{C}/\mathcal{O}_{\bar{K}}) = \left\langle \pi^{4t+\bar{b}_1+\bar{b}_2}\bar{\theta}_1 \wedge \bar{\theta}_2 \right\rangle = \pi^{4t+\bar{b}_1+\bar{b}_2}\Lambda^2(\mathcal{O}_{\bar{K}}^3/\mathcal{O}_{\bar{K}})$$

and, by the formula for Θ in Proposition 6.14,

$$\Theta(\Lambda^2(\bar{C}/\mathcal{O}_{\bar{K}})) = \frac{1}{16\sqrt{N(\delta)}}\pi^{4t+\bar{b}_1+\bar{b}_2} \cdot \kappa(\mathcal{O}_{\bar{K}}^3)$$

Meanwhile,

$$\bar{I} = \frac{1}{\sqrt{\pi^{\bar{s}}\delta\omega_C}} \left\langle \pi^{\bar{a}_1}\bar{\xi}_1, \pi^{\bar{a}_2}\bar{\xi}_2, \pi^{\bar{a}_3}\bar{\xi}_3 \right\rangle \tag{128}$$

so

$$\begin{aligned}\Lambda^3\bar{I} &= \frac{1}{\sqrt{\pi^{3\bar{s}}N(\delta\omega_C)}}\pi^{\bar{a}_1+\bar{a}_2+\bar{a}_3} \left\langle \bar{\xi}_1 \wedge \bar{\xi}_2 \wedge \bar{\xi}_3 \right\rangle \\ &= \frac{1}{\sqrt{\pi^{3\bar{s}}N(\delta\omega_C)}}\pi^{\bar{a}_1+\bar{a}_2+\bar{a}_3}\Lambda^3(\mathcal{O}_{\bar{K}}^4/\mathcal{O}_K).\end{aligned}$$

So the condition for Θ to define an isomorphism between $\Lambda^2(\bar{C}/\mathcal{O}_{\bar{K}})$ and $\Lambda^3(\bar{\mathcal{O}}/\mathcal{O}_{\bar{K}})$ is that

$$4t + \bar{b}_1 + \bar{b}_2 - 4e - \frac{1}{2}v(N(\delta)) = \bar{a}_1 + \bar{a}_2 + \bar{a}_3 - \frac{3}{2}\bar{s} - \frac{1}{2}v(N(\delta\omega_C)),$$

or, since $v(N(\omega_C)) = \bar{s}$,

$$4t - 4e + \bar{b}_1 + \bar{b}_2 + 2\bar{s} = \bar{a}_1 + \bar{a}_2 + \bar{a}_3,$$

as desired.

Likewise, we use the formula

$$\Phi(\kappa(\alpha)) = 4\delta\alpha^2$$

from Proposition 6.14 to transform the Φ-condition to the following:

(i) For every $\xi \in \bar{I}$, we have $4\delta\xi^2 \in \bar{C} + \bar{K}$

(ii) For every $\xi, \eta \in \bar{I}$, we have $8\pi^{-t}\delta\xi\eta \in \bar{C} + \bar{K}$.

In terms of the basis (128) for $\bar{I}$, this is to say that the diagonal entries of the matrix representing Φ belong to $\bar{C} + \bar{K}$ and the off-diagonal entries to $\mathfrak{t}\bar{C} + \bar{K}$. Hence it suffices to consider (i) for ξ a basis element and (ii) for ξ, η distinct basis elements.

To test whether an $\alpha \in \bar{K}^3$ lies in

$$\bar{C} = \left\langle 1, \pi^{2t+\bar{b}_1}\bar{\theta}_1, \pi^{2t+\bar{b}_2}\bar{\theta}_2 \right\rangle,$$

we can pair it with a basis of the dual lattice $\bar{C}^\vee$ with respect to the trace pairing. Let $(\lambda_0, \lambda_1, \lambda_2)$ be the dual basis to $(\bar{\theta}_0, \bar{\theta}_1, \bar{\theta}_2)$ (that is, $\mathrm{tr}(\bar{\theta}_i\lambda_j) = \mathbf{1}_{i=j}$). Then (λ_1, λ_2) is a basis for $(\mathcal{O}_K^3)^{\mathrm{tr}=0}$, and we have already met λ_2: it is ω_C, up to a unit. Hence

$$\begin{aligned}\bar{C}^\vee &= \left\langle \lambda_0, \pi^{-2t-\bar{b}_1}\lambda_1, \pi^{-2t-\bar{b}_2}\lambda_2 \right\rangle \\ &= \langle\lambda_0\rangle + \pi^{-2t-\bar{b}_1}(\mathcal{O}_{\bar{K}}^3)^{\mathrm{tr}=0} + \pi^{-2t-\bar{b}_2}\langle\omega_C\rangle\end{aligned}$$

We actually wish to test not whether $\alpha \in \bar{C}$, but the weaker condition $\alpha \in \bar{C} + \bar{K}$, so (due to the natural duality between $\bar{C}/\mathcal{O}_{\bar{K}}$ and $(\bar{C}^\vee)^{\mathrm{tr}=0}$) we pair only with elements of

$$(\bar{C}^\vee)^{\mathrm{tr}=0} = \pi^{-2t-\bar{b}_1}(\mathcal{O}_{\bar{K}}^3)^{\mathrm{tr}=0} + \pi^{-2t-\bar{b}_2}\langle\hat{\omega}_C\rangle.$$

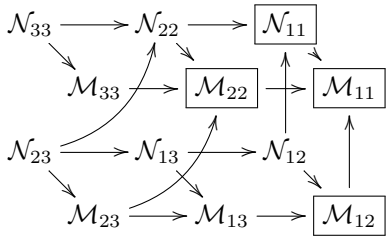
Hence $\alpha \in \bar{C} + \bar{K}$ if and only if

- $\pi^{-2t-\bar{b}_2}\,\mathrm{tr}(\omega_C\alpha)$ is integral, and
- $\pi^{-2t-\bar{b}_1}\,\mathrm{tr}(\alpha\kappa)$ is integral for $\kappa \in \{(1;-1;0),(0;1;-1)\}$; that is, all coordinates of α are congruent modulo $\pi^{2t+\bar{b}_1}$.

This is the origin of the $\mathcal{M}$- and $\mathcal{N}$-conditions respectively. Applying this to the values $\alpha = 4\delta\xi^2, 8\pi^{-t}\delta\xi\eta$ derived from the basis above yields the desired form of all the Φ-conditions. ■

We say that the condition $\mathcal{M}_{ij}$ or $\mathcal{N}_{ij}$ is *active* if its corresponding modulus $\bar{m}_{ij}$ or $\bar{n}_{ij}$ is positive. An inactive condition is automatically satisfied (noting that $\bar{\omega}_C^{-1}$ has nonnegative valuations).

Because the a's and b's have been sorted in increasing order, and because $0 \leq t \leq e$, we have the following implications among the activity of the $\mathcal{M}_{ij}$ and $\mathcal{N}_{ij}$:



The next lemma limits our concern to the four boxed conditions:

Lemma 18.2. (*a*) *Suppose that the $\bar{a}_i$ and $\bar{\xi}_i$ come from the extender decomposition of a quartic ring and a resolvent thereof. Then:*

- *No conditions are active except $\mathcal{M}_{11}$, $\mathcal{M}_{12}$, $\mathcal{M}_{22}$, $\mathcal{N}_{11}$, and $\mathcal{N}_{12}$.*
- *$\mathcal{M}_{12}$ and $\mathcal{M}_{22}$ are not both active.*
- *$\mathcal{N}_{12}$ is* very weakly active, *that is, $\bar{n}_{12} \leq \bar{s}/2$.*

(*b*) *Suppose that the $\bar{a}_i$ and $\bar{\xi}_i$ come from the extender decomposition of <u>some</u> lattice $I \subseteq R$. Suppose that the inactivity restrictions from part (a) hold and that conditions $\mathcal{M}_{11}$, $\mathcal{M}_{12}$, $\mathcal{M}_{22}$, and $\mathcal{N}_{11}$ are satisfied. Then $\mathcal{N}_{12}$ is satisfied, and the $\bar{a}_i$ and $\bar{\xi}_i$ actually come from a quartic ring. That is, "$\mathcal{N}_{12}$ is automatic if it is very weakly active."*

Proof. (a) Suppose that the $\bar{a}_i$ and $\bar{\xi}_i$ come from a quartic ring.

If $\mathcal{M}_{13}$ is active, so are $\mathcal{M}_{12}$ and $\mathcal{M}_{11}$. Since the $\bar{\xi}_i$ are supposed to form an $\mathcal{O}_{\bar{K}}$-basis of $\mathcal{O}_{\bar{K}}^3$, we obtain for all $\bar{\xi} \in \mathcal{O}_{\bar{K}}^3$,

$$\mathrm{tr}(\bar{\xi}_1\bar{\xi}) \equiv 0 \mod \mathfrak{m}_{\bar{K}}.$$

Since $\bar{\xi}_1$ is primitive, this is a contradiction.

If $\mathcal{M}_{12}$ and $\mathcal{M}_{22}$ are active, then so is $\mathcal{M}_{11}$. We have a 2-dimensional subspace $V = \langle \bar{\xi}_1, \bar{\xi}_2 \rangle$ of the 3-dimensional space $k_{\bar{K}}^3$ that is isotropic for the trace pairing. But the trace pairing is nondegenerate, so this is a contradiction.

If $\mathcal{M}_{33}$ is active, so are $\mathcal{M}_{22}$ and $\mathcal{M}_{11}$. If $\operatorname{char} k_K \neq 2$, then $t = e = 0$ so $\mathcal{M}_{12}$ is also active, and we have a contradiction as above. If $\operatorname{char} k_K = 2$, we use that squaring is a linear operation mod 2 to obtain that for all $\bar{\xi} \in \mathcal{O}_{\bar{K}}^3$,

$$\operatorname{tr}(\bar{\xi}^2) \equiv 0 \mod \mathfrak{m}_{\bar{K}},$$

which is a contradiction.

If $\mathcal{N}_{22}$ is active, note that $\operatorname{char} k_K = 2$ since $\mathcal{M}_{22}$ is active. There are two cases. If $\bar{s} = 0$, then $\bar{\omega}_C^{-1}$ is a unit, so the condition

$$\mathcal{N}_{ii}\colon \quad \text{All coordinates of} \quad \bar{\omega}_C^{-1} \cdot \bar{\xi}_i^2 \quad \text{are congruent} \mod \pi^{\bar{n}_{ii}}$$

determines $\bar{\xi}_i^2 \mod \mathfrak{m}_{\bar{K}}$ up to scaling. But since we are in characteristic 2, square roots are unique, and $\bar{\xi}_1$ and $\bar{\xi}_2$ are scalar multiples mod $\mathfrak{m}_{\bar{K}}$, a contradiction. Now assume $\bar{s} > 0$, so $\bar{\omega}_C^{-1} \equiv (u; 0; 0)$ for some unit $u \in \mathcal{O}_{\bar{K}}^\times$. Now $\mathcal{N}_{ii}$ gives $\bar{\xi}_i^{(K)} \equiv 0 \mod \mathfrak{m}_{\bar{K}}$. But now $\mathcal{M}_{ii}$ gives that $\bar{\xi}_i$ is a unit multiple of $(0; 1; 1)$ modulo $\mathfrak{m}_{\bar{K}}$, a contradiction.

Finally, assume that $\mathcal{N}_{12}$ is active and not very weakly active: that is, $\bar{n}_{12} > \bar{s}/2$. Note that $\bar{n}_{11} > \bar{s}$ since otherwise $\mathcal{N}_{22}$ would be active. If $\bar{s} = 0$, then $\mathcal{N}_{11}$ implies that $\bar{\xi}_1^2 \equiv \omega_C \mod \mathfrak{m}_C$, up to scaling, and then $\mathcal{N}_{12}$ implies that $\bar{\xi}_1 \bar{\xi}_2 \equiv \omega_C \mod \mathfrak{m}_C$, up to scaling. Since ω_C is a unit, this is a contradiction. So assume $\bar{s} > 0$. Note that ω_C is a unit multiple of $(0; 1; -1)$ modulo $\pi^{\bar{s}}$ and that $\bar{\omega}_C^{-1}$ is a unit multiple of $(1; 0; 0)$ modulo $\pi^{\bar{s}}$. Now $\mathcal{N}_{11}$ implies that

$$\bar{\xi}_1^2 \equiv \omega_C \mod \mathfrak{m}_{\bar{K}} \omega_C = \mathfrak{m}_{\bar{K}}(\pi^{\bar{s}}; 1; 1).$$

So $v_K(\bar{\xi}_1^{(K)}) = \bar{s}/2$ exactly (recalling the notion of $\xi^{(K)}$ from Notation 17.9). If $v_K(\bar{\xi}_2^{(K)}) > 0$ also, we get $\bar{\xi}_1 \equiv \bar{\xi}_2 \mod \mathfrak{m}_{\bar{K}}$ by the same argument as when N_{22} is active. So $\bar{\xi}_2^{(K)}$ is a unit, and the $\mathcal{N}_{12}$ condition

$$\mathcal{N}_{12}: \quad \text{All coordinates of} \quad \bar{\omega}_C^{-1} \cdot \bar{\xi}_1 \bar{\xi}_2 \quad \text{are congruent} \mod \pi^{\bar{n}_{12}}$$

is unsatisfied, because the K-coordinate has valuation $\bar{s}/2$ and the others have higher valuation.

(b) Note that $\bar{n}_{12} \leq \frac{1}{2}\bar{n}_{11}$ because otherwise $\mathcal{N}_{22}$ would be active. We have $\bar{\omega}_C^{-1}$ a unit multiple of $(1;0;0)$ modulo $\pi^{2\bar{n}_{12}}$, so $\mathcal{N}_{11}$ implies that $\pi^{2\bar{n}_{12}} | (\bar{\xi}_1^2)^{(K)}$, that is, $\pi^{\bar{n}_{12}} | \bar{\xi}_1^{(K)}$. Now $\pi^{\bar{n}_{12}} \mid \bar{\omega}_C^{-1}\bar{\xi}_1$, so $\mathcal{N}_{12}$ is satisfied. ■

Based on this, we will count quartic rings with fixed resolvent. Since a lot will happen with various things being fixed and others varying, it is worthwhile to lay down the following:

Conventions 18.3. We fix variables in the following order:

- First, we fix the *resolvent data,* which comprise
  - a resolvent $C \subseteq R$;
  - an extender decomposition $C = \left\langle 1, \pi^{\bar{b}_1}\bar{\theta}_1, \pi^{\bar{b}_2}\bar{\theta}_2 \right\rangle$, which fixes $\hat{\omega}_C$ and $\bar{s}$. We can, and do, assume that $\bar{s}$ is finite;
  - a tracedness parameter t, $0 \leq t \leq e$, which defines a reduced resolvent $C_{\mathfrak{t}}$.
- Then we fix the *discrete data* of a quartic ring, which comprises
  - a choice of *coarse coset* $[\delta] \in H^1/\mathcal{L}_0$. There are $|H^0|$ cosets $\delta_0\mathcal{L}_0$. Then $\delta = \delta_0\tau$, where $\tau \in \mathcal{O}_R^\times$ can vary;
  - its extender indices $\bar{a}_i$, which are constrained by the integrality needed for a sublattice of $\sqrt{\delta\hat{\omega}_C}R$ and the inactivity inequalities of Lemma 18.2.
- Then we choose δ and $\bar{\xi}_1$, which are constrained by the $\mathcal{M}_{11}$ and $\mathcal{N}_{11}$ conditions.

- Then we choose $\bar{\xi}_2$, which is constrained by its coprimitivity with $\bar{\xi}_1$ and by the $\mathcal{M}_{12}$ and $\mathcal{M}_{22}$ conditions.

- Lastly, we choose $\bar{\xi}_3$, which is constrained by its coprimitivity with $\bar{\xi}_1$ and $\bar{\xi}_2$.

Whenever we speak about possibilities for any of the items on this list, it will be implicitly assumed (if not stated) that all the previous items have been fixed in conformity with their respective restrictions.

Since $\bar{\xi}_1 \in \pi^{-\bar{a}'_1}\sqrt{\delta\hat{\omega}_C}R$, conditions $\mathcal{M}_{11}$ and $\mathcal{N}_{11}$ can be viewed in another way, which will be simpler for some purposes:

Lemma 18.4. *A $\bar{\xi}_1 \in \sqrt{\delta\hat{\omega}_C}R \cap \mathcal{O}_{\bar{K}}^3$ satisfies the $\mathcal{M}_{11}$ and $\mathcal{N}_{11}$ resolvent conditions if and only if the quotient*

$$\beta = \frac{\bar{\xi}_1^2}{\omega_C} \in \pi^{-2\bar{a}'_1+\bar{s}}R$$

is a linear combination of the reduced basis vectors of C of the form

$$\beta = x + y\pi^{n_{11}-\bar{s}}\bar{\theta}_1 + z\pi^{m_{11}}\bar{\theta}_2, \quad x \in \pi^{-2\bar{a}_1+\bar{s}}K, \quad y, z \in \mathcal{O}_K.$$

Proof. Since $\frac{\pi^{\bar{a}'_1}\bar{\xi}_1}{\sqrt{\delta\hat{\omega}_C}}$ is the first basis element for $\bar{I}$, the $\mathcal{M}_{11}$ and $\mathcal{N}_{11}$ conditions are equivalent to

$$\bar{K} + \bar{C} \ni 4\delta\left(\frac{\pi^{\bar{a}'_1}\bar{\xi}_1}{\sqrt{\delta\hat{\omega}_C}}\right)^2 = \frac{4\pi^{2\bar{a}'_1}\bar{\xi}_1^2}{\omega_C} = 4\pi^{2\bar{a}_1+4\bar{b}_1-4\bar{b}_1-\bar{s}}\beta = 4\pi^{2\bar{a}_1-\bar{s}}\beta,$$

that is,

$$\beta \in \bar{K} + \pi^{\bar{s}-2\bar{a}_1-2e}\bar{C} = \bar{K} + \pi^{n_{11}-\bar{s}}\mathcal{O}_{\bar{K}}\bar{\theta}_1 + \pi^{m_{11}}\mathcal{O}_{\bar{K}}\bar{\theta}_2.$$

Since $(1, \pi^{\bar{b}_1}\bar{\theta}_1, \pi^{\bar{b}_2}\bar{\theta}_2)$ form an $\mathcal{O}_K$-basis for C, we can always find $x \in \pi^{\bar{s}-2\bar{a}_1}K$ and $y, z \in K$ such that

$$\beta = x + y\pi^{n_{11}-\bar{s}}\bar{\theta}_1 + z\pi^{m_{11}}\bar{\theta}_2.$$

Then the resolvent conditions simplify to $y, z \in \mathcal{O}_K$. ∎

18.1 Transformation, and ring volumes in the white zone

We will proceed to compute the volumes of the solution sets in which the reduced vectors ξ_i lie. (We use reduced vectors ξ_i, not extender vectors $\bar{\xi}_i$, because the latter do not lie in a controllable $\mathcal{O}_K$-lattice.) For simplicity, we will transform everything to R itself, which we normalize so that $\mathcal{O}_R$ has volume 1, and to its projectivization $\mathbb{P}(\mathcal{O}_R)$, to which we give a volume of $1 + 1/q + 1/q^2$, so that a distinguished affine open has volume 1.

The simplest way to do this is as follows.

Lemma 18.5. *Fix the discrete data. In particular, $\delta = \tau\delta_0$ lies in a fixed coarse coset. There is a $\gamma = \gamma_i \in \bar{K}^3$ with the properties that, letting*

$$\gamma_i = \frac{\gamma_{i,0}}{\sqrt{\tau}},$$

we have that $\xi_i' = \gamma_i^{-1}\xi_i$ is a primitive vector in $\mathcal{O}_R$.

Proof. Note that ξ_i must lie in

$$J = \pi^{-a_i'}\sqrt{\delta\hat{\omega}_C}R \cap \mathcal{O}_{\bar{K}}^3 = \sqrt{\tau}J_0, \tag{129}$$

where

$$J_0 = \pi^{-a_i'}\sqrt{\delta_0\hat{\omega}_C}R \cap \mathcal{O}_{\bar{K}}^3$$

is an $\mathcal{O}_R$-lattice of dimension 1. As $\mathcal{O}_R$ is a principal ideal ring (it's a product of DVR's), we obtain that $J_0 = \gamma_i\mathcal{O}_R$ for some γ_i, clearly not a zero-divisor. Since $\xi_i \in J \setminus \pi J$, we get $\xi_i' = \gamma_i^{-1}\xi_i \in \mathcal{O}_R \setminus \pi\mathcal{O}_R$, as desired. ∎

The valuations of γ may be computed by observing the smallest nonnegative valuation of an element of J at each place. The ξ_i form a set of reduced vectors for a sublattice of $\sqrt{\delta\hat{\omega}_C}I$ if and only if the ξ_i' lie in certain explicit subsets of $\mathcal{O}_R$, computed below.

Unramified.

- If $[\delta\hat{\omega}_C] \in \mathcal{L}_0$, then all a_i are integers, and $\gamma_i = \gamma$ is a unit. The three ξ' must form a basis of $\mathcal{O}_R$. If they are found successively, their ring volumes are respectively $\boxed{1 + 1/q + 1/q^2}$, $\boxed{1 + 1/q}$, and $\boxed{1}$.

- If $[\delta\hat{\omega}_C] \in (1; \pi; \pi)\mathcal{L}_0$, then there is one $a_{j_0} \in \mathbb{Z}$; there $\gamma_{j_0} \sim (1; \sqrt{\pi}; \sqrt{\pi})$, and

$$\xi'_{j_0} \in \mathcal{O}_K^\times \times \mathcal{O}_Q,$$

  a subset whose projectivization has volume $\boxed{1}$. Meanwhile, two a_{j_1}, a_{j_2} lie in $\mathbb{Z} + 1/2$; there $\gamma_{j_k} \sim (\sqrt{\pi}; 1; 1)$, and

$$\xi'_{j_k} \in \mathcal{O}_K \times \mathcal{O}_Q$$

  with their $\mathcal{O}_Q$-coordinates forming a basis of $\mathcal{O}_Q$; thus ξ'_{j_1} has volume $\boxed{1 + 1/q}$ and ξ'_{j_2} has volume $\boxed{1}$.

Splitting type 1^3.

- Here $[\delta\hat{\omega}_C] \in \mathcal{L}_0$. The a_i fill out the classes in $\frac{1}{3}\mathbb{Z}/\mathbb{Z}$, but all γ_i are units and all ξ'_i lie in $\mathcal{O}_R^\times$, a subset whose projectivization has volume $\boxed{1}$.

Lemma 18.6. *In the white (i.e. free) zone where no $\mathcal{M}_{ij}$ or $\mathcal{N}_{ij}$ is active, we take all γ_i as in Lemma 18.5. The ring volume of triples (ξ'_1, ξ'_2, ξ'_3) is given in terms of the discrete data as follows:*

1. *If R is unramified and $[\delta\hat{\omega}_C] \in \mathcal{L}_0$, the ring volume is $(1 + 1/q + 1/q^2)(1 + 1/q)$.*

2. *If R is unramified and $[\delta\hat{\omega}_C] \notin \mathcal{L}_0$, the ring volume is $1 + 1/q$.*

3. *If R is totally ramified, the ring volume is 1.*

18.2 From ring volumes to ring counts

Lemma 18.7. *Let $\mathcal{O}$ be a quartic ring. The set V of triples (ξ_1', ξ_2', ξ_3') in $\mathbb{P}^2(\mathcal{O}_R)^3$ whose associated ring is $\mathcal{O}$ has a volume determined by the discrete data of $\mathcal{O}$ alone. It is given by*

$$\mu(V) = q^{-\lceil a_2 - a_1 \rceil - \lceil a_3 - a_2 \rceil - \lceil a_3 - a_1 \rceil + \frac{3d_0^{\text{tame}}}{2} + v_K\left(N(\gamma_1\gamma_2\gamma_3)\right)} \cdot c,$$

where

$$d_0^{\text{tame}} = \sum_{R_i} \left(e_{R_i/K} - 1\right)$$

is the standard lower bound for the discriminant valuation, attained for tame extensions, and

$$c = \begin{cases} 1 & \text{if } a_1 = a_2 = a_3 \\ \left(1 + \frac{1}{q} + \frac{1}{q^2}\right) & \text{if } a_1 = a_2 < a_3 \text{ or } a_1 < a_2 = a_3 \\ \left(1 + \frac{1}{q}\right)\left(1 + \frac{1}{q} + \frac{1}{q^2}\right) & \text{if } a_1 < a_2 < a_3. \end{cases}$$

Proof. We have

$$\xi_i, \gamma_i \in \pi^{-a_i'}\sqrt{\delta\hat{\omega}_C}R, \quad \xi_i' \in \mathcal{O}_R.$$

To determine whether $(\Xi_1', \Xi_2', \Xi_3') \in V$, there are two conditions: firstly, the generators $\pi^{a_i}\Xi_1$, where $\Xi_i = \Xi_i'\gamma_i$ are the associated reduced basis vectors, belong to the correct lattice

$$\pi^{a_i}\Xi_i \in \sqrt{\pi^{\bar{s}}\delta\omega_C}I = \langle \pi^{a_1}\xi_1, \pi^{a_2}\xi_2, \pi^{a_3}\xi_3 \rangle ; \tag{130}$$

and secondly, they generate the whole of $\sqrt{\pi^{\bar{s}}\delta\omega_C}I$. Since the $\pi^{a_i}\xi_i$ form a K-basis for $\sqrt{\delta\hat{\omega}_C}R$, we can write

$$\Xi_i = \sum_{j=1}^{3} \pi^{a_j - a_i} c_{ij} \xi_i \tag{131}$$

for some coefficients $c_{ij} \in K$. Condition (130) is then equivalent to

$$v\left(c_{ij}\right) \geq \max\{a_i - a_j, 0\},$$

while the condition that the $\pi^{a_i}\Xi_i$ generate the whole of $\sqrt{\pi^{s'}\delta\omega_C}I$ is equivalent to the change of basis being invertible:

$$v\left(\det\left[c_{ij}\right]\right) = 0.$$

Thus we have parametrized V by the group

$$\Gamma = \left\{[c_{ij}] \in \mathrm{GL}_3(\mathcal{O}_K) : v\left(c_{ij}\right) \geq a_i - a_j\right\}.$$

More precisely, V is in continuous bijection with the cosets $T\backslash\Gamma$, where $T = \left(\mathcal{O}_K^\times\right)^3$ is the subgroup of diagonal matrices, because the $\Xi_i \in \mathbb{P}(\mathcal{O}_R)$ are defined only up to scaling.

Without the invertibility condition, the volume of matrices in $\mathrm{Mat}_3(\mathcal{O}_K)$ satisfying the valuation restrictions defining Γ is

$$q^{-\sum_{1\leq i,j\leq 3}\max\{0,\lceil a_i - a_j\rceil\}} = q^{-\lceil a_2 - a_1\rceil - \lceil a_3 - a_2\rceil - \lceil a_3 - a_1\rceil}.$$

The invertibility depends only on the c_{ij} modulo π, and the fraction of matrices over k_K of the shapes

$$\begin{bmatrix} * & * & * \\ * & * & * \\ * & * & * \end{bmatrix}, \begin{bmatrix} * & * & * \\ 0 & * & * \\ 0 & * & * \end{bmatrix}, \quad \text{and} \quad \begin{bmatrix} * & * & * \\ 0 & * & * \\ 0 & 0 & * \end{bmatrix}$$

that are nondegenerate is seen to be

$$\left(1 - \frac{1}{q}\right)^3 \cdot c,$$

accounting for the three cases in the definition of c. Projectivizing, $T\backslash\Gamma$ is a subset of $(\mathbb{P}^3\mathcal{O}_K)^3$ of

volume

$$q^{-\lceil a_2 - a_1 \rceil - \lceil a_3 - a_2 \rceil - \lceil a_3 - a_1 \rceil} \cdot c.$$

It remains to compute how the volume transforms under the bijection $\Psi : T\backslash\Gamma \cong V$ that we have constructed. This map is K-linear and is a product of the three maps

$$\begin{aligned} \Psi_i : K \times K \times K &\to R \\ (c_{i1}, c_{i2}, c_{i3}) &\mapsto \sum_{j=1}^{3} c_{ij} \pi^{a_j - a_i} \frac{\gamma_j}{\gamma_i} \xi'_j. \end{aligned}$$

On the domain where it sends primitive vectors to primitive vectors, Ψ_i scales volumes by q^{-n_i}, where n_i is the determinant valuation, i.e.

$$\Psi_i \left(\Lambda^3 \mathcal{O}_K^3 \right) = \pi^{n_i} \Lambda^3 \mathcal{O}_R. \tag{132}$$

Extending scalars to $\mathcal{O}_{\bar{K}}$, the left side of (132) becomes

$$\begin{aligned} \Psi_i \left(\Lambda^3 \mathcal{O}_{\bar{K}}^3 \right) &= \prod_j \pi^{a_j - a_i} \bigwedge_j \frac{\gamma_j \xi'_j}{\gamma_i} \\ &= \frac{\pi^{\sum_j a_j - 3a_i}}{N(\gamma_i)} \bigwedge_j \xi_j \end{aligned}$$

When R is tamely ramified, the wedge product of the ξ_j generates the whole of $\Lambda^3 \mathcal{O}_{\bar{K}}$, because the ξ_j are an extender basis. Indeed, in all cases, if we let

$$d_0^{\text{wild}} = d_0 - d_0^{\text{tame}},$$

then

$$\langle \xi_1 \wedge \xi_2 \wedge \xi_3 \rangle = \pi^{d_0^{\text{wild}}/2} \Lambda^3 \mathcal{O}_{\bar{K}}^3.$$

Accordingly, we get

$$\Psi_i\left(\Lambda^3\mathcal{O}_{\bar{K}}\right) = \frac{\pi^{\sum_j a_j - 3a_i + \frac{d_0^{\text{wild}}}{2}}}{N(\gamma_i)}\Lambda^3\mathcal{O}_{\bar{K}}.$$

Meanwhile, the right side of (132) is

$$\pi^{n_i}\Lambda^3\left(\mathcal{O}_R \otimes_{\mathcal{O}_K} \mathcal{O}_{\bar{K}}\right) = \pi^{n_i + \frac{d_0}{2}}\Lambda^3\mathcal{O}_{\bar{K}}.$$

Hence

$$n_i = \sum_j a_j - 3a_i - v_K\left(N(\gamma_i)\right) - \frac{d_0^{\text{tame}}}{2}$$

so

$$\sum_i n_i = -v_K\left(N(\gamma_1\gamma_2\gamma_3)\right) - \frac{3d_0^{\text{tame}}}{2}$$

and

$$\mu(V) = \mu\left(T\backslash\Gamma\right)\cdot q^{-\sum_i n_i} = q^{-\lceil a_2 - a_1\rceil - \lceil a_3 - a_2\rceil - \lceil a_3 - a_1\rceil + \frac{3d_0^{\text{tame}}}{2} + v_K\left(N(\gamma_1\gamma_2\gamma_3)\right)}\cdot c,$$

as desired. ■

Consequently, we can compute the number of rings with any given discrete data by finding the volume of permissible (ξ_1', ξ_2', ξ_3'), and dividing by $\mu(V)$. We carry out the computation of this volume in the succeeding sections. Observe that $\mu(V)$ equals $q^{2a_1 - 2a_3}$ times a correction that depends only on the a_i mod 1 and whether any a_i are equal. This will simplify the entry of the ring volumes into Sage at the end of the proof.

19 The conic over $\mathcal{O}_K$

For each $\alpha \in R^\times$, the equation

$$\text{tr}(\alpha\xi^2) = 0$$

defines a conic on the projectivization of R. Its determinant is $D_0 N(\alpha)$, up to squares of units, with respect to any $\mathcal{O}_K$-basis of $\mathcal{O}_R$, where D_0 is the discriminant of $\mathcal{O}_R$. As we will find, it is preferable to transform the conic so that its discriminant has as low valuation as possible:

Definition 19.1. Let K be a local field, $\operatorname{char} K \neq 2$. By a *conic* over $\mathcal{O}_K$ we mean a lattice V of dimension 3 over $\mathcal{O}_K$ equipped with an integral bilinear form $\mathcal{C}$, or equivalently an integer-matrix quadratic form $\mathcal{C} : V \to \mathcal{O}_K$, up to scaling by $\mathcal{O}_K^\times$. We say that $\mathcal{C}$ is

- *unimodular* if $\det \mathcal{C} \sim 1$ (note that $\det \mathcal{C}$ is uniquely defined up to squares of units);
- *tiny* if $\det \mathcal{C} \sim \pi$ and there exists a $v \in V$ such that $\mathcal{C}(v)$ is a unit;
- *relevant* if it is either unimodular or tiny.

Remark 19.2. Between changing basis and rescaling the whole form $\mathcal{C}$, we can scale $\det \mathcal{C}$ by any unit: hence we will sometimes assume that $\det \mathcal{C}$ is exactly 1 or π.

Let $\diamondsuit$ be a generator of the different ideal $\mathfrak{d}_{R/K}$. For instance, we can take

$$\diamondsuit = \begin{cases} 1 & R \text{ unramified} \\ \pi_R^2 & R \text{ totally tamely ramified} \end{cases} \tag{133}$$

Then by the definition of the different, the formula

$$\lambda^\diamondsuit(\xi) = \operatorname{tr} \frac{\xi}{\diamondsuit}$$

defines a linear functional $\lambda^\diamondsuit : \mathcal{O}_R \to \mathcal{O}_K$ that is *perfect,* that is, $\lambda^\diamondsuit$ generates the dual $\mathcal{O}_R^\vee$ as an $\mathcal{O}_R$-module, and hence the pairing

$$(x, y) \mapsto \lambda^\diamondsuit(xy)$$

is a perfect $\mathcal{O}_K$-linear pairing on $\mathcal{O}_R$. If $\alpha \in \mathcal{O}_R$, then the conic

$$\lambda^\diamondsuit(\alpha \xi^2)$$

is $\mathcal{O}_K$-integral on $\mathcal{O}_R$ (because the corresponding bilinear form $\lambda^{\diamondsuit}(\alpha\xi\eta)$ is integral) with determinant $N(\alpha)$. We will put the conic defined by the $\mathcal{M}_{11}$- and $\mathcal{M}_{22}$-conditions in this form.

The entities involved in transformation will be marked by the symbol $\odot$ ("odot"). This is the symbol for a circle in Euclidean geometry, and it is chosen to reflect a particular simplifying fact: after the transformation, the conic is *self-congruent*, that is, any two points on it can be taken to one another by an *isometry* of $\mathbb{P}^2(\mathcal{O}_K)$ preserving the conic. This will follow from the independence of basepoint in Lemmas 19.9 and 19.10. The general conic over a p-adic field is not self-congruent.

Lemma 19.3. *Let $i \in \{1,2\}$. Fix the discrete data such a way that $\mathcal{M}_{ii}$ is active. Recall that $\delta = \delta_0\tau$ is in a fixed coarse coset. Then there is a multiplier $\gamma_i^{\odot} \in R^{\times}$ with the following property:*

$$\xi_i^{\odot} = \frac{\xi_i'}{\gamma_i^{\odot}} = \frac{\xi_i}{\gamma_i\gamma_i^{\odot}\sqrt{\tau}}$$

is a primitive vector in $\mathcal{O}_R$, and the $\mathcal{M}_{11}$ condition $\operatorname{tr}(\xi_1^2) \equiv 0 \mod \pi^{m_{11}}$ is equivalent to a condition of the form

$$\lambda^{\diamondsuit}\left(\delta^{\odot}{\xi^{\odot}}^2\right) \equiv 0 \mod \pi^{m_{11}^{\odot}},$$

where $m_{11}^{\odot} = m_{11} - p^{\odot}$ is an integer and $\delta^{\odot} = \delta_0^{\odot}\tau \in \mathcal{O}_R$, where $\delta_0^{\odot}$ depends on the discrete data alone and satisfies

$$[\delta_0^{\odot}] = [\delta_0\hat{\omega}_C\diamondsuit] \in H^1 \quad \textit{and} \quad v_K(N(\delta_0^{\odot})) \in \{0,1\},$$

so that the conic $\mathcal{M}^{\odot}(\xi^{\odot}) = \lambda^{\diamondsuit}\left(\delta^{\odot}{\xi^{\odot}}^2\right)$ is relevant. Moreover, $\mathcal{M}^{\odot}$ is unimodular exactly when

$$[\delta_0\hat{\omega}_C\diamondsuit] \in \mathcal{L}_0.$$

Proof. We have $\xi_1 \in \pi^{-a_1-2b_1}\sqrt{\delta\hat{\omega}_C}\cdot R$.

Note that whatever $\gamma_i^{\odot}$ we pick, the conic takes the form

$$\lambda^{\diamondsuit}\left(\diamondsuit{\gamma_i^{\odot}}^2\gamma_i^2\tau{\xi_i^{\odot}}^2\right) \equiv 0 \mod \pi^{\bar{m}_{ii}},$$

or, for any $p^\odot$,

$$\lambda^\diamondsuit \left(\frac{\diamondsuit {\gamma_i^\odot}^2 \gamma_i^2}{\pi^{p^\odot}} \tau {\xi_i^\odot}^2 \right) \equiv 0 \mod \pi^{\bar{m}_{ii} - p^\odot}.$$

So we seek to pick $\gamma_i^\odot$ and $p^\odot$ so that

$$\delta_0^\odot = \frac{\diamondsuit {\gamma_i^\odot}^2 \gamma_i^2 \delta_0}{\pi^{p^\odot}}$$

lies in $\mathcal{O}_R$ with norm of valuation 0 or 1, and

$$m_{ii}^\odot = \bar{m}_{ii} - p^\odot$$

is an integer. The second condition is easily seen to follow from the first.

Unramified. If $[\delta_0 \hat{\omega}_C] \in \mathcal{L}_0$, then all extender indices are in $\mathbb{Z}$ and γ_i is a unit, so $\delta_0^\odot$ is a unit as well, choosing $\gamma_i^\odot = 1$ and $p^\odot = 0$. Thus we get

If $[\delta_0 \hat{\omega}_C] \in (1; \pi; \pi)\mathcal{L}_0$ for some ordering of the coordinates, then $[\delta] = [(1; \pi; \pi)\delta']$ for some unit δ'. By Corollary 17.5, either

- $a_i' \in \mathbb{Z}$ and $\xi_i \in \sqrt{\delta'}(\mathcal{O}_K^\times \times \sqrt{\pi}\mathcal{O}_Q)$, or
- $a_i' \in \mathbb{Z} + \frac{1}{2}$ and $\xi_i \in \sqrt{\delta'}(\sqrt{\pi}\mathcal{O}_K \times \mathcal{O}_Q)$.

In the first case, $\mathcal{M}_{11}$ is unsatisfiable if active, because $\alpha \xi_i^2$ has exactly one coordinate of zero valuation. So we have the second case. Observe that $\vec{v}(\gamma_i) = (1/2, 0, 0)$, so choosing $\gamma_i^\odot = 1$ and $p^\odot = 0$, we get $\vec{v}(\delta^\odot) = (1, 0, 0)$: the conic has determinant $\sim \pi$. Note that $\mathcal{M}^\odot \not\equiv 0 \mod \pi$ as a quadratic form: after passing to an unramified extension we may assume that $L = K \times K \times K$, and then $\mathcal{M}^\odot$ is diagonal with two of the three coefficients units. So $\mathcal{M}^\odot$ is tiny.

For compatibility with the other splitting types, we let

$$h_i = \begin{cases} 0, & [\delta_0 \hat{\omega}_C] \in \mathcal{L}_0 \\ 1, & \text{otherwise.} \end{cases}$$

Splitting type (1^3)**.** Here $\mathcal{O}_R$ is generated by a uniformizer π_R with $\pi_R^3 = \pi$ (for a suitably chosen uniformizer π). Under the Minkowski embedding, $\pi_R = \sqrt[3]{\pi} \cdot \bar{\zeta}_3$, where

$$\bar{\zeta}_3 = (1; \zeta_3; \zeta_3^2).$$

We have $\diamondsuit = \pi_R^2$.

Here $[\delta_0 \hat{\omega}_C] \in \mathcal{L}_0$ always. The extender indices are in $\frac{1}{3}\mathbb{Z}$, and γ_i is always a unit. Let $h = h_i \in \{0, 1, -1\}$ be the integer such that

$$a_i' \in \mathbb{Z} - \frac{h}{3}.$$

Then

$$\xi_1 \in \pi^{h/3}\sqrt{\delta^\odot}R = \bar{\zeta}_3^{-h}\sqrt{\delta^\odot}R;$$

indeed, since ξ_1 is primitive in $\mathcal{O}_K^3$,

$$\xi_1 \in \bar{\zeta}_3^{-h}\sqrt{\delta^\odot}\mathcal{O}_R^\times.$$

If $h = 0$, then $\mathcal{M}_{11}$ is unsatisfiable because the trace of a unit in $\mathcal{O}_R$ is always a unit.

If $h = 1$, the choice $\gamma_i^\odot = 1$, $p^\odot = 2/3$ works, making $\delta^\odot$ a unit.

If $h = -1$, we can no longer take $\gamma_i^\odot = 1$, because the maximal possible value for $p^\odot$ is $1/3$ and the corresponding conic has determinant $\sim \pi^2$. Instead, take $\gamma_i^\odot = \pi_R^{-2}$. Then the corresponding values of $\xi^\odot$, instead of being units, have valuation $2/3$ and thus are still primitive in $\mathcal{O}_R$. Take $p^\odot = -2/3$ and observe that $\delta^\odot$ is again a unit.

■

To summarize, the salient data of the transformation is shown here:

spl.t.	a_1' mod $\mathbb{Z}$	h_1	$[\delta\hat{\omega}_C\diamondsuit] \in$	$v_K\left(\gamma^{(K)}\gamma^{\odot(K)}\right)$	$v_K\left(\gamma^{Q}\gamma^{\odot Q}\right)$	$p^{\odot}$	$\delta^{\odot} \sim$	$\xi' \sim$
ur	0	0	$\mathcal{L}_0$	0	0	0	1	?
ur	1/2	1	$(1;\pi;\pi)\mathcal{L}_0$	1/2	0	0	$(\pi;1;1)$	$(?;1;1)$
1^3	$-1/3$	1	$\mathcal{L}_0$	0	0	2/3	1	1
1^3	1/3	-1	$\mathcal{L}_0$	$-2/3$	$-2/3$	$-2/3$	1	π_R^2

(134)

The advantage of making the conic's determinant associate to either 1 or π is that we have to solve very few isomorphism types of conics. Although we do not prove the following classification, it animates the choice of what invariants we compute:

Conjecture 19.4. *Let $\mathcal{C}$ be a relevant conic over the ring of integers $\mathcal{O}_K$ of a local field K.*

(*a*) *If $\mathcal{C}$ is tiny, it is determined up to isomorphism by its* Brauer class $\varepsilon(\mathcal{C}) \in \{\pm 1\}$*, the single bit telling whether $\mathcal{C}(\vec{x}) = 0$ has a nonzero solution over K.*

(*b*) *If $\mathcal{C}$ is unimodular, it is determined up to isomorphism by its Brauer class $\varepsilon(\mathcal{C})$ and its* squareness level $\ell(\mathcal{C})$*, the largest $\ell \in \mathbb{Z}, 0 \leq \ell \leq e/2$, such that*

$$\mathcal{C} \equiv c\lambda^2 \mod \pi^{\min\{2\ell+1,e\}}$$

as a quadratic form, for some constant $c \in \mathcal{O}_K^{\times}$ and linear form λ. Moreover, all combinations of values (ε, ℓ) occur, except that for e even, $\ell(\mathcal{C}) = e/2$ implies $\varepsilon(\mathcal{C}) = 1$ by Proposition 19.7 below. Thus there are exactly $e+1$ isomorphism classes of conics of determinant 1.

Note that if $\mathcal{C}$ is unimodular and $2\ell + 1 \leq e$, then $\mathcal{C}$ is congruent to a $c\lambda^2$ modulo $\pi^{2\ell}$ if and only if modulo $\pi^{2\ell+1}$, as the x^2, y^2, z^2 coefficients have square ratios modulo $\pi^{2\ell+1}$ and the cross-terms are multiples of 2 anyway. So the squareness level carries the same amount of information as the

squareness

$$\square(\mathcal{C}) = \max\left\{i : \mathcal{C} \equiv c\lambda^2 \mod \pi^i \text{ as a quadratic form}\right\} \in \left\{0, 2, 4, \ldots, 2\left\lfloor \frac{e-1}{2} \right\rfloor\right\} \cup \{e\}.$$

(We cannot have $\square(\mathcal{C}) > e$, or the determinant would vanish modulo π.)

When we use coordinates, we will generally use one of two explicit types of conics: the *diagonal conic*

$$aX^2 + bY^2 + cZ^2 = 0$$

and the *basepoint conic*

$$2XZ - Y^2 + aZ^2 = 0,$$

so called because it passes through the basepoint $[1 : 0 : 0]$ and is tangent to the line $Z = 0$ there. We begin with results concerning the diagonal conic.

19.1 Diagonal conics

Lemma 19.5. *Any relevant conic $\mathcal{C}$ is diagonalizable, that is, there exists a basis $(v_1, \ldots, v_3)$ for the given lattice V such that*

$$\mathcal{C}(x_1v_1 + x_2v_2 + x_3v_3) = a_1x_1^2 + a_2x_2^2 + a_3x_3^2.$$

Proof. When $\operatorname{char} k_K \neq 2$, we have that *any* conic is diagonalizable by an easy Gram-Schmidt procedure (in fact more is true: see O'Meara [46], 92:1). So we assume that $\operatorname{char} k_K = 2$. Here a quadratic space is not diagonalizable in general, and we must use the restrictions given on $\mathcal{C}$.

Write the matrix of $\mathcal{C}$, with respect to any basis (ξ_1, ξ_2, ξ_3), as

$$\mathcal{C} = \begin{bmatrix} a & f & e \\ f & b & d \\ e & d & c \end{bmatrix}.$$

In the case that $\mathcal{C}$ is unimodular, we see from

$$\det \mathcal{C} = abc + 2def - ad^2 - be^2 - cf^2 \sim 1$$

that at least one of the diagonal entries—say a—is a unit. Then we can use a to eliminate f and e (that, is, add multiples of ξ_1 to ξ_2 and ξ_3). Now if b (or, symmetrically, c), is nonzero modulo π, we use it to eliminate d, and we are done, as we have found the requisite diagonal form. However, it is possible that

$$\mathcal{C} \equiv \begin{bmatrix} a & & \\ & & d \\ & d & \end{bmatrix} \mod \pi$$

for units a and d. Rescaling ξ_3, we can assume that

$$\mathcal{C} \equiv a \cdot \begin{bmatrix} 1 & & \\ & & 1 \\ & 1 & \end{bmatrix} \mod \pi.$$

At first we are doubtful, because the unimodular form

$$\mathcal{C}_2 = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}$$

on $\mathcal{O}_K^2$ is not diagonalizable. However, we can use the identity

$$\begin{bmatrix} 1 & 1 & 1 \\ 1 & 1 & \\ 1 & & 1 \end{bmatrix} \begin{bmatrix} 1 & & \\ & & 1 \\ & 1 & \end{bmatrix} \begin{bmatrix} 1 & 1 & 1 \\ 1 & 1 & \\ 1 & & 1 \end{bmatrix} \equiv \begin{bmatrix} 1 & & \\ & 1 & \\ & & 1 \end{bmatrix} \mod 2$$

to change to a basis in which

$$\mathcal{C} \equiv a \cdot \begin{bmatrix} 1 & & \\ & 1 & \\ & & 1 \end{bmatrix} \mod \pi.$$

Then the diagonalization proceeds without a hitch.

If $\mathcal{C}$ is tiny, we proceed similarly. Taking a a unit (since we are given $\mathcal{C}(\xi_1) \sim 1$ for some ξ_1), we can eliminate f and e. Then since

$$\det \mathcal{C} = a(bc - d^2) \sim \pi,$$

we must have at least one of b and c a unit, as otherwise $\det \mathcal{C}$ would be either a unit (if d is a unit) or a multiple of π^2 (if $\pi \mid d$). So we can eliminate d and again get the desired diagonalization. ■

The following lifting lemma for solutions modulo 4π will be essential for us.

Lemma 19.6. *Let $\mathcal{C}$ be a diagonalized conic on an $\mathcal{O}_K$-lattice V, and assume that $v(\det \mathcal{C}) \leq 1$. Let $v \in V$ be a primitive vector with*

$$\mathcal{C}(v) \equiv 0 \mod \pi^m, \quad m > 2e.$$

Then there exists a $v' \in V$ such that

$$v' \equiv v \mod \pi^{m-e} \quad \textit{and} \quad \mathcal{C}(v') = 0.$$

Proof. We may write the conic in diagonal form

$$\mathcal{C}(x_1 v_1 + \cdots + x_n v_n) = a_1 x_1^2 + \cdots + a_n x_n^2.$$

Let $v = x_1 v_1 + \cdots + x_n v_n$. Since v is primitive, not all the x_i are zero modulo π. We claim that

there is an i with

$$\pi \nmid a_i \quad \text{and} \quad \pi \nmid x_i. \tag{135}$$

If not, then $\det \mathcal{C} \sim \pi$, and without loss of generality, $a_1, \ldots, a_{n-1}$ are units while $a_n \sim \pi$; and x_n is a unit while $x_1, \ldots, x_{n-1}$ are multiples of π. Summing, we find that

$$\mathcal{C}(v) \equiv a_n x_n^2 \not\equiv 0 \mod \pi^2,$$

a contradiction.

Choose i satisfying (135). We will construct v' by changing only the x_i coordinate of v to a different value x_i'. The desired condition $\mathcal{C}(v') = 0$ takes the form

$$x_i'^2 = y$$

for some $y \equiv x_i^2$ modulo π^m. Since $m > 2e$, we have that y is also a square and, indeed, has a (unique) square root x_i' satisfying $x_i' \equiv x_i \mod \pi^{m-e}$. This constructs the desired v'. ■

Here are two easy corollaries.

Proposition 19.7. *If e is even and $\mathcal{C}$ is a unimodular conic of squareness e (the maximal possible value), then $\varepsilon(\mathcal{C}) = 1$, that is, $\mathcal{C}$ has a rational point.*

Proof. We may assume that $\mathcal{C}$ is diagonal:

$$\mathcal{C}(x_1\xi_1 + x_2\xi_2 + x_3\xi_3) = a_1x_1^2 + a_2x_2^2 + a_3x_3^2.$$

Then $\varepsilon(\mathcal{C})$ is a Hilbert symbol,

$$\varepsilon(\mathcal{C}) = \left\langle \frac{-a_2}{a_1}, \frac{-a_3}{a_1} \right\rangle.$$

Both arguments are squares of units modulo 2. But since e is even, they are actually squares modulo 2π, so the Hilbert symbol is 1 by Lemma 7.19. ■

Proposition 19.8. *Let $\mathcal{C}$ and $\mathcal{C}'$ be conics of determinant 1 and squareness level ℓ. Suppose that the associated bilinear forms of $\mathcal{C}$ and $\mathcal{C}'$ are congruent modulo $\pi^{2e-2\ell}$. Then $\varepsilon(C) = \varepsilon(C')$.*

Proof. We may assume that $\mathcal{C}$ is diagonal:

$$\mathcal{C}(x_1\xi_1 + x_2\xi_2 + x_3\xi_3) = a_1x_1^2 + a_2x_2^2 + a_3x_3^2.$$

Although $\mathcal{C}'$ need not be diagonal with respect to the same basis, the orthogonalization procedure furnished by the proof of Lemma 19.5 yields a basis (ξ_1', ξ_2', ξ_3') with $\xi_j' \equiv \xi_j \mod \pi^{2e-2\ell}$ such that $\mathcal{C}'$ is diagonal with respect to it,

$$\mathcal{C}'(x_1\xi_1' + x_2\xi_2' + x_3\xi_3') = a_1'x_1^2 + a_2'x_2^2 + a_3'x_3^2$$

with $a_j \equiv a_j' \mod \pi^{2e-2\ell}$. New compare

$$\varepsilon(\mathcal{C}) = \left\langle \frac{-a_2}{a_1}, \frac{-a_3}{a_1} \right\rangle \quad \text{and} \quad \varepsilon(\mathcal{C}') = \left\langle \frac{-a_2'}{a_1'}, \frac{-a_3'}{a_1'} \right\rangle$$

The arguments to the Hilbert symbols are squares modulo $\pi^{2\ell+1}$, so the value of the Hilbert symbol is unchanged under multiplying by units that are squares modulo $\pi^{\max\{2\ell+1, 2e-2\ell\}}$ by Lemma 7.19, and that is exactly what we have done. ∎

19.2 The solution volume of the conic

We now use the basepoint form to determine volumes of conics.

Lemma 19.9 (**Igusa zeta function of a conic**). *Let $\mathcal{C}$ be a conic of determinant 1 on the projectivization $\mathbb{P}(V)$ of a 3-dimensional vector space V. Suppose that $\mathcal{C}$ has Brauer class $\varepsilon(\mathcal{C}) = 1$, that is, it admits a basepoint v_0 such that $\mathcal{C}(v_0) = 0$.*

Let $U_{m^\odot, n^\odot}$ be the volume of $v \in \mathbb{P}(V)$ (counting the whole $\mathbb{P}(V)$ to have volume $1 + q^{-1} + q^{-2}$)

such that

$$v \equiv v_0 \mod \pi^{n^\odot} \tag{136}$$

$$\mathcal{C}(v) \equiv 0 \mod \pi^{m^\odot}. \tag{137}$$

(Note that these $m^\odot$ and $n^\odot$ correspond to the $m_{11}^\odot$ and $n^\odot$ of Lemmas 19.3 and 19.18.)

Then for $m^\odot$ and $n^\odot$ integers with $m^\odot > 2e$ and $m^\odot \geq 2n^\odot$, the volume $U_{m^\odot,n^\odot}$ depends only on $m^\odot$, $n^\odot$, and the squareness level $\ell = \ell(\mathcal{C})$. It is given by

$$U_{m^\odot,n^\odot} = q^{2e-m^\odot-n^\odot}, \quad n^\odot \geq e$$

and the recurrence

$$\frac{U_{m^\odot,n^\odot}}{U_{m^\odot,n^\odot+1}} = \begin{cases} 2 & n^\odot = e - 2\ell - 1 \geq 0 \\ q & n^\odot \equiv e \mod 2, n^\odot > e - 2\ell - 1, n^\odot > 0 \\ q+1 & n^\odot = 0, \ell = \frac{e}{2} \\ 1 & \textit{otherwise.} \end{cases}$$

Explicitly,

$$U_{m^\odot,n^\odot} = \begin{cases} q^{e-m^\odot-n^\odot} & n^\odot \geq e & \textit{(a} \text{ black conic}\textit{)} \\ q^{-m^\odot+\left\lfloor \frac{e-n^\odot}{2} \right\rfloor} & e \geq n^\odot > e - 2\ell - 1, n^\odot > 0 & \textit{(a} \text{ blue conic}\textit{)} \\ 2q^{-m^\odot+\ell} & 0 \leq n^\odot \leq e - 2\ell - 1 & \textit{(a} \text{ green conic}\textit{)} \\ \left(1 + \frac{1}{q}\right) q^{-m^\odot+e/2}, & n^\odot = 0, \ell = \frac{e}{2}, e \textit{ even} & \textit{(a} \text{ large conic}\textit{)} \end{cases}$$

Proof. For the black-conic case, we diagonalize the conic to

$$\mathcal{C}(X, Y, Z) = aX^2 + bY^2 + cZ^2.$$

Let the basepoint be $v_0 = [X_0 : Y_0 : Z_0]$. Note that two coordinates of v_0, say X_0 and Y_0, are nonzero modulo π. We may scale so that $Y_0 = 1$ and so that all solutions we seek have $Y = 1$. This eliminates the issue of scaling ambiguity.

The $n^\odot$-pixel of $[X : 1 : Z]$ satisfying (136) has volume $q^{-2n^\odot}$. For fixed Z, with $Z \equiv Z_0 \mod \pi^{n^\odot}$ the condition (137) simplifies to $X^2 \equiv u \mod \pi^{m^\odot}$, where u is a unit with $u \equiv X_0^2 \mod \pi^{n^\odot+e}$. Hence its solutions form a congruence class mod $\pi^{m^\odot-e}$, and overall, the solution volume is $q^{n^\odot} \cdot q^{e-m^\odot} = q^{e-m^\odot-n^\odot}$.

We use this as the base case to prove the recursive formula (and hence also the explicit formula) for $U_{m^\odot,n^\odot}$ by downward induction on $n^\odot$. Our aim is to determine the number r of $(n^\odot+1)$-pixels within the $n^\odot$-pixel of v_0 that contain a solution to $\mathcal{C}(v) = 0$, or equivalently, to $\mathcal{C}(v) \equiv 0 \mod \pi^{m^\odot}$. Then, by induction, there is a volume $U_{m^\odot,n^\odot+1}$ of solutions in each of those, so $U_{m^\odot,n^\odot} = rU_{m^\odot,n^\odot+1}$ as desired. It remains to compute

$$r = \frac{U_{m^\odot,n^\odot}}{U_{m^\odot,n^\odot+1}}.$$

We now abandon the diagonalized form and choose coordinates such that the basepoint is $v_0 = [1 : 0 : 0]$ and the tangent line there is $Z = 0$. Then the conic has the form

$$\mathcal{C}(X, Y, Z) = 2gXY + 2dXZ - cY^2 + 2bYZ + aZ^2.$$

Note that π does not divide both d and g, for then the conic's determinant

$$\begin{vmatrix} 0 & g & d \\ g & -c & b \\ d & b & a \end{vmatrix} = 2bdg + cd^2 - ag^2$$

would be divisible by π^2. So, by symmetry, we may assume $d \sim 1$. We scale the conic so that $d = 1$, and then the transformation $Z \mapsto Z - gY$ makes $g = 0$. Also, the transformation $X \mapsto X - bY$

makes $b = 0$. Now $c = 1$ to make the determinant 1. Thus the conic takes the basepoint form

$$\mathcal{C}(X, Y, Z) = 2XZ - Y^2 + aZ^2,$$

where $a \in \mathcal{O}_K$ is the only undetermined coefficient. By definition of squareness level, we know that a is a square modulo $\pi^{\min\{2\ell+1,e\}}$, but not modulo $\pi^{2\ell+3}$ if $\ell < \lfloor e/2 \rfloor$. For any $a' \in \mathcal{O}_K$, the transformation $Y \mapsto Y + a'Z$ can be used to increment a by the square a'^2, followed by another $X \mapsto X - b'Y$ to remove the YZ term. Picking a' appropriately, we can arrange so that $v(a)$ *reveals the squareness:* either

- $\ell < \lfloor e/2 \rfloor$ and $v(a) = 2\ell + 1$, or
- $\ell = \lfloor e/2 \rfloor$ and $2|a$. In this case, indeed, the transformation $X \mapsto X - a/2$ makes $a = 0$. (So we have proved one case of Conjecture 19.4: for $\ell = \lfloor e/2 \rfloor$ and $\varepsilon = 1$, the conic takes the fixed form $2XZ - Y^2$.)

To parametrize $\mathcal{C}(\mathcal{O}_K)$, we use the age-old trick of *stereographic projection,* that is, drawing lines of varying slope through the known basepoint $[1 : 0 : 0]$. An easy calculation shows that the second intersection of the line $sZ - tY = 0$ with the conic $\mathcal{C}$ is $[s^2 - at^2 : 2st : 2t^2]$, yielding an isomorphism

$$\begin{aligned} \mathbb{P}^1(K) &\cong \mathcal{C}(K) \\ [s : t] &\mapsto [s^2 - at^2 : 2st : 2t^2]. \end{aligned}$$

If $[s : t]$ is in lowest terms over $\mathcal{O}_K$, then $[s^2 - at^2 : 2st : 2t^2]$ need not be in lowest terms over $\mathcal{O}_K$, but will have cancellation by π^j, where $j = \min\{v_K(s^2 - at^2), e + v_K(st), e + v_K(t^2)\}$. Note that $j \le e$ because s and t are coprime, so

$$j = \min\{v_K(s^2 - at^2), e\}.$$

Note also that the resulting point

$$[X : Y : Z] = \left[\frac{s^2 - at^2}{\pi^j} : \frac{2st}{\pi^j} : \frac{2t^2}{\pi^j}\right]$$

lies in the $(e-j)$-pixel of $[1:0:0]$, but not in the $(e-j+1)$-pixel if $j > 0$. Hence the points we are interested in, namely in the $n^\odot$-pixel of the basepoint but outside the $(n^\odot+1)$-pixel, correspond exactly to values of $[s:t]$ for which $j = e - n^\odot$. That is, the valuation $v(s^2 - at^2)$ must be exactly $e - n^\odot$ (if $n^\odot > 0$) or at least e (if $j = 0$).

Observe that when $n^\odot < e - 2\ell - 1$, there are no solutions. Also, when $n^\odot > e - 2\ell - 1$ is of the same parity as e, there are no solutions, because

$$s^2 - at^2 \equiv s^2 \mod \pi^{\min\{2\ell+1, e\}}$$

has even valuation if nonzero mod $\pi^{\min\{2\ell+1,e\}}$. The ratio $U_{m^\odot,n^\odot}/U_{m^\odot,n^\odot+1}$ is thus 1 in these cases, as claimed.

- Suppose that $n^\odot = e - 2\ell - 1$. If $n^\odot > 0$, we seek the $[s:t]$ such that $s^2 - at^2$ attains its maximal valuation $2\ell+1$: this happens when $\pi^{\ell+1}|s$. If $n^\odot = 0$, we seek $\pi^e|s^2$, which is still equivalent to $\pi^{\ell+1}|s$. Hence we are looking at the $[s:t]$ with $t = 1$, $s = \pi^{\ell+1}s'$, where $s' \in \mathcal{O}_K$. Then the resulting point on $\mathcal{C}(\mathcal{O}_K)$ is

$$\begin{aligned}
[X : Y : Z] &= \left[\frac{s^2 - at^2}{\pi^{2\ell+1}} : \frac{2st}{\pi^{2\ell+1}} : \frac{2t^2}{\pi^{2\ell+1}}\right] \\
&= \left[\frac{\pi^{2\ell+2}s'^2 - a}{\pi^{2\ell+1}} : \frac{2\pi^{\ell+1}s'}{\pi^{2\ell+1}} : \frac{2t^2}{\pi^{2\ell+1}}\right] \\
&= \left[\pi s'^2 - \frac{a}{\pi^{2\ell+1}} : \frac{2s'}{\pi^\ell} : \frac{2}{\pi^{2\ell+1}}\right] \\
&\equiv \left[\pi s'^2 - \frac{a}{\pi^{2\ell+1}} : 0 : \frac{2}{\pi^{2\ell+1}}\right] \mod \pi^{n^\odot+1} = \pi^{e-2\ell}.
\end{aligned}$$

We claim that this is actually the same point modulo $\pi^{n^\odot+1}$ regardless of s', that is, the $\pi s'^2$ term contributes nothing. If $2\ell + 1 = e$, this is clear because $n^\odot = 0$. Otherwise, $a' = a/\pi^{2\ell+1}$

is a unit, and if we multiply all three coordinates by

$$\frac{a'}{a' + \pi s'} \equiv 1 \mod \pi,$$

the last two coordinates do not change mod $\pi^{n^\odot+1}$ because they are 0 mod $\pi^{n^\odot}$. Thus all points $[X : Y : Z]$ obtained lie in a single $(n^\odot+1)$-pixel, and hence the ratio $U_{m^\odot,n^\odot}/U_{m^\odot,n^\odot+1}$ is 2.

- Suppose that $n^\odot \equiv e \mod 2$, $n^\odot > e - 2\ell - 1$, and $n^\odot > 0$. Then $e - n^\odot = j = 2j'$ is even, with $j' \leq \ell$. The pairs $[s : t]$ yielding $s^2 - at^2 \sim \pi^j$ are exactly those with $s \sim \pi^{j'}$. Write $t = 1$, $s = \pi^{j'} s'$, where $s' \in \mathcal{O}_K^\times$. Then the resulting point on $\mathcal{C}(\mathcal{O}_K)$ is

$$\begin{aligned}
[X : Y : Z] &= \left[\frac{s^2 - at^2}{\pi^j} : \frac{2st}{\pi^j} : \frac{2t^2}{\pi^j}\right] \\
&= \left[-\frac{a}{\pi^{2j'}} + s'^2 : \frac{2s'}{\pi^{j'}} : \frac{2}{\pi^{2j'}}\right] \\
&\equiv \left[s'^2 : 0 : \frac{2}{\pi^{2j'}}\right] \qquad \mod \pi^{n^\odot+1},
\end{aligned}$$

where at the last step we multiplied all three coordinates by the unit

$$\frac{s'^2}{s'^2 - \frac{a}{\pi^{2j'}}} \equiv 1 \mod \pi.$$

We get $q - 1$ different $(n^\odot + 1)$-pixels, one for each value of s' mod π. Hence the ratio $U_{m^\odot,n^\odot}/U_{m^\odot,n^\odot+1}$ is q.

- Finally, suppose that $n^\odot = 0$ and $\ell = \frac{e}{2}$. Write $t = 1$, $s = \pi^{e/2} s'$, where $s' \in \mathcal{O}_K$. We get

$$\begin{aligned}
[X : Y : Z] &= \left[\frac{s^2}{\pi^e} : \frac{2st}{\pi^e} : \frac{2t^2}{\pi^e}\right] \\
&= \left[\frac{2s'}{\pi^{e/2}} + s'^2 : \frac{2s'}{\pi^{e/2}} : \frac{2}{\pi^e}\right] \\
&\equiv \left[s'^2 : 0 : \frac{2}{\pi^e}\right] \qquad \mod \pi = \pi^{n^\odot+1}.
\end{aligned}$$

We get q different 1-pixels, one for each value of s' mod π. Hence the ratio $U_{m^\odot,n^\odot}/U_{m^\odot,n^\odot+1}$ is $q+1$. ■

For determinant π, we use the same method. Fortunately, everything comes out much simpler.

Lemma 19.10 (**Igusa zeta function of a conic**). *Let $\mathcal{C}$ be an integer-matrix conic over $\mathcal{O}_K$ of determinant π. Suppose that $\mathcal{C}$ has Brauer class $\varepsilon(\mathcal{C}) = 1$, that is, it admits a basepoint v_0 such that $\mathcal{C}(v_0) = 0$.*

Let $U_{m^\odot,n^\odot}$ be the volume of $v \in \mathbb{P}(V)$ such that

$$v \equiv v_0 \mod \pi^{n^\odot} \tag{138}$$

$$\mathcal{C}(v) \equiv 0 \mod \pi^{m^\odot}. \tag{139}$$

Then for $m^\odot > 2e$ and $m^\odot \geq 2n^\odot$, the volume $U_{m^\odot,n^\odot}$ depends only on $m^\odot$ and $n^\odot$:

$$U_{m^\odot,n^\odot} = \begin{cases} q^{e-m^\odot-n^\odot} & n^\odot > e \quad (a \text{ black conic}) \\ 2q^{-m^\odot} & 0 \leq n^\odot \leq e \quad (a \text{ green conic}) \end{cases}$$

Proof. Diagonalize the conic to the form

$$\mathcal{C}(X,Y,Z) = aX^2 + bY^2 + c\pi Z^2 = 0,$$

where $a, b, c \in \mathcal{O}_K^\times$. Observe that X_0 and Y_0 are units, and scale so that $Y = Y_0 = 1$.

If $n^\odot > e$, then for each $Z \equiv Z_0 \mod \pi^{n^\odot}$, the condition $\mathcal{C}(X,Y,Z) \equiv 0 \mod \pi^{m^\odot}$ simplifies to $X^2 \equiv u \mod \pi^{m^\odot}$, where $u \equiv X_0^2 \mod \pi^{n^\odot+e+1}$, and hence the square roots X with $X \equiv X_0 \mod \pi^{n^\odot}$ form a single congruence class mod $\pi^{m^\odot-e}$. So the volume is $q^{e-m^\odot-n^\odot}$.

If $n^\odot = e$, then we use the same method, but now the equation $X^2 \equiv u \mod \pi^{m^\odot}$, where $u \equiv X_0^2$ mod π^{2e+1}, has as solution set two classes mod $\pi^{m^\odot-e}$, each the negative of the other.

We claim that these are all the solutions mod $\pi^{m^\odot}$; that is, that the whole conic lies within an e-pixel. Suppose there is such an $[X : 1 : Z] \not\equiv [X_0 : 1 : Z_0] \mod 2$, and let $v_K(X - X_0) = i$,

$v_K(Z - Z_0) = j$. Then

$$a(X^2 - X_0^2) = \pi c(Z^2 - Z_0^2).$$

If $i < e$, then the left side has even valuation $2i$ which cannot be matched by the right side. If $j < e$, then the right side has odd valuation $2j + 1$ which cannot be matched by the left side. This completes the proof.

■

19.3 The Brauer class

In this section we understand the Brauer class of conics of the form

$$\mathcal{A}: \quad \operatorname{tr}(\alpha x^2) = 0.$$

This is a conic in the $\mathbb{P}^2(K)$ of possible values of x. Over K, there are just two types of conic, one with points and one without. Our first task will be to understand which case occurs for each α.

Our main result will be the following.

Lemma 19.11. *If $\alpha \in R^{N=1}$, define*

$$\varepsilon(\alpha) = \begin{cases} 1 & \text{if } \operatorname{tr}(\alpha x^2) = 0 \text{ for some nonzero } x \in L \\ -1 & \text{otherwise.} \end{cases}$$

Then the map of $\mathbb{F}_2$-vector spaces

$$H^1 \to \mu_2$$

$$\alpha \mapsto \varepsilon(\alpha)/\varepsilon(1)$$

is a nondegenerate quadratic form whose associated bilinear form is none other than the Hilbert

pairing on H^1. That is,

$$\varepsilon(\alpha\beta) = \varepsilon(1) \cdot \varepsilon(\alpha) \cdot \varepsilon(\beta) \cdot \langle \alpha, \beta \rangle_\varepsilon .$$

The proof is not especially difficult, but it uses different tools than the rest of the paper and so will be deferred. See Appendix A.

Remark 19.12. ε comes up, in a related context, in the work of Bhargava and Gross ([7], §7.2), where it is stated to be a quadratic form, at least in the tamely ramified case.

Remark 19.13. Over fields of characteristic not 2, a quadratic form is uniquely determined by its associated bilinear form. However, over $\mathbb{F}_2$, the local Hilbert pairing $\langle \bullet, \bullet \rangle_\varepsilon$ on H^1 lifts to $|(H^1)^*| = |H^1|$ quadratic forms, thanks to the ambiguity by adding a linear functional. It is not hard to show that these quadratic forms are exactly

$$\alpha \mapsto \frac{\varepsilon(\omega\alpha)}{\varepsilon(\omega)},$$

for each $\omega \in H^1$.

19.4 The squareness

For the cases in Lemma 19.3 in which the transformed conic $\mathcal{M}$ is unimodular, we need also to compute its squareness.

If $\mathcal{C}$ is a unimodular conic, the maximal

Lemma 19.14. *Let $[\heartsuit] = [1] \in H^1$. (The reason for this strange definition is that, in splitting type $1^2 1$, we will need a $[\heartsuit] \neq [1]$ in general.)*

The conic

$$\mathcal{M}(\xi^\odot) = \lambda^\diamondsuit \left(\delta^\odot \xi^{\odot 2} \right), \quad \delta^\odot \in \mathcal{O}_R^\times$$

has squareness

$$\square(\mathcal{M}) = \max\left\{\ell : [\delta^{\odot}\heartsuit] \equiv 1 \mod \pi^{\ell}; \quad \ell = e, \text{ or } \ell < e \text{ and } \ell \text{ is odd}\right\} \tag{140}$$

$$= \begin{cases} \min\left\{2\ell(\delta\hat{\omega}_C\diamondsuit\heartsuit) + 1, e\right\}, & R \text{ unramified} \\ \min\left\{2\left\lfloor \dfrac{\ell(\delta\hat{\omega}_C\diamondsuit\heartsuit)}{2}\right\rfloor + 1, e\right\}, & R \text{ ramified.} \end{cases} \tag{141}$$

Remark 19.15. As stated, the lemma only requires $\heartsuit$ to be defined modulo $\mathcal{L}_{\lfloor e/2\rfloor}$ (unramified types) resp. $\mathcal{L}_{2\lfloor e/2\rfloor}$ (ramified types). We will mostly use $\heartsuit$ in this way, but when we do the brown zone, we will need a finer definition and will mention this.

Proof. In unramified splitting type, we first claim that going up to an *unramified* extension K'/K does not change either the left or the right side of (140). The right-hand side is less than $\lfloor e/2\rfloor$ only if $[\delta\hat{\omega}_C\heartsuit]$ is represented by a generic unit $\delta^{\odot} = 1 + \alpha\pi^{2i+1}$, $2i+1 < e$, and this generic unit remains generic in $R' = K' \otimes_K R$. As to the left side, we can diagonalize the conic $\mathcal{M}$ to have the form

$$\mathcal{M}(X, Y, Z) = aX^2 + bY^2 + cZ^2, \quad abc = 1.$$

Then

$$\square(\mathcal{M}) = \min\left\{2\ell(b/a) + 1, 2\ell(c/b) + 1, e\right\},$$

and this remains invariant over K'.

Therefore, we may assume that $R \cong K \times K \times K$ is totally split. Let $\delta^{\odot} = (a; b; c)$. Then $\mathcal{M}$ is diagonal and

$$\begin{aligned} \square(\mathcal{M}) &= \min\left\{2\ell(b/a) + 1, 2\ell(c/b) + 1, e\right\} \\ &= \min\left\{2\ell(a) + 1, 2\ell(b) + 1, 2\ell(c) + 1, e\right\} \\ &= \min\left\{2\ell(\delta^{\odot}) + 1, e\right\}, \end{aligned}$$

as desired.

In splitting type 1^3, we can scale $\delta^{\odot}$ by $(\mathcal{O}_R^{\times})^2$ so that its level is manifest:

$$\delta^{\odot} = 1 + \alpha \cdot \pi_R^{2j+1},$$

where $\alpha \in \mathcal{O}_R^{\times}$ and where

$$j \in \{1, 3, 4, 6, \ldots, 3e-2, 3e, \infty\}$$

controls $\ell(\delta^{\odot})$. Let $\delta^{\odot} = a + b\pi_R + c\pi_R^2$ and note that, in the basis $(1, \pi_R, \pi_R^2)$, the conic

$$\mathcal{M}(\xi') = \mathrm{tr}(\pi_R^{-2}\delta^{\odot}\xi'^2)$$

has matrix

$$\begin{bmatrix} c & b & a \\ b & a & \pi c \\ a & \pi c & \pi b \end{bmatrix}.$$

Since a is a unit, we get

$$\begin{aligned} \ell(\mathcal{M}) &= \max\left\{ i \leq e : \frac{c}{a} \text{ and } \frac{\pi b}{a} \text{ are squares mod } \pi^i \right\} \\ &= \min\left\{ 2\left\lfloor \frac{j-1}{3} \right\rfloor, e \right\} \\ &= \min\left\{ \left\lfloor \frac{\ell(\delta^{\odot})}{2} \right\rfloor, e \right\}, \end{aligned}$$

as desired.

■

We have the following corollary:

Lemma 19.16. *The Brauer class $\varepsilon(\delta)$ takes the same value for all δ in the coset $\hat{\omega}_C \heartsuit \diamondsuit \mathcal{L}_{\lceil e'/2 \rceil}$.*

Proof. Let $[\delta] = [\kappa\hat{\omega}_C\heartsuit\diamondsuit]$, where

$$\kappa \equiv 1 \mod \begin{cases} \pi^{2\lceil e/2\rceil+1}, & R \text{ unramified} \\ \pi^{2\lceil e/2\rceil}, & R \text{ ramified.} \end{cases}$$

Then $[\delta^{\odot}\heartsuit] \in \mathcal{L}_{\lceil e'/2\rceil}$, so the conic $\mathcal{M} = \mathcal{M}_\delta$ has maximal squareness e. If e is even, we know that $\varepsilon(\delta) = 1$ by Proposition 19.7. So we may assume that e is odd.

Now $\kappa \equiv 1 \mod 2\pi$, so the associated bilinear forms

$$\mathcal{M}(\xi,\eta) = \lambda^{\diamondsuit}(\delta^{\odot}\xi\eta) \quad \text{and} \quad \mathcal{M}'(\xi,\eta) = \lambda^{\diamondsuit}(\kappa\delta^{\odot}\xi\eta)$$

are congruent modulo 2π. So by Proposition 19.8, the two conics have the same Brauer class. ∎

19.5 $\mathcal{N}_{11}$

In this section, we will transform the $\mathcal{N}_{11}$-condition, which says that all coordinates of $\bar{\omega}_C^{-1} \cdot \xi_1^2$ are congruent modulo $\pi^{n_{11}}$, into a more manageable form.

We will sometimes need to make some subtle reductions, and thus we make the following definition:

Definition 19.17. A *first vector problem* $\mathfrak{P}$ consists of a choice of resolvent algebra R and as much of the discrete data as is needed to make $\mathcal{M}_{11}$ and $\mathcal{N}_{11}$ meaningful: the coarse coset $\delta_0\mathcal{L}_0$, the resolvent extender vector θ_1 (which determines $\hat{\omega}_C$ and $\bar{s}$), and the moduli m_{11} and n_{11}. These are required to satisfy the requisite integrality properties, which essentially say that

$$B_{\theta_1}(m_{11}, n_{11} - \bar{s}) = \pi^{m_{11}}\mathcal{O}_K\theta_1 + \pi^{n_{11}-\bar{s}}\mathcal{O}_K\theta_2$$

is a subset of R, but are otherwise untethered from a cubic or a quartic ring. The *answer* to a first

vector problem is the weighting

$$W_{\mathfrak{P}} = W_{\theta_1, m_{11}, n_{11}} : \delta_0 \mathcal{L}_0 \to \mathbb{Q}_{\geq 0}$$

that attaches to each quartic algebra $\delta \in \delta_0 \mathcal{L}_0$ the volume of $\xi_1' \in \mathbb{P}(\mathcal{O}_R)$ such that the corresponding $\xi_1 = \xi_1' \gamma_1$ satisfies the resolvent conditions

$$\begin{aligned} \mathcal{M}_{11} : &\qquad \operatorname{tr}(\xi_1^2) \equiv 0 \mod \pi^{m_{11}} \\ \mathcal{N}_{11} : &\quad \text{All coordinates of } \bar{\omega}_C^{-1} \cdot \xi_1^2 \text{ are congruent} \mod \pi^{n_{11}}. \end{aligned}$$

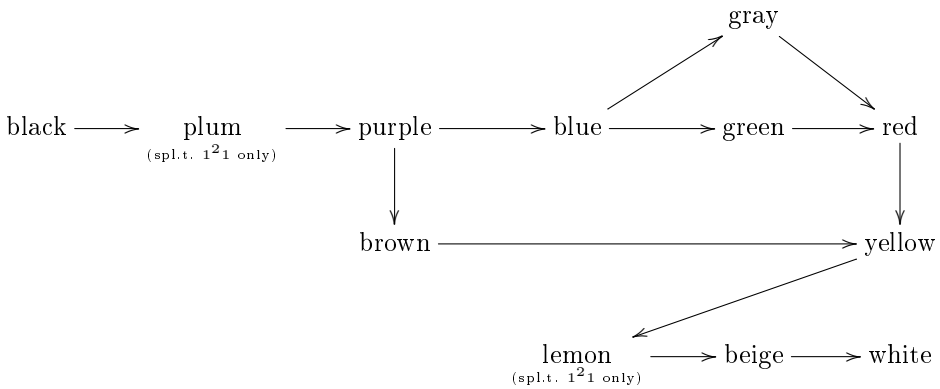
We normalize volumes so that

$$\mu(R) = 1 \quad \text{and} \quad \mu(\mathbb{P}(R)) = 1 + \frac{1}{q} + \frac{1}{q^2}.$$

We write $W^{\odot}$ instead of W when we wish to normalize instead by the vector $\xi_1^{\odot} = \xi_1'/\gamma^{\odot}$ in Lemma 19.3. Thus

$$W_{\mathfrak{P}}^{\odot} = q^{v\left(N_{R/K}(\gamma^{\odot})\right)} W_{\mathfrak{P}}.$$

First vector problems will be sorted into *zones*, given by linear inequalities on m_{11} and n_{11}, and having the properties that within each zone, the answer has a uniform description. Zones will be named by colors in such a way that a brightening of the color correlates with a lowering of m_{11} and/or n_{11} and an increase in the answer. Brightening is governed by the following poset:



Lemma 19.18. *Fix the data of a first vector problem $\mathfrak{P}$ in such a way that $\mathcal{N}_{11}$ is active with*

$$0 < n_{11} \leq 2e < m_{11}^{\odot} \tag{142}$$

and there is a solution ξ_0 to $\mathfrak{P}$. Let $\xi_0^{\odot} = \xi_0/\gamma_1^{\odot}$ be its transform. Then there is an $n^{\odot} \in \mathbb{Z}_{\geq 0}$ such that, for any ξ_1 satisfying $\mathcal{M}_{11}$,

$$\xi_1 \text{ satisfies } \mathcal{N}_{11} \iff \xi_1^{\odot} \equiv \xi_0^{\odot} \mod \pi^{n^{\odot}}.$$

The value of $n^{\odot}$ is given as follows:

- *In unramified splitting types,*

$$n^{\odot} = \left\lceil \frac{n_{11}}{2} \right\rceil.$$

- *In splitting type (1^3),*

$$n^{\odot} = \left\lceil \frac{n_{11}}{2} - \frac{h_1}{3} \right\rceil.$$

Remark 19.19. The condition $n_{11} \leq 2e$ (which, as we will see, restricts us to the blue, green, red, yellow, and lemon zones) can be removed, but then our conclusion must be that there is a family $\{\xi_{0(1)}, \ldots, \xi_{0(r)}\}$ of basic solutions, $r \in \{1, 2, 4\}$. The formula for $n^{\odot}$ becomes more complicated, and we will be able to solve these zones by other means.

Proof of Lemma 19.18. In view of Lemma 19.6, we may assume $m_{11} = \infty$, replacing $\xi_1^{\odot}$ by a value in the same e-pixel that satisfies $\mathcal{M}^{\odot}(\xi_1^{\odot}) = 0$ exactly.

Let ξ_0 be a fixed solution to $\mathfrak{P}$, and let ξ_1 be any solution to $\mathcal{M}_{11}$. Observe that ξ_1^2 and ξ_0^2 are both traceless, so their wedge product $\xi_1^2 \wedge \xi_0^2$ is a scalar multiple of $(1;1;1) \in \mathcal{O}_{\bar{K}}^3$. (Here we identify $\Lambda^2 \mathcal{O}_{\bar{K}}^3$ with $\mathcal{O}_{\bar{K}}^3$ via the trace pairing and standard orientation, so that the wedge product is given by the same formula as the cross product on $\mathbb{R}^3$.) Let $\{\xi_0^2, \alpha\}$ be an $\mathcal{O}_{\bar{K}}$-basis for the traceless plane in $\mathcal{O}_{\bar{K}}^3$. Write

$$\xi_1^2 = c_0 \xi_0^2 + c_1 \alpha.$$

The coefficient c_1 controls how far ξ_1 deviates from ξ_0 and thus the satisfaction of $\mathcal{N}_{11}$:

$$\begin{aligned} \mathcal{N}_{11} &\iff \text{All coordinates of } \quad \bar{\omega}_C^{-1} \cdot \xi_1^2 \quad \text{are congruent} \mod \pi^{n_{11}} \\ &\iff \text{All coordinates of } \quad c_1 \bar{\omega}_C^{-1} \alpha \quad \text{are congruent} \mod \pi^{n_{11}} \end{aligned}$$

We claim that the element $\bar{\omega}_C^{-1} \alpha \in \mathcal{O}_{\bar{K}}^3$ does *not* have all coordinates congruent mod $\mathfrak{m}_{\bar{K}}$:

- If $\bar{s} = 0$, then $\bar{\omega}_C$ is a unit so this is equivalent to α and ξ_0^2 being linearly independent modulo $\mathfrak{m}_{\bar{K}}$;
- If $\bar{s} > 0$, then $\bar{\omega}_C \sim (1; \pi^{\bar{s}}; \pi^{\bar{s}})$, so $\xi_0^{(K)}$ has positive valuation. Hence $\alpha^{(K)}$ and $(\bar{\omega}_C \alpha)^{(K)}$ are units, while $(\bar{\omega}_C \alpha)^{(Q)}$ is not.

Consequently

$$\mathcal{N}_{11} \iff c_1 \equiv 0 \mod \pi^{n_{11}} \tag{143}$$

$$\iff \xi_1^2 \wedge \xi_0^2 \equiv 0 \mod \pi^{n_{11}}. \tag{144}$$

Now (144) is advantageous, because the wedge product $\xi_1^2 \wedge \xi_0^2$ has all its coordinates equal, so

we can test $\mathcal{N}_{11}$ by looking at any one of them. We have (coordinate indices mod 3)

$$\begin{aligned}\left(\xi_1^2 \wedge \xi_0^2\right)^{(i)} &= {\xi_1^{(i+1)}}^2 {\xi_0^{(i-1)}}^2 - {\xi_1^{(i-1)}}^2 {\xi_0^{(i+1)}}^2 \\ &= \left(\xi_1^{(i+1)}\xi_0^{(i-1)} - \xi_1^{(i-1)}\xi_0^{(i+1)}\right)\left(\xi_1^{(i+1)}\xi_0^{(i-1)} + \xi_1^{(i-1)}\xi_0^{(i+1)}\right)\end{aligned}$$

and the two factors are congruent modulo 2, so, since $n_{11} \leq 2e$,

$$\mathcal{N}_{11} \iff (\xi_1 \wedge \xi_0)^{(i)} \equiv 0 \mod \pi^{n_{11}/2}. \tag{145}$$

We now examine this for each coordinate i in turn, and for each splitting type.

Unramified. We first dispose of the case $h_1 = 1$. Here the conic is tiny, and by Lemma 19.10, all solutions ξ_1 satisfy

$$\begin{aligned}\xi_1^{\odot} &\equiv \xi_0^{\odot} \mod \pi^e \\ \xi_1 &\equiv \xi_0 \mod \left(\pi^{e+1/2}; \pi^e; \pi^e\right) \\ \xi_1^2 &\equiv \xi_0^2 \mod \left(\pi^{2e+1}; \pi^{2e}; \pi^{2e}\right).\end{aligned}$$

Since we are assuming $n_{11} \leq 2e$, we find that $\mathcal{N}_{11}$ is automatic, and $n^{\odot} \leq e$ may be chosen at will.

Now assume that $h_1 = 0$. Here $\delta^{\odot} \in \mathcal{O}_R^{\times}$ and $\xi_0, \xi_1 \in \sqrt{\delta^{\odot}}\mathcal{O}_R$ are $\mathcal{O}_{\bar{K}}$-primitive. We scale ξ_1 by $\mathcal{O}_K^{\times}$ to be as close to ξ_0 as possible. Then $k = v(\xi_1 - \xi_0)$ is an integer, and

$$\xi_0 \quad \text{and} \quad \frac{\xi_1 - \xi_0}{\pi^k}$$

are linearly independent elements of $\sqrt{\delta^{\odot}}\mathcal{O}_R$. In particular, their wedge product is primitive, so

$$v(\xi_0 \wedge \xi_1) = k.$$

Hence

$$\begin{aligned}\mathcal{N}_{11} &\iff k \geq \frac{n_{11}}{2} \\ &\iff k \geq \left\lceil \frac{n_{11}}{2} \right\rceil \\ &\iff \xi_1 \equiv \xi_0 \mod \pi^{\lceil n_{11}/2 \rceil} \\ &\iff \xi_1^{\odot} \equiv \xi_0^{\odot} \mod \pi^{\lceil n_{11}/2 \rceil},\end{aligned}$$

as desired.

Splitting type (1^3)**.** Scale $\xi_1 \in \bar{\zeta}_3^{-h_1}\sqrt{\delta^{\odot}}\mathcal{O}_R^{\times}$ to be as close to ξ_0 as possible, and consider the valuation $k = v(\xi_1 - \xi_0) \in \frac{1}{3}\mathbb{Z}$. If $k \geq e$, then both $\mathcal{N}_{11}$ and its claimed transformation are easily seen to hold, so assume that $k < e$. Then:

- We cannot have $k \in \mathbb{Z}$, for then rescaling ξ_1 would bring it closer to ξ_0.
- If $k \in \mathbb{Z} + h_1/3$, then $v(\xi_1^2 - \xi_0^2) = 2k \in \mathbb{Z} - h_1/3$, and $\xi_1^2 - \xi_0^2$ has its first-order term a multiple of

$$\begin{aligned}&\left(\bar{\zeta}_3^{-h_1}\sqrt{\delta^{\odot}}\right)^2 \cdot \pi_R^{2k} \\ &= \bar{\zeta}_3^{h_1}\delta^{\odot} \cdot \pi^{2k}\bar{\zeta}_3^{-h_1} \\ &= \delta^{\odot}\pi^{2k},\end{aligned}$$

  which has trace $\sim \pi^{2k}$, contradicting the constraint that both ξ_1^2 and ξ_0^2 are traceless.

Hence $k \in \mathbb{Z} - h_1/3$. Note that

$$v(\xi_1 \wedge \xi_0) = v\big((\xi_1 - \xi_0) \wedge \xi_0\big) = k,$$

since the leading terms of ξ_0 and $\xi_1 - \xi_0$ are multiples of different powers of ζ_3. So

$$\begin{aligned}
\mathcal{N}_{11} &\iff k \geq n_{11}/2 \\
&\iff k \geq -\frac{h_1}{3} + \left\lceil \frac{n_{11}}{2} - \frac{h_1}{3} \right\rceil - r, \quad \text{any } r \text{ in the interval } [0,1) \\
&\iff \xi_1 \equiv \xi_0 \mod \pi^{-\frac{h_1}{3} + \lceil \frac{n_{11}}{2} - \frac{h_1}{3} \rceil - r} \\
&\iff \xi_1^{\odot} \equiv \xi_0^{\odot} \mod \pi^{\frac{1}{3} + \lceil \frac{n_{11}}{2} - \frac{h_1}{3} \rceil - r}.
\end{aligned}$$

We take $r = 1/3$ to get the claimed

$$n^{\odot} = \left\lceil \frac{n_{11}}{2} - \frac{h_1}{3} \right\rceil.$$

■

20 Boxgroups

If $\mathcal{N}_{11}$ is strongly active, then

$$\beta = \frac{\xi_1^2}{\omega_C}$$

is a unit. By Lemma 18.4, the solutions to $\mathfrak{P}$ arise from the β that lie in the box

$$x + y\pi^{n_{11}-s}\theta_1 + z\pi^{m_{11}}\theta_2, \quad x \in \pi^{-2a_1+s}K, \quad y, z \in \mathcal{O}_K.$$

Necessarily $-2a_1 + s \in \mathbb{Z}$ and $x \in \mathcal{O}_K^{\times}$. Also, $[\delta] = [\beta] \in H^1$. So the support of δ is bound up with the H^1-classes of units in various boxes. Certain boxes have pride of place: those for which the corresponding subset of H^1 is a group, which we will call a *boxgroup*.

In this section, our aim is to define certain subgroups of H^1. We fix the resolvent data. We do not fix the discrete data, but we will reference the transformation $\gamma_{1,0}$ of the conic that occurs in Lemma 19.3 when $L \cong K \times R$ is the algebra for $\delta \in \mathcal{L}_0$ and m_{11} is large enough.

20.1 Signatures

Recall that in Lemma 16.1, we filtered H^1 by level spaces $\mathcal{L}_0 \supset \mathcal{L}_1 \supset \cdots \supset \mathcal{L}_{e'}$, where

$$e' = \begin{cases} e, & R \text{ unramified} \\ 2e, & R \text{ ramified.} \end{cases}$$

We would like to define some additional subgroups of H^1. We use the following notion.

Definition 20.1. If $S \subseteq H^1$ is a subgroup, define the *signature* of S to be the sequence of $e'+2$ subgroups

$$S_i = \frac{S \cap \mathcal{L}_i}{S \cap \mathcal{L}_{i+1}} \subseteq \mathcal{L}_i/\mathcal{L}_{i+1}, \quad -1 \le i \le e.$$

The following subgroups $S_i \subseteq \mathcal{L}_i/\mathcal{L}_{i+1}$ will occur frequently and will be given names:

- 0 denotes the zero subgroup $\mathcal{L}_{i+1}/\mathcal{L}_{i+1}$;
- $\star$ denotes the entire group $\mathcal{L}_i/\mathcal{L}_{i+1}$;
- $\top$, in unramified resolvent for $0 \le i < e$, denotes the order-q subgroup

$$\top = \{[1 + a\pi^{2i+1}\theta_1 : a \in \mathcal{O}_K]\};$$

Thus, for instance, $\mathcal{L}_i$ for $0 \le i \le e'$ has signature $0.0^i\star^{e'-i}.\star$. We separate the first and last terms of a signature by periods, because they carry less information than the other elements in general. In splitting types 3 and 1^3, we can omit these terms.

Moreover, $\mathcal{L}_i$ is the only subgroup with its signature. In general, however, the signature does not uniquely determine the subgroup, though it does determine the *size* of the subgroup, since

$$|S| = \prod_i |S_i|.$$

Note also that if S has signature $S_{-1}S_0 \dots S_{e'-1}S_e$, then $S^\perp$ has signature $S_e^\perp S_{e'-1}^\perp \dots S_0^\perp S_{-1}^\perp$, since the Tate pairing on H^1 induces a perfect pairing between $\mathcal{L}_i/\mathcal{L}_{i+1}$ and $\mathcal{L}_{e'-i-1}/\mathcal{L}_{e'-i}$.

In this section, our aim will be to define a family of *boxgroups* in terms of which the ring totals will be written. These boxgroups will depend on the resolvent data alone. In the unramified splitting types they will have signature

$$0.0^{\ell_0}\top^{\ell_1}\star^{\ell_2}.\star, \quad \sum_i \ell_i = e$$

and will be denoted by $T(\ell_0, \ell_1, \ell_2)$. In splitting type 1^3 they will have signatures

$$0.(00)^{\ell_0}(0\star)^{\ell_1}(\star\star)^{\ell_2}.\star \quad \text{and} \quad 0.(00)^{\ell_0}(\star 0)^{\ell_1}(\star\star)^{\ell_2}.\star, \quad \sum_i \ell_i = e$$

and will be denoted by $T_{-1}(\ell_0, \ell_1, \ell_2)$ and $T_1(\ell_0, \ell_1, \ell_2)$ respectively.

20.2 Boxgroups in unramified splitting type

Lemma 20.2. *Let $m, n \in \mathbb{N}^+ \cup \{\infty\}$, $m \geq n > 0$. Let $B_{\theta_1}(m, n)$ be the box*

$$B_{\theta_1}(m, n) = \{\pi c_0 + \pi^n c_1\theta_1 + \pi^m c_2\theta_2 : c_i \in \mathcal{O}_K\}.$$

(a) For every $\xi \in 1 + B_{\theta_1(m,n)}$,

$$B_{\theta_1}(m, n) = \xi B_{\xi^{-1}\theta_1}(m, n) \tag{146}$$

$$1 + B_{\theta_1}(m, n) = \xi(1 + B_{\xi^{-1}\theta_1}(m, n)). \tag{147}$$

(b) If

$$m \leq 2n + s,$$

then $B_{\theta_1}(m, n)$ is closed under multiplication and the translate $1 + B_{\theta_1}(m, n)$ is a group under multiplication.

Proof. (a) Since $\xi \equiv 1 \bmod \pi$, we can take $\xi^{-1}\theta_2$ in the role of θ_2 for defining $\xi B_{\xi^{-1}\theta_1}(m, n)$, which is a lattice with basis $[\pi^n\xi, \pi^n\theta_1, \pi^m\theta_2]$, all of which are contained in $B_{\theta_1}(m, n)$. This proves the reverse inclusion of (146), and equality follows by comparing volumes. To get (147), we

add ξ to both sides and use $\xi - 1 \in B_{\theta_1}(m,n)$ to simplify the left-hand side.

(b) Observe that $B_{\theta_1}(m,n)$ is a lattice with basis $[\pi^n, \pi^n\theta_1, \pi^m\theta_2]$. Since $m \geq n$, the only product that does not clearly lie in the lattice is $(\pi^n\theta_1)^2$, whose 1- and θ_1-components are divisible by π^{2n}, and whose θ_2-component is divisible by π^{2n+s}. Since $m \leq 2n+s$, this product lies in the lattice.

Thus $B_{\theta_1}(m,n)$ is closed under multiplication and so is $1 + B_{\theta_1}(m,n)$. To show the existence of inverses, simply note that

$$\frac{1}{1+\xi} = 1 - \xi + \xi^2 - \cdots$$

converges to an element of $1 + B_{\theta_1}(m,n)$ for every $\xi \in B_{\theta_1}(m,n)$.

■

Lemma 20.3. *Let*

$$\square_C = \min\{2\ell(\hat{\omega}_C) + 1, e\}$$

be the squareness of the conic for $\delta = 1$; put $\square_C = 0$ if $[\hat{\omega}_C] \notin \mathcal{L}_0$ (i.e. s is odd).

If θ_1 is translated by a suitable element of $\mathcal{O}_K$ and scaled by a suitable element of $\mathcal{O}_K^\times$ (neither of which change the associated resolvent C), then there is an $\eta \in \mathcal{O}_R$ such that

$$\eta^2 \equiv \theta_1 \mod \pi^{s+\square_C} \tag{148}$$

and

$$\eta \in \left\langle 1, \theta_1, \pi^{\lceil \frac{s}{2} \rceil}\theta_2, 2\theta_2 \right\rangle. \tag{149}$$

Proof. If s is odd, then we can scale and translate θ_1 so that

$$\theta_1 \equiv (1;0;0) \mod \pi^s.$$

Then $\eta = \theta_1$ satisfies the desired conditions.

If s is even, then by definition of $\square_C$, there is a linear form λ such that

$$\operatorname{tr}(1^{\odot}\xi^{\odot 2}) \equiv c \cdot \lambda(\xi^{\odot})^2 \mod \pi^{\square_C}$$

as functions of $\xi^{\odot} \in \mathcal{O}_R$. Here $1^{\odot}$, the transform of $\delta = 1$ under Lemma 19.3, is a unit whose class in H^1 is $[\hat{\omega}_C]$; for concreteness, we may take

$$1^{\odot} = \frac{\hat{\omega}_C}{(\pi^s; 1; 1)}.$$

Since $\hat{\omega}_C$ is traceless, the conic has a distinguished basepoint, namely $\xi'_0 = [\pi^{s/2}; 1; 1]$. Pick a $\xi' = \xi'_1$ in the kernel of λ that does *not* lie in the same 1-pixel as the basepoint. We claim that the choice

$$\eta = (1; \pi^{s/2}; \pi^{s/2})\xi'_1$$

fulfills the conditions.

The θ_2-coefficient of η'^2 is given by

$$\operatorname{tr}(\omega_C \eta^2) = \pi^s \operatorname{tr}(1^{\odot}\xi_1'^2) \equiv \pi^s \lambda(\xi'_1) = 0 \mod \pi^{s+\square_C}.$$

Hence there are $a, b \in \mathcal{O}_K$ such that

$$\eta^2 \equiv a + b\theta_1 \mod \pi^{s+\square_C}.$$

We claim that $\pi \nmid b$, which makes it possible to replace θ_1 by $a + b\theta_1$. Suppose not. If $s = 0$, we get $\xi'_1 \equiv \xi'_0$ modulo π, contrary to hypothesis. If $s > 0$, we get $\pi | a$ so $\pi | (\xi'_1)^{(K)}$; we also know that $\pi | (\xi'_0)^{(K)}$. But $1^{\odot}$ is a unit, so λ' is a perfect linear functional, and its kernel in $\mathbb{P}^2(k_K)$ intersects the line $(\xi')^{(K)} \equiv 0$ in only one 1-pixel, a contradiction.

As for (149), it can be rewritten as

$$v_K(\eta^{(2)} - \eta^{(3)}) \geq \min\left\{\frac{s}{2}, e\right\}.$$

To prove this, observe that

$$\left(\eta^{(2)} - \eta^{(3)}\right)\left(\eta^{(2)} + \eta^{(3)}\right) = (\eta^{(2)})^2 - (\eta^{(3)})^2 \equiv \theta_1^{(2)} - \theta_1^{(3)} \equiv 0 \mod \pi^s,$$

with the two factors on the left-hand side congruent modulo $2 \sim \pi^e$. ■

Lemma 20.4. *Let $0 < n \leq m \leq 2e$ be integers such that*

$$m \leq 2n + s \qquad \textit{(the gray-red inequality)} \tag{150}$$

$$m \leq n + \square_C + s \qquad \textit{(the gray-green inequality)} \tag{151}$$

$$m \leq e + \frac{n + s + 1}{2} \qquad \textit{(the gray-blue inequality).} \tag{152}$$

Then the projection $[1 + B_{\theta_1}(m, n)]$ of $1 + B_{\theta_1}(m, n)$ onto H^1 is a subgroup of signature

$$0.0^{\ell_0}\top^{\ell_1}\star^{\ell_2}.\star$$

where

$$\ell_0 = \left\lfloor \frac{n}{2} \right\rfloor$$
$$\ell_1 = \left\lfloor \frac{m}{2} \right\rfloor - \left\lfloor \frac{n}{2} \right\rfloor$$
$$\ell_2 = e - \left\lfloor \frac{m}{2} \right\rfloor.$$

Proof. The gray-red inequality (150) ensures that the projection $T = [1 + B_{\theta_1}(m, n)]$ is a subgroup. It is clear that

$$\mathcal{L}_{\lfloor \frac{n}{2} \rfloor} \subseteq T \subseteq \mathcal{L}_{\lfloor \frac{m}{2} \rfloor},$$

so the signature of T has the shape $0.0^{\ell_0}?^{\ell_1}\star^{\ell_2}.\star$. Those middle ℓ_1 components of the signature are at least $\top$, because for $i \geq \lfloor n/2 \rfloor$ and for all $a \in K$, we have

$$[1 + a\pi^{2i+1}\theta_1] \in T.$$

Thus the signature is at least the one claimed.

To prove that equality occurs, we fix $m \leq 2e$ and proceed by downward induction on n. The base case $n = m$ is clear since $T = \mathcal{L}_{\lfloor \frac{m}{2} \rfloor}$. When moving from $n+1$ to n, note that $|T|$ can grow by at most a factor of

$$[1 + B(m,n) : (1 + B(m,n+1))(1 + \pi^n \mathcal{O}_K)] = q.$$

If n is odd, there is nothing to prove, as we claim that $|T|$ actually grows by a factor of q. If n is even, we claim that T does not change. It suffices to prove that each of the q cosets in

$$\frac{(1 + B(m,n))}{(1 + B(m,n+1))(1 + \pi^n \mathcal{O}_K)}$$

contains a square. For $c \in \mathcal{O}_K$, consider

$$(1 + \pi^{\frac{n}{2}} c\eta)^2 = 1 + 2\pi^{\frac{n}{2}} c\eta + \pi^n c^2 \eta^2.$$

The last term is $\pi^n c^2 \theta_1$ up to an error in $\pi^{n+s+\square_C}\mathcal{O}_R$, which is in $\pi^m \mathcal{O}_R$ by the gray-green inequality. We claim that the cross term $2\pi^{n/2} c\eta$ lies in $B(m, n+1)$ also. If s is odd, this is trivial since we took $\eta = \theta_1$. Otherwise, we have

$$2\pi^{n/2}\eta \in 2\pi^{n/2} \left\langle 1, \theta_1, \pi^{s/2}\theta_2, 2\theta_2 \right\rangle = B_{\theta_1}\left(e + \frac{n}{2} + \min\left\{\frac{s}{2}, e\right\}, e + \frac{n}{2}\right)$$

We get the needed inequality

$$e + \frac{n}{2} + \frac{s}{2} \geq m$$

from the gray-blue inequality, the difference of whose sides lies in $\mathbb{Z} + 1/2$ by parity considerations.

So we have found a square in the coset $1 + \pi^n c^2 \theta_1 + B(m, n+1) = (1 + \pi^n c^2 \theta_1)(1 + B(m, n+1))$, as desired. ■

As a corollary, we have:

Lemma 20.5. *For every triple (ℓ_0, ℓ_1, ℓ_2) of nonnegative integers satisfying*

$$\ell_0 + \ell_1 + \ell_2 = e \tag{153}$$

$$\ell_1 \leq \ell_0 + \frac{s}{2} + 1 \qquad (\textit{the gray-red inequality}) \tag{154}$$

$$\ell_1 \leq \frac{s + \square_C + 1}{2} \qquad (\textit{the gray-green inequality}) \tag{155}$$

$$\ell_1 \leq \ell_2 + \frac{s}{2} + 1, \qquad (\textit{the gray-blue inequality}) \tag{156}$$

there is a boxgroup $T(\ell_0, \ell_1, \ell_2) \subseteq H^1$ *of signature* $0.0^{\ell_0} \top^{\ell_1} \star^{\ell_2} . \star$. *such that, if m, n are integers satisfying the conditions of Lemma 20.4, then*

$$[1 + B_{\theta_1}(m, n)] = T\left(\left\lfloor \frac{n}{2} \right\rfloor, \left\lfloor \frac{m}{2} \right\rfloor - \left\lfloor \frac{n}{2} \right\rfloor, e - \left\lfloor \frac{m}{2} \right\rfloor\right).$$

Proof. If $\ell_1 = 0$, take $T(\ell_0, 0, \ell_2) = \mathcal{L}_{\ell_0}$, the unique subgroup with the correct signature.

Otherwise, let $m = 2\ell_0 + 2\ell_1$, $n = 2\ell_0 + 1$ in the preceding lemma. The transformation of the gray-red, gray-green, and gray-blue conditions is routine.

For the last claim, note that decreasing m or increasing n can only make the conditions of Lemma 20.4 truer, with the exception of the condition $m \geq n$. If $\lfloor m/2 \rfloor = \lfloor n/2 \rfloor$, then clearly $[1 + B_{\theta_1}(m, n)] = \mathcal{L}_{\lfloor m/2 \rfloor}$, so we can assume that

$$n \leq 2\left\lfloor \frac{n}{2} \right\rfloor + 1 < 2\left\lfloor \frac{m}{2} \right\rfloor \leq m.$$

Clearly

$$[1 + B_{\theta_1}(m, n)] \supseteq \left[1 + B_{\theta_1}\left(2\left\lfloor \frac{m}{2} \right\rfloor, n\right)\right],$$

but both sides have the same signature, so equality holds. Likewise,

$$\left[1+B_{\theta_1}\left(2\left\lfloor\frac{m}{2}\right\rfloor,n\right)\right]\subseteq\left[1+B_{\theta_1}\left(2\left\lfloor\frac{m}{2}\right\rfloor,2\left\lfloor\frac{n}{2}\right\rfloor+1\right)\right]=T\left(\left\lfloor\frac{n}{2}\right\rfloor,\left\lfloor\frac{m}{2}\right\rfloor-\left\lfloor\frac{n}{2}\right\rfloor,e-\left\lfloor\frac{m}{2}\right\rfloor\right),$$

but both sides have the same signature, so equality holds. ■

20.2.1 Supplementary boxgroups

As thus defined, all boxgroups T satisfy $\mathcal{L}_e \subseteq T \subseteq \mathcal{L}_0$. Groups not satisfying these inclusions occur will be denoted as follows.

If $s > 0$, so that a distinguished splitting $R \cong K \times Q$ exists, consider the image $\iota(K^\times)$ of the map

$$\begin{aligned}\iota\colon K^\times/(K^\times)^2 &\to H^1\\ a &\mapsto [(a;1)] = [(1;a)].\end{aligned}$$

We find that $\iota(K^\times)$ has signature

$$\top.\top^e.\top$$

where the middle e-many $\top$'s denote the usual subgroups

$$\top_i = \{1+\pi^{2i+1}a\theta_1\} = \{1+\pi^{2i+1}a(1;0)\} \subseteq \mathcal{L}_i/\mathcal{L}_{i+1}$$

and where the initial $\top_{-1} = \{[1],[(1;\pi)]\} \subseteq H^1/\mathcal{L}_0$ and the final $\top_e = \{1+4a : a \in \mathcal{O}_K\} \subseteq \mathcal{L}_e$ have size 2 and $|H^0|/2$ respectively. In particular,

$$|\iota(K^\times)| = |H^0|q^e = \sqrt{|H^1|}.$$

From the explicit description in terms of the Hilbert pairing, we find that $\iota(K^\times)$ is isotropic and hence maximally isotropic for $\langle\bullet,\bullet\rangle$.

The group $\iota(K^\times)$ is always important, but it does not behave well with respect to boxgroups unless $s > 2e$, in which case we give it the name $T(\emptyset, e, \emptyset)$.

If $s > 2\ell_1$, we let

$$T(e-\ell_1, \ell_1, \emptyset) = \iota(K^\times) \cap \mathcal{L}_{\ell_{e-\ell_1}} = \{[(a;1)] \in H^1 : a \equiv 1 \mod \pi^{2e-2\ell_1+1}\}$$

$$T(\emptyset, \ell_1, e-\ell_1) = \iota(K^\times) \cdot \mathcal{L}_{\ell_1} = \{[(a;\alpha)] \in H^1 : \alpha \equiv 1 \mod \pi^{2\ell_1+1}\}.$$

Their signatures are, respectively, $0.0^{\ell_0}\top^{e-\ell_0}.\top$ and $\top.\top^{\ell_1}x^{e-\ell_1}.x$.

The restrictions on s ensure that these boxgroups satisfy such natural relations as

$$T(e-\ell_1, \ell_1, \emptyset) \cdot \mathcal{L}_e = T(e-\ell_1, \ell_1, 0)$$

$$T(\emptyset, \ell_1, e-\ell_1) \cap \mathcal{L}_0 = T(0, \ell_1, e-\ell_1),$$

which we will often use without comment.

Finally, in all cases, we let

$$T(e, \emptyset, \emptyset) = \{1\}$$

$$T(\emptyset, \emptyset, e) = H^1.$$

It will turn out that $T(\ell_0, \ell_1, \ell_2)$ and $T(\ell_2, \ell_1, \ell_0)$ are orthogonal complements whenever both are defined (Lemma 21.13). Actually, this is simple to prove in the case that one of ℓ_0, ℓ_1, ℓ_2 is the symbol $\emptyset$. The sizes of these groups follow immediately from their signatures:

Lemma 20.6. *If $T(\ell_0, \ell_1, \ell_2)$ is defined and $\ell_1 \neq \emptyset$, then*

$$|T(\ell_0, \ell_1, \ell_2)| = |H^0| q^{e+\ell_2-\ell_0},$$

where if $\emptyset$ occurs as either ℓ_0 or ℓ_2, it must be replaced by $-1/[k_K : \mathbb{F}_2] = \log_q(1/2)$.

20.3 Boxgroups in splitting type 1^3

Let $h \in \{1, -1\}$ be the integer such that

$$b_1 \in \mathbb{Z} + \frac{h}{3}, \quad \theta_1 \in \bar{\zeta}_3^h \mathcal{O}_R^\times, \quad \theta_2 \in \bar{\zeta}_3^{-h} \mathcal{O}_R^\times.$$

Note the tight connection with the h_i of Lemma 19.3. Namely, if $\mathcal{N}_{11}$ is strongly active, then β is a unit in Lemma 18.4, from which we get $m_{11} \in \mathbb{Z}$, $a_1 \in \mathbb{Z}$, and $h_1 = h$.

Let

$$\square_C = \min\left\{2\left\lfloor \frac{\ell(\hat{\omega}_C)}{2} \right\rfloor + 1, e\right\}$$

be the squareness of the conic

$$\mathcal{M}(\xi^\odot) = \lambda^\diamondsuit(1^\odot {\xi^\odot}^2)$$

that occurs for $\delta = 1$. Note that there is just one conic, with $[1^\odot] = [\hat{\omega}_C]$, although we turn our attention to the part where $\xi^\odot \sim 1$ resp. $\xi^\odot \sim \pi_R^2$ according as $h_i = 1$ resp. -1. Then

Lemma 20.7. *Fix a resolvent C. If θ_1 is translated and scaled appropriately, there is an $\eta \in \bar{\zeta}_3^{-h} \mathcal{O}_R^\times$ such that*

$$\eta^2 \equiv \theta_1 \mod \pi^{\square_C - \frac{2h}{3}}.$$

Proof. By Lemma 19.14, $\mathcal{M}$ has squareness $\square_C$, which means that there is a linear form λ and a scalar $c \in \mathcal{O}_K^\times$ such that

$$\mathcal{M}(\xi^\odot) \equiv c \cdot \lambda(\xi^\odot)^2 \mod \pi^{\square_C}$$

The zero locus of $\mathcal{M}$ modulo π, or equivalently of λ modulo π, consists of $(q+1)$-many 1-pixels, q of which consist of units and the remaining one of elements $\xi^\odot \sim \pi_R^2$. If we were searching for a $\xi^\odot = \xi_1^\odot$ with $h_1 = h$, we would have $v(\xi^\odot) = \frac{1-h}{3}$. We pick a $\xi^\odot$ of the *other* valuation $v(\xi^\odot) = \frac{1+h}{3}$ which lies in the kernel of λ, ensuring that

$$\mathcal{M}(\xi^\odot) \equiv 0 \mod \pi^{\square_C}.$$

Then take

$$\eta = \pi^{2b_1 - \frac{h}{3}} \sqrt{\frac{1^{\odot}}{\hat{\omega}_C \diamondsuit}} \xi^{\odot} \in \bar{\zeta}_3^{-h} R.$$

(See pp. XI.304–05 for motivation and details.) Note that

$$\begin{aligned} \operatorname{coef}_{\theta_2}(\eta^2) &= \pi^{-4b_1 - s + 2(2b_1 - \frac{h}{3})} \mathcal{M}\left(\xi^{\odot 2}\right) \\ &\equiv 0 \mod \pi^{\square_C - \frac{2h}{3}} \end{aligned}$$

Hence there are

$$a \in \begin{cases} \sqrt[3]{\pi^2}\mathcal{O}_K, & h = 1 \\ \sqrt[3]{\pi}\mathcal{O}_K, & h = -1 \end{cases}$$

and $b \in \mathcal{O}_K$ such that

$$\eta^2 \equiv a + b\theta_1 \mod \pi^{\square_C - \frac{2h}{3}}.$$

Since η is a unit, we must have $\pi \nmid b$, so θ_1 can be replaced by $a + b\theta_1$. ■

The following lemma is proved just like Lemma 20.2.

Lemma 20.8. *If m and n satisfy*

$$0 < n < m < 2e, \quad m \in \mathbb{Z} - \frac{h}{3}, \quad n \in \mathbb{Z} + \frac{h}{3},$$

Let $B_{\theta_1}(m,n)$ be the box

$$B_{\theta_1}(m,n) = \{\pi c_0 + \pi^n c_1 \theta_1 + \pi^m c_2 \theta_2 : c_0, c_1, c_2 \in \mathcal{O}_K\} \subseteq \mathcal{O}_R.$$

(a) For every $\xi \in 1 + B_{\theta_1(m,n)}$,

$$B_{\theta_1}(m,n) = \xi B_{\xi^{-1}\theta_1}(m,n) \tag{157}$$

$$1 + B_{\theta_1}(m,n) = \xi(1 + B_{\xi^{-1}\theta_1}(m,n)). \tag{158}$$

(*b*) *If*

$$m \leq 2n,$$

then $B_{\theta_1}(m,n)$ is closed under multiplication and the translate $1+B_{\theta_1}(m,n)$ is a group under multiplication.

Our goal is to study the projection of $1+B_{\theta_1}(m,n)$ onto H^1. The following yields the conditions under which a useful group is formed thereby:

Lemma 20.9. *Let $0<n<m\leq 2e$ be rational numbers with $m\in\mathbb{Z}-\frac{h}{3}, n\in\mathbb{Z}+\frac{h}{3}$. Assume that*

$$m \leq 2n \qquad (\textit{the gray-red inequality}) \tag{159}$$

$$m \leq n+\square_C-\frac{2h}{3} \qquad (\textit{the gray-green inequality}) \tag{160}$$

$$m \leq \frac{n+1}{2}+e \qquad (\textit{the gray-blue inequality}). \tag{161}$$

Write

$$m^{\triangle}=m-\frac{2h}{3}\in\mathbb{Z}, \quad n^{\triangle}=n+\frac{2h}{3}\in\mathbb{Z}.$$

Then the projection $T=[1+B_{\theta_1}(m,n)]$ of $1+B_{\theta_1}(m,n)$ onto H^1 is a subgroup of signature

$$.(00)^{\ell_0}(\star 0)^{\ell_1}(\star\star)^{\ell_2}.$$

or

$$.(00)^{\ell_0}(0\star)^{\ell_1}(\star\star)^{\ell_2}.$$

for $h=1$ and $h=-1$ respectively, where

$$\ell_0=\left\lfloor\frac{n^{\triangle}}{2}\right\rfloor$$
$$\ell_1=\left\lfloor\frac{m^{\triangle}}{2}\right\rfloor-\left\lfloor\frac{n^{\triangle}}{2}\right\rfloor$$
$$\ell_2=e-\left\lfloor\frac{m^{\triangle}}{2}\right\rfloor$$

except for the case $h = 1$, $m^{\triangle} = 2i + 1$, $n^{\triangle} = 2i + 2$ *(*$i \in \mathbb{Z}$*), where* $T = \mathcal{L}_{2i+1}$.

Proof. Suppose $h = 1$. For $a \in \mathcal{O}_K^{\times}$, there are elements in T of the form

$$[1 + a\pi^{2i+\frac{1}{3}}\theta_1], \quad i \geq \left\lceil \frac{3n-1}{6} \right\rceil = \left\lfloor \frac{n^{\triangle}}{2} \right\rfloor$$
$$[1 + a\pi^{2i+\frac{5}{3}}\theta_2], \quad i \geq \left\lceil \frac{3m-5}{6} \right\rceil = \left\lfloor \frac{m^{\triangle}}{2} \right\rfloor.$$

Likewise, in the case $h = -1$, there are elements in T of the form

$$[1 + a\pi^{2i+\frac{5}{3}}\theta_1], \quad i \geq \left\lceil \frac{3n-5}{6} \right\rceil = \left\lfloor \frac{n^{\triangle}}{2} \right\rfloor$$
$$[1 + a\pi^{2i+\frac{1}{3}}\theta_2], \quad i \geq \left\lceil \frac{3m-1}{6} \right\rceil = \left\lfloor \frac{m^{\triangle}}{2} \right\rfloor.$$

This shows that the signature of T is at least as large as claimed.

To show equality, we fix $m < 2e$ and proceed by downward induction on n. The base case $n = m - 1/3$ (for $h = 1$) or $n = m - 2/3$ (for $h = -1$) is clear since $T = \mathcal{L}_{m^{\triangle}-1}$ or $\mathcal{L}_{2\lfloor m^{\triangle}/2 \rfloor + 1}$ respectively. When moving from $n + 1$ to n, note that $|T|$ can grow by at most a factor of

$$[1 + B(m,n) : (1 + B(m,n+1))(1 + \pi^{\lceil n \rceil}\mathcal{O}_K)] = q.$$

If $n^{\triangle}$ is odd, there is nothing to prove, as we claim that $|T|$ actually grows by a factor of q. If $n^{\triangle}$ is even, we are claiming that T does not change. It suffices to prove that each of the q cosets in

$$\frac{(1 + B(m,n))}{(1 + B(m,n+1))(1 + \pi^{\lceil n \rceil}\mathcal{O}_K)}$$

contains a square. Recall the approximate square root $\eta \in \bar{\zeta}_3^{-h}\mathcal{O}_R^{\times}$ from Lemma 20.7, which satisfies

$$\eta^2 \equiv \theta_1 \mod \pi^{\square_C - \frac{2h}{3}}.$$

For $c \in \mathcal{O}_K$, consider

$$(1 + \pi^{\frac{n}{2}} c\eta)^2 = 1 + 2\pi^{\frac{n}{2}} c\eta + \pi^n c^2 \eta^2. \tag{162}$$

The last term is $\pi^n c^2 \theta_1$ up to an error in $\pi^{n+\square_C - \frac{2h}{3}} \mathcal{O}_R$. To say that this is in $\pi^m \mathcal{O}_R$, we need the inequalities

$$m \leq n + \square_C - \frac{2h}{3} \quad \text{and} \quad m \leq n + e - \frac{2h}{3}.$$

The first of these is (160), and the second follows easily from (159) and (161). We claim that the middle term of (162) lies in $\pi^m \mathcal{O}_R$ also, that is,

$$m \leq \frac{n}{2} + e.$$

This follows from (161) and the fact that $m - n/2 \in \mathbb{Z}$. So we have found a square in the coset $1 + \pi^n c^2 \theta_1 + B(m, n+1) = (1 + \pi^n c^2 \theta_1)(1 + B(m, n+1))$, as desired. ■

As a corollary, just like Lemma 20.5, we get the following:

Lemma 20.10. *For every triple (ℓ_0, ℓ_1, ℓ_2) of nonnegative integers satisfying*

$$\ell_0 + \ell_1 + \ell_2 = e \tag{163}$$

$$\ell_1 \leq \ell_0 \qquad (\textit{the gray-red inequality}) \tag{164}$$

$$\ell_1 \leq \frac{\square_C + 1}{2} - h \qquad (\textit{the gray-green inequality}) \tag{165}$$

$$\ell_1 \leq \ell_2, \qquad (\textit{the gray-blue inequality}) \tag{166}$$

there is a boxgroup $T_h(\ell_0, \ell_1, \ell_2) \subseteq H^1$ *of signature*

$$.(00)^{\ell_0} (\star 0)^{\ell_1} (\star\star)^{\ell_2}.$$

or

$$.(00)^{\ell_0} (0\star)^{\ell_1} (\star\star)^{\ell_2}.$$

for $h = 1$ and $h = -1$ respectively, such that, if m, n are rational numbers satisfying the conditions of Lemma 20.9, then

$$[1 + B_{\theta_1}(m, n)] = T(\ell_0', \ell_1', \ell_2')$$

where $\ell_0', \ell_1', \ell_2'$ are the numbers ℓ_0, ℓ_1, ℓ_2 defined in Lemma 20.9.

Proof. If $\ell_1 = 0$, take $T(\ell_0, 0, \ell_2) = \mathcal{L}_{\ell_0}$. Otherwise, take

$$n^{\triangle} = 2\ell_0 + 1 \in 2\mathbb{Z} + 1, \quad m^{\triangle} = 2e - 2\ell_2 \in 2\mathbb{Z},$$

In other words,

$$n = 2\ell_0 + 1 - \frac{2h}{3}, \quad m = 2e - 2\ell_2 + \frac{2h}{3}.$$

Conditions (164)–(166) immediately imply (159)–(161). Just as in Lemma 20.5, we then argue that increasing m by 1 (resp. decreasing n by 1), if it does not violate (159)–(161), yields a boxgroup of the same signature that is contained in (resp. contains) $T_h(\ell_0, \ell_1, \ell_2)$ and thus must equal $T_h(\ell_0, \ell_1, \ell_2)$. ■

The subscript "h" in $T_h(\ell_0, \ell_1, \ell_2)$ is logically superfluous, because θ_1 is fixed. But it allows the following manipulation. Define

$$T_{-1}(\ell_0, \ell_1, \ell_2) = T_1(\ell_0 + \ell_1, -\ell_1, \ell_1 + \ell_2)$$

for all (ℓ_0, ℓ_1, ℓ_2) for which either side has been defined. Note that $T_1(\ell_0, 0, e - \ell_0) = T_{-1}(\ell_0, 0, e - \ell_0) = \mathcal{L}_{2\ell_0}$ already fulfills this relation, while allowing

$$T_1(\ell_0, -1, e + 1 - \ell_0) = T_{-1}(\ell_0 - 1, 1, e - \ell_0) = \mathcal{L}_{2\ell_0 + 1}$$

saves us the trouble of excluding the case $h = 1$, $m^{\triangle} = 2i + 1$, $n^{\triangle} = 2i + 2$ from Lemma 20.9. We do not use any other boxgroups with negative ℓ_1 within this paper, but in the code we do, converting everything to a T_{-1}.

20.4 The recentering lemma

When θ_1 is nearly a square, we will sometimes be able to assume that it *is* a square, thanks to the following lemma, which we state separately for each splitting type.

Lemma 20.11. *If C is unramified and s is even, then there is an element $\psi_C \in 1 + B_{\theta_1}(\infty, \square_C)$ and $a \in \mathcal{O}_K$, $b \in \mathcal{O}_K^\times$ such that $\theta_1' = a + b\psi_C^{-1}\theta_1 = \eta^2$ is a square in $\mathcal{O}_R$.*

Proof. It is easy to see that tweaking θ_1 by addends in $\mathcal{O}_K$ or multipliers in $\mathcal{O}_K^\times$, which do not change the underlying resolvent ring C, do not affect the truth of the lemma either. We may therefore assume, by Lemma 20.3, that there is an η such that

$$\eta^2 \equiv \theta_1 \mod \pi^{s+\square_C}.$$

In particular, $\eta^2 \equiv \theta_1 \bmod \pi^{2\ell+1}\mathcal{O}_K[\theta_1]$. Let $k = \square_C$. Notice that θ_1' can take all values in the orbit

$$\theta_1' = \frac{a_{11}\theta_1 + a_{12}}{a_{21}\theta_1 + a_{22}} = \frac{a_{12}}{a_{22}} + \frac{(a_{11}a_{22} - a_{12}a_{21})\theta_1}{a_{22}(a_{21}\theta_1 + a_{22})}$$

of θ_1 under the congruence subgroup

$$\Gamma(k) = \left\{ \gamma = \begin{bmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{bmatrix} \in \mathrm{GL}_2(\mathcal{O}_K) : \gamma \equiv \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} \mod \pi^k \right\}.$$

We claim that this orbit is precisely the pixel $\theta_1 + \pi^k\mathcal{O}_K[\theta_1]$. The orbit is clearly contained in this pixel and contains all elements of the form

$$\gamma(\theta_1) = \frac{(1 + a_{11}'\pi^k)\theta_1 + a_{12}'\pi^k}{a_{21}'\pi^k\theta_1 + (1 + a_{22}'\pi^k)} \equiv \theta_1 + \pi^k(a_{12}' + (a_{11}' - a_{22}')\theta_1 + a_{21}'\theta_1^2) \mod \pi^{2k}\mathcal{O}_K[\theta_1].$$

So at least the orbit contains a point in each congruence class mod $\pi^{2k}\mathcal{O}_K[\theta_1]$ in the claimed pixel. But applying general elements of $\Gamma(2k)$ to each of those, we get a point in each congruence class mod $\pi^{4k}\mathcal{O}_K[\theta_1]$, and so on. Hence, the orbit is dense in the pixel, and being compact, it coincides

with the pixel, establishing the desired result. ■

Lemma 20.12. *If R is of splitting type 1^3, there is an element $\psi_C \in 1 + B_{\theta_1}(\infty, \square_C - 2h/3)$ and $a \in \pi^{-h/3}K \cap \mathcal{O}_{\bar{K}}$, $b \in \mathcal{O}_K^\times$ such that $\theta_1' = a + b\psi_C^{-1}\theta_1 = \eta^2$ is a square, $\eta \in \bar{\zeta}_3^{-h}\mathcal{O}_R$.*

Proof. It is easy to see that tweaking θ_1 by addends in $\mathcal{O}_K$ or multipliers in $\mathcal{O}_K^\times$, which do not change the underlying resolvent ring C, do not affect the truth of the lemma either. We may therefore assume, by Lemma 20.7, that there is an η such that

$$\eta^2 \equiv \theta_1 \mod \pi^k$$

where $k = \square_C - 2h/3$. Notice that θ_1' can take all values in the orbit

$$\theta_1' = \frac{a_{11}\theta_1 + a_{12}}{a_{21}\theta_1 + a_{22}} = \frac{a_{12}}{a_{22}} + \frac{(a_{11}a_{22} - a_{12}a_{21})\theta_1}{a_{22}(a_{21}\theta_1 + a_{22})}$$

of θ_1 under the congruence subgroup

$$\Gamma(k) = \left\{ \gamma = \begin{bmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{bmatrix} \in \mathrm{GL}_2(\mathcal{O}_{\bar{K}}) : a_{ij} \in \pi^{\frac{h}{3}(i-j)}K, \gamma \equiv \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} \mod \pi^k \right\}.$$

We claim that this orbit is precisely the pixel

$$\{\theta_1' \in \bar{\zeta}_3^h \mathcal{O}_R^\times : \theta_1' \equiv \theta_1 \mod \pi^k\}.$$

The orbit is clearly contained in this pixel and contains all elements of the form

$$\gamma(\theta_1) = \frac{(1 + a_{11}'\pi^k)\theta_1 + a_{12}'\pi^k}{a_{21}'\pi^k\theta_1 + (1 + a_{22}'\pi^k)} \equiv \theta_1 + \pi^k(a_{12}' + (a_{11}' - a_{22}')\theta_1 + a_{21}'\theta_1^2) \mod \pi^{2k}$$

where the a_{ij}' are integral in the appropriate groups $\pi^{\frac{h}{3}(i-j)-k}K$.

So at least the orbit contains a point in each congruence class mod $\pi^{2k}\mathcal{O}_K[\theta_1]$ in the claimed pixel. But applying general elements of $\Gamma(2k)$ to each of those, we get a point in each congruence

class mod $\pi^{4k}\mathcal{O}_K[\theta_1]$, and so on. Hence, the orbit is dense in the pixel, and being compact, it coincides with the pixel, establishing the desired result. ■

20.5 Charmed cosets

Lemma 20.13. *Let H be a finite 2-torsion group, and let $\varepsilon : H \to \{\pm 1\}$ be a nondegenerate quadratic form over $\mathbb{F}_2$. Let $V \subseteq H$ be a subspace that is* coisotropic; *that is, $V^\perp$ is isotropic, or equivalently, V contains a maximal isotropic subspace. Then:*

(*a*) *There is exactly one coset $\alpha V \subseteq H$ such that*

$$\sum_{\delta \in \alpha V} \varepsilon(\alpha) \neq 0.$$

Indeed, the sum is

$$\pm_\varepsilon \sqrt{|H|},$$

where $\pm_\varepsilon \in \{\pm 1\}$ is an invariant of the quadratic space (V, ε). We call αV the charmed coset *of V.*

(*b*) *On any coset $\beta V^\perp$ inside the charmed coset αV, ε is constant. By contrast, on any coset $\beta V^\perp$ outside the charmed coset, ε is equidistributed.*

Proof. (a) Assume first that V is maximal isotropic. Then $|V| = \sqrt{|H|}$. (If an $\mathbb{F}_2$-space admits a nondegenerate quadratic form, its dimension is even if finite.) On each coset αV, ε looks like a linear form, that is, there is a $\lambda_\alpha \in V^*$ such that

$$\varepsilon(\alpha\beta) = \varepsilon(\alpha) \cdot \lambda_\alpha(\beta).$$

Note that the linear form λ_α is independent of coset representative, so we have a mapping

$$\lambda : H/V \to V^*.$$

If λ takes the same value on two different cosets $\alpha_1 V, \alpha_2 V$, then we see that ε is linear on the union $\alpha_1 V \sqcup \alpha_2 V$. Then the associated bilinear form $\langle , \rangle_\varepsilon$ is isotropic on the space $V \oplus \{0, \alpha_2/\alpha_1\}$, which is too big to be isotropic. So λ is injective. Comparing sizes, we see that λ is surjective also. So there is one coset αV on which ε is identically 1 or -1. This is the charmed coset. On the remaining cosets, the values of ε are those of a nontrivial linear functional on V and hence are equidistributed between 1 and -1.

For a general V, take $N \subseteq V$ maximal isotropic. Every V-coset decomposes into N-cosets, and only the one containing the charmed coset of N will yield a nonzero sum for ε, namely $\pm|V| = \pm\sqrt{|H|}$.

A priori the sign $\pm$ of the sum on the charmed coset depends on both ε and V. But if $N \subseteq V$ are coisotropic, then it is easy to see that N and V yield the same sign. Then, taking $V = H$, we obtain that one sign holds for all coisotropic subspaces.

(b) Take $N \subseteq V$ maximal isotropic. Then the charmed coset αV of V is the one containing a charmed coset αN of N on which $\varepsilon = \pm_\varepsilon 1$ is constant.

If $\beta/\alpha \in V$, then for all $\gamma \in V^\perp$, we have $\langle \alpha\beta, \gamma \rangle = 1$ so

$$\begin{aligned} \varepsilon(\beta\gamma) &= \varepsilon(\beta)\varepsilon(\alpha)\varepsilon(\alpha\gamma)\,\langle \alpha\beta, \gamma \rangle \\ &= \varepsilon(\beta), \end{aligned}$$

since $\alpha, \alpha\gamma \in \alpha N$. By contrast, if $\beta/\alpha \notin V$, there exists $\gamma \in V^\perp$ such that $\langle \alpha\beta, \gamma \rangle = -1$. Then $\varepsilon(\beta\gamma) = -\varepsilon(\beta)$, so ε is nonconstant on $\beta V^\perp$. But $V^\perp$ is isotropic, so ε is a linear form (plus a constant) on $\beta V^\perp$ and is therefore equidistributed.

■

As you might expect, we apply this lemma to the space $H = H^1$ with its quadratic form ε. We will eventually find that $\pm_\varepsilon = 1$ (it is "positively charmed," one might say) though this is not obvious.

Let ε_C be the following translation of ε: for $[\alpha] \in H^1$,

$$\varepsilon_C(\alpha) = \varepsilon\left(\hat{\omega}_C \alpha\right) = \begin{cases} 1, & \operatorname{coef}_{\bar{\theta}_2}(\alpha\xi^2) = 0 \text{ for some } \xi \in R^\times \\ -1, & \text{otherwise.} \end{cases}$$

Note that ε_C is still a quadratic form on H^1 whose associated bilinear form is the Hilbert symbol $\langle \bullet, \bullet \rangle_R$. Note that $\varepsilon_C(1) = 1$. Lemma 19.16 can be interpreted as saying that

$$\heartsuit\diamondsuit\mathcal{L}_{\lfloor e'/2 \rfloor}$$

is charmed for ε_C.

If $V \subseteq H^1$ is a subspace, we let

$$F_V = \mathbf{1}_V$$

be its characteristic function. If V is coisotropic, we denote by $G_{\varepsilon_a, V}$, resp. $G_{\varepsilon_C, V}$ the characteristic function of its charmed coset with respect to one of the quadratic forms $\varepsilon_a, \varepsilon_C$ whose associated bilinear form is the Hilbert pairing. The ε_a will be omitted if clear. The following results will power the computation of Fourier transforms of ring totals, a necessary step in our desired reflection theorems.

Lemma 20.14. *Let V be a subspace of H^1.*

(a)

$$\widehat{F_V} = \frac{|V|}{|H^0|} F_{V^\perp}.$$

(b) If V is coisotropic, then

$$\widehat{G_{\varepsilon_a, V}} = \frac{|V|}{|H^0|} \varepsilon_a(1) \varepsilon_a F_{V^\perp}.$$

(c) If V is coisotropic, then

$$\widehat{\varepsilon_a G_V} = \pm_{\varepsilon_a} q^e \varepsilon_a(1) \varepsilon_a F_V.$$

Proof. Part (a) is a standard property of the Fourier transform. For parts (b) and (c), let $N \subseteq V$ be a maximal isotropic subspace, so

$$V \supseteq N = N^{\perp} \supseteq V^{\perp}.$$

Let βN be the charmed coset of N, so βV is the charmed coset of V.

For (b), we compute

$$\begin{aligned}\widehat{G_V}(\delta) &= \frac{1}{|H^0|} \sum_{\alpha \in V} \langle \alpha\beta, \delta \rangle \\ &= \frac{1}{|H^0|} \langle \beta, \delta \rangle \sum_{\alpha \in V} \langle \alpha, \delta \rangle \\ &= \frac{|V|}{|H^0|} \langle \beta, \delta \rangle \, F_{V^{\perp}}(\delta).\end{aligned}$$

Hence it remains to prove that, for $\delta \in V^{\perp}$,

$$\langle \beta, \delta \rangle = \varepsilon_a(\delta).$$

By the definition of the associated bilinear form,

$$\langle \beta, \delta \rangle = \varepsilon_a(1)\varepsilon_a(\delta)\varepsilon_a(\beta)\varepsilon_a(\delta\beta).$$

But $\varepsilon_a(\beta) = \varepsilon_a(\delta\beta)$ since both arguments lie in the charmed isotropic coset βN. This establishes (b).

For (c), we compute

$$\begin{aligned}\widehat{\varepsilon_a G_V} &= \frac{1}{|H^0|}\sum_{\alpha\in V}\varepsilon_a(\alpha\beta)\,\langle\alpha\beta,\delta\rangle \\ &= \frac{1}{|H^0|}\sum_{\alpha\in V}\varepsilon_a(1)\varepsilon_a(\delta)\varepsilon_a(\alpha\beta\delta) \\ &= \frac{\varepsilon_a(1)\varepsilon_a(\delta)}{|H^0|}\sum_{\alpha\in V}\varepsilon_a(\alpha\beta\delta).\end{aligned}$$

The last sum equals $\pm_{\varepsilon_a}\sqrt{|H^1|}$ if $\beta\delta V$ is charmed, 0 otherwise. But βV is charmed, so the relevant condition is that $\delta\in V$. So

$$\begin{aligned}\widehat{\varepsilon_a G_V} &= \frac{\varepsilon_a(1)\varepsilon_a(\delta)}{|H^0|}\cdot\pm_{\varepsilon_a}\sqrt{|H^1|}F_V(\delta) \\ &= \pm_{\varepsilon_a} q^e\varepsilon_a(1)\varepsilon_a(\delta)F_V(\delta),\end{aligned}$$

as desired. ■

20.6 The projectors

On the space of complex- (or even rational-) valued functions on H^1, we can define certain projectors that divide up the work to be done. First look at the cosets of $\mathcal{L}_0$. Let

$$I = \begin{cases}\mathcal{L}_0\cup(1;\pi;\pi)\mathcal{L}_0, & \bar{s}>0\\ \mathcal{L}_0, & \bar{s}=0\end{cases}$$

be the union $\mathcal{L}_0\cup\alpha\mathcal{L}_0$ of up to two cosets, using the distinguished splitting $R\cong K\times Q$ if $\bar{s}>0$. Let I_0, I_1, I_2 be the restriction operators that restrict the support of a function to $\mathcal{L}_0$, $I\setminus\mathcal{L}_0$, and $H^1\setminus I$, respectively. They are orthogonal idempotents (I_1 and/or I_2 may vanish). Let J_i be the conjugate of I_i under the Fourier transform. Each J_i is convolution by a certain function supported on $\mathcal{L}_{e'}$; J_0 is none other than the *smear operator* $\mathfrak{S}_{e'}$ which will occur below. Since $\mathcal{L}_{e'}\subseteq\mathcal{L}_0$, each I_i commutes with each J_j, so the I_iJ_j form a system of nine orthogonal idempotents. For orderliness of

presentation, we transform all ring answers to a sum of terms each in the image of one idempotent. The Fourier transform interchanges the images of I_iJ_j and I_jJ_i. In splitting type (111), all nine idempotents are nonzero, although I_1J_2 and I_2J_1 will be found to annihilate every ring total. In the remaining splitting types, some of the idempotents vanish, and correspondingly some terms of our answers can be ignored.

Definition 20.15. In unramified splitting types, we define the use of a symbol x as follows, where the ℓ_i are such that the relevant boxgroups are well defined:

- $xF(0,\ell_1,\ell_2) = I_1(F(\emptyset,\ell_1,\ell_2))$, so that

$$F(\emptyset,\ell_1,\ell_2) = F(0,\ell_1,\ell_2) + xF(0,\ell_1,\ell_2).$$

- $xxF(0,0,e) = I_2(F(\emptyset,\emptyset,e))$, so that

$$F(\emptyset,\emptyset,e) = F(0,0,e) + xF(0,0,e) + xxF(0,0,e).$$

- $Fx(\ell_0,\ell_1,0) = 2\cdot J_1(F(\ell_0,\ell_1,\emptyset))$, so that, if there is a distinguished coarse coset,

$$2F(\ell_0,\ell_1,\emptyset) = F(\ell_0,\ell_1,0) + Fx(\ell_0,\ell_1,0).$$

- $Fxx(e,0,0) = |H^0|\cdot J_2(F(e,\emptyset,\emptyset))$, so that

$$|H^0|F(e,\emptyset,\emptyset) = F(e,0,0) + Fx(e,0,0) + Fxx(e,0,0).$$

- $xFx(0,e,0) = 2\cdot I_1J_1(F(\emptyset,e,\emptyset))$ (note there must be a distinguished coarse coset for this to

be meaningful), so that

$$\begin{aligned} 2F(\emptyset, e, \emptyset)) &= 2F(0, e, \emptyset) + 2xF(0, e, \emptyset) \\ &= F(\emptyset, e, 0) + Fx(\emptyset, e, 0) \\ &= F(0, e, 0) + xF(0, e, 0) + Fx(0, e, 0) + xFx(0, e, 0). \end{aligned}$$

- The same definitions with G replacing F, as appropriate. We find that xG, xxG, and xGx are applicable.

Observe that these definitions are crafted so that the following cute rule applies:

Lemma 20.16. *Let N be one of the symbols Fx, xF, Fxx, xxF, xFx, and let N' be the symbol made by spelling N backward. If the ℓ_i are integers such that $N(\ell_0, \ell_1, \ell_2)$ is meaningful, then*

$$\widehat{N(\ell_0, \ell_1}, \ell_2) = q^{\ell_2 - \ell_0} N'(\ell_2, \ell_1, \ell_0).$$

(This lemma also holds for $N = F$, though this will be proved later: see Lemma 21.13.)

This will allow us to write the ring totals for all three unramified splitting types in a uniform way and verify reflection for them simultaneously.

For the unshifted quadratic form ε, $\mathcal{L}_i$ is charmed for $i \geq e'/2$, an easy consequence of for $i \geq e'/2$, from which we derive:

Lemma 20.17. *The function $\varepsilon_C = \varepsilon_C F(\emptyset, \emptyset, e)$ has at most the following projections nonzero:*

(a) *If $[\hat{\omega}_C] \in \mathcal{L}_0$, then $I_0 J_0$, $I_1 J_1$, and $I_2 J_2$.*

(b) *If $[\hat{\omega}_C] \notin \mathcal{L}_0$, then $I_0 J_1$, $I_1 J_0$, and $I_2 J_2$.*

Proof. It suffices to prove that

$$I_i \left(\varepsilon_C F(\emptyset, \emptyset, e)\right) = (x^i F)(0, 0, e)$$

is in the image of J_j, for each pair (i,j) mentioned in the lemma. Now $\mathcal{L}_0$ is charmed for the unshifted quadratic form ε, an easy consequence of Proposition 19.8. Hence $\hat{\omega}_C\mathcal{L}_0$ is charmed for ε_C, from which we get

$$(x^iF)(0,0,e) = (x^jG)(0,0,e).$$

Taking the Fourier transform by Lemma 20.14(c),

$$\widehat{(x^iF)}(0,0,e) = \pm_{\varepsilon_C}(x^jF)(0,0,e),$$

which lies in the image of I_j. Hence the original $(x^iF)(0,0,e)$ lies in the image of J_j, as desired. ■

20.7 Notation

If $T(\ell_0,\ell_1,\ell_2)$ is a boxgroup, we let $F(T) = F(\ell_0,\ell_1,\ell_2)$ be its characteristic function, and $G(T) = G(\ell_0,\ell_1,\ell_2)$ be the characteristic function of its charmed coset, if applicable. Let $T^\times(\ell_0,\ell_1,\ell_2)$ denote the subset of elements of $T(\ell_0,\ell_1,\ell_2)$ having minimal level, assuming this level is less than e':

$$T^\times(\ell_0,\ell_1,\ell_2) = \begin{cases} T(\ell_0,\ell_1,\ell_2) \setminus T(\ell_0+1,\ell_1-1,\ell_2), & \ell_0 \geq 0, \ell_1 \geq 1 \\ T(\ell_0,\ell_1,\ell_2) \setminus T(\ell_0+1,0,\ell_2-1), & \ell_0 \geq 0, \ell_1 = 0 \\ T(\emptyset,\ell_1,\ell_2) \setminus T(0,\ell_1,\ell_2), & \ell_0 = \emptyset \end{cases}$$

Let $F^\times(\ell_0,\ell_1,\ell_2)$ and $G^\times(\ell_0,\ell_1,\ell_2)(\delta)$ be the characteristic functions of $T^\times(\ell_0,\ell_1,\ell_2)$ and $\psi_C T^\times(\ell_0,\ell_1,\ell_2)$, respectively. This will provide enough notation to write the ring totals in the succeeding sections.

21 Ring volumes for ξ_1'

In this section, we will compute the volume of vectors $\xi_1' \in \mathcal{O}_R$ satisfying the $\mathcal{M}_{11}$ and $\mathcal{N}_{11}$ conditions. A sample of our answers are tabulated in Appendix B.

Because $\bar{\xi}_1 = \xi_1$, we freely omit the bar on $m_{11} = m_{11}$ and $n_{11} = n_{11}$.

21.1 The smearing lemma

We now prove a simple lemma that allows us to reduce to the case m_{11} large.

Lemma 21.1. *For a first vector problem $\mathfrak{P}$, define u_1 to be the unique value such that, when the conic is transformed to minimal discriminant in accordance with 19.3, $\beta^{\odot} = \delta^{\odot}\xi_1^{\odot 2}$ must lie in $\pi^{u_1}\mathcal{O}_R \setminus \pi^{u_1+1}\mathcal{O}_R$, to wit:*

$$u_1 = \begin{cases} 1 & \text{if } (\sigma, h_1) \in \{(1^3, -1)\} \\ 0 & \text{otherwise.} \end{cases}$$

Assume that the m_{11} and n_{11} of $\mathfrak{P}$ satisfy

$$m_{11}^{\odot} > u_1$$

(so $\mathcal{M}_{11}$ is active even after transformation) and $m_{11}^{\odot} > n_{11}$. Let $m_{11}^{\sharp} > m_{11}$ lie in the same class mod $\mathbb{Z}$, and let $m_{11}^{\odot\sharp}$ be the corresponding value of m'_{11}. Let $\mathfrak{P}^{\sharp}$ be the first vector problem with $m_{11} = m_{11}^{\sharp}$ and the rest of the data the same.

Then the answer to $\mathfrak{P}$ can be computed from that of $\mathfrak{P}^{\sharp}$ by the following formula:

$$W_{\mathfrak{P}} = q^{m_{11}^{\sharp} - m_{11}} \mathfrak{S}_r W_{\mathfrak{P}^{\sharp}}$$

Here the smear operator *$\mathfrak{S}_r$ is defined by the following convolution:*

$$\mathfrak{S}_r W(\delta) = \frac{1}{|\mathcal{L}_r|} \sum_{\alpha \in \mathcal{L}_r} W(\alpha\delta),$$

and r is the level for which

$$\mathcal{L}_r = \left\{ [\eta] : \eta \equiv 1 \mod \pi^{m_{11}^{\odot} - u_1} \right\}.$$

We call this the *smearing lemma* because it states that the function $W_{\mathfrak{P}}$ can be obtained from $W_{\mathfrak{P}^{\sharp}}$ by averaging over the cosets of $\mathcal{L}_r$, like reducing the resolution of a picture by averaging over larger pixels. Here the symbol $\sharp$ is used to mark the "sharper" image given by the solutions of $\mathfrak{P}^{\sharp}$

and should not be confused with the use of the same symbol in the context of tilting.

The level r is given explicitly as follows:

- In unramified type,
$$r = \left\lfloor \frac{m_{11}}{2} \right\rfloor, \quad 0 < m_{11} \leq 2e$$

- In splitting type 1^3,
$$r = \lfloor m_{11} \rfloor, \quad 0 < m_{11} \leq 2e.$$

Proof. We will prove the identity by computing in two ways the volume of the set

$$\mathcal{S} = \left\{ \begin{array}{rl} \eta \equiv 1 & \mod \pi^{m_{11}^{\odot} - u_1}, \\ (\eta, \xi') : \lambda^{\diamond}(\eta \delta^{\odot} \xi'^2) \equiv 0 & \mod \pi^{m_{11}^{\odot \sharp}}, \\ \bar{\omega}_C^{-1} \gamma^2 \xi'^2 \equiv a & \mod \pi^{n_{11}} \text{ for some } a \in \mathcal{O}_K \end{array} \right\} \subseteq \mathcal{O}_R^{\times} \times \mathbb{P}(\mathcal{O}_R). \tag{167}$$

First, fix $\eta \in 1 + \pi^{m_{11}^{\odot} - u_1} \mathcal{O}_R$. The conditions on ξ' are seen to be the $\mathcal{M}_{11}$ and $\mathcal{N}_{11}$ conditions for δ replaced by $\eta\delta$; the omission of the η factor in $\mathcal{N}_{11}$ makes no difference, since the left-hand side is a multiple of π^{u_1} and the addition would have valuation at least

$$(m_{11}^{\odot} - u_1) + u_1 = m_{11}^{\odot} \geq n_{11}.$$

So the volume of ξ' for fixed η is $W_{\mathfrak{P}^\sharp}(\delta\eta)$, and since $[\eta]$ takes all classes in $\mathcal{L}_r$ equally often while ranging in a pixel of volume $q^{-3(m_{11}^{\odot} - u_1)}$, we get

$$\mu(\mathcal{S}) = \frac{q^{-3(m_{11}^{\odot} - u_1)}}{|\mathcal{L}_r|} \sum_{\eta \in \mathcal{L}_r} W_{\mathfrak{P}^\sharp}(\delta\eta).$$

On the other hand, a fixed $\xi' \in \mathcal{O}_R$ has a chance of being the second coordinate of a pair in $\mathcal{S}$ only if

- it satisfies the $\mathcal{N}_{11}$ condition $\bar{\omega}_C^{-1} \gamma^2 \xi'^2 \equiv a \mod \pi^{n_{11}}$ for some $a \in \mathcal{O}_K$, and

- it satisfies the $\mathcal{M}_{11}$ condition for some $\eta = 1 + \pi^{m_{11}^{\odot} - u_1}\eta'$, $\eta' \in \mathcal{O}_R$; in particular,

$$\begin{aligned} 0 &\equiv \lambda^{\diamondsuit}(\eta\delta^{\odot}\xi'^2) \\ &= \lambda^{\diamondsuit}(\delta\xi'^2) + \pi^{m_{11}^{\odot} - u_1}\lambda^{\diamondsuit}(\eta'\delta\xi'^2) \\ &= \lambda^{\diamondsuit}(\delta\xi'^2) + \pi^{m_{11}^{\odot}}\lambda^{\diamondsuit}\left(\pi^{-u_1}\delta\xi'^2\right) \\ &\equiv \lambda^{\diamondsuit}(\delta\xi'^2) \mod \pi^{m_{11}^{\odot}}. \end{aligned}$$

The volume of ξ' satisfying these conditions is, by definition, none other than $W_{\mathfrak{P}}$. For fixed ξ', the value of η' is constrained by $\mathcal{M}_{11}$ alone:

$$\begin{aligned} \pi^{m_{11}^{\odot} - u_1}\lambda^{\diamondsuit}(\eta'\delta^{\odot}\xi'^2) &\equiv 0 \mod \pi^{m_{11}^{\odot\sharp}} \\ \lambda^{\diamondsuit}\left(\eta' \cdot \pi^{-u_1}\delta^{\odot}\xi'^2\right) &\equiv 0 \mod \pi^{m_{11}^{\odot\sharp} - m_{11}^{\odot}} = \pi^{m_{11}^{\sharp} - m_{11}}. \end{aligned}$$

Since $\lambda^{\diamondsuit}$ is a perfect linear functional and $\pi^{-u_1}\delta^{\odot}\xi'^2$ is a primitive vector in $\mathcal{O}_R$, the volume of η' satisfying this congruence is $q^{m_{11} - m_{11}^{\sharp}}$, which makes a volume of $q^{-3(m_{11}^{\odot} - u_1) + m_{11} - m_{11}^{\sharp}}$ for η. So

$$\mu(\mathcal{S}) = \pi^{-3(m_{11}^{\odot} - u_1) + m_{11} - m_{11}^{\sharp}} W_{\mathfrak{P}}(\delta).$$

Comparing the two expressions for $\mu(\mathcal{S})$, the result follows. ■

21.2 The zones when $\mathcal{N}_{11}$ is strongly active (black, plum, purple, blue, green, and red)

In this section, we solve first vector problems in which $\mathcal{N}_{11}$ is strongly active, that is, $n_{11} > \bar{s}$. In view of the smearing lemma, we assume that $m_{11} > 2e$. Let n_c ("n for the colorful zones") be $n_{11} - \bar{s}$.

The following little symmetry will be occasionally useful:

Lemma 21.2. *Let $\psi = a + b\theta_1 \in \mathcal{O}_R$ with $a \in \mathcal{O}_K^{\times}$, $b \in \pi^{n_{11}}\mathcal{O}_K^{\times}$, and let $\mathfrak{P}'$ be the first vector problem derived from $\mathfrak{P}$ by replacing the pertinent extender vector θ_1 by $\theta_1' = \psi^{-1}\theta_1$. Then:*

(a) $\hat{\omega}_{\mathfrak{P}'} = \psi^{-1}\hat{\omega}_{\mathfrak{P}}$.

(b) $\varepsilon_{\mathfrak{P}'}(\delta) = \varepsilon_{\mathfrak{P}}(\psi^{-1}\delta)$.

(c) $W_{\theta_1',m_{11},n_{11}}(\delta) = W_{\theta_1,m_{11},n_{11}}(\psi^{-1}\delta)$.

Proof. The left-hand side is the volume of ξ' for which

$$\begin{aligned}\delta\left(\frac{\xi'}{\xi_0'}\right)^2 &\in \mathcal{O}_K^\times + B_{\psi^{-1}\theta_1}(m_{11},n_{11}) \\ &= \psi^{-1}\cdot\left(\mathcal{O}_K^\times + B_{\theta_1}(m_{11},n_{11})\right)\end{aligned}$$

by Lemma 20.2(a), since $\psi \in \mathcal{O}_K^\times + B_{\theta_1}(m_{11},n_{11})$. So the condition on ξ' can be written as

$$\delta\psi\left(\frac{\xi'}{\xi_0'}\right)^2 \in \mathcal{O}_K^\times + B_{\theta_1}(m_{11},n_{11}),$$

of which the solution volume is seen to be $W_{\theta_1,m_{11},n_{11}}(\psi\delta)$.

■

The following formula for the sum of the values of $W_{m_{11},n_{11}}$ will be essential:

Lemma 21.3. *If the values of m_{11} and n_{11} make $\mathcal{N}_{11}$ strongly active, then $W_{m_{11},n_{11}} = 0$ unless the chosen coarse coset is $\mathcal{L}_0$. In this case*

$$\sum_{\delta\in\mathcal{L}_0} W_{m_{11},n_{11}}(\delta) = |H^0|q^{2e-m_{11}-n_{11}+\frac{\bar{s}}{2}+\frac{d_0}{2}+v(N(\gamma))}$$

where $d_0 = v_K(\mathrm{Disc}_K R)$; equivalently,

$$\sum_{\delta\in\mathcal{L}_0} W^{\odot}_{m_{11},n_{11}}(\delta) = |H^0|q^{2e-m_{11}-n_{11}+\frac{\bar{s}}{2}+\frac{d_0}{2}+v(N(\gamma\gamma^{\odot}))}.$$

Proof. By Lemma 18.4, the support of $W_{m_{11},n_{11}}$ consists of the classes $[\delta] = [\beta]$ in H^1 of elements β of the box

$$\mathcal{O}_K^\times + B_{m_{11},n_c} = \{x + y\pi^{n_c}\theta_1 + z\pi^{m_{11}}\theta_2, \quad x\in\mathcal{O}_K^\times, \quad y,z\in\mathcal{O}_K\}.$$

Our method is to show that $W_{m_{11},n_{11}}(\delta)$ can be interpreted as the volume of β of class $[\delta]$ in the box, up to a scalar. Then since each β belongs to just one square-class, the sum is known.

Since $m_{11}, n_c > 0$, β must be a unit, explaining why $[\delta] \in \mathcal{L}_0$. For fixed $\delta \in \mathcal{O}_R^\times$, as ξ' ranges over the solution set of its transformed conditions, β ranges over the elements of its box of class $[\delta]$, up to scaling. The correspondence is given by a relation of the form

$$\beta = \delta \left(\frac{\xi'}{\xi'_0} \right)^2, \tag{168}$$

where

$$\xi'_0 = \frac{1}{\gamma} \sqrt{\delta \omega_C}$$

is an element of $\mathcal{O}_R$ constructed from the γ of Lemma 18.5 whose valuations represent a lower bound on the valuations of ξ'.

Now we compare the projective volumes of β and ξ' satisfying the $\mathcal{M}_{11}$ and $\mathcal{N}_{11}$ conditions. In the sequence

$$\xi' \longmapsto \frac{\xi'}{\xi'_0} \longmapsto \left(\frac{\xi'}{\xi'_0} \right)^2 \longmapsto \delta \left(\frac{\xi'}{\xi'_0} \right)^2 = \beta,$$

each member is a primitive vector in $\mathcal{O}_R$, so we can speak of projective volumes.

Dividing by ξ'_0 is a one-to-one operation that scales both affine and projective volumes by

$$q^{v_K(N_{R/K}(\xi'_0))} = q^{\bar{s}/2 - v(N(\gamma))}.$$

So there is a volume $q^{\bar{s}/2 - v(N(\gamma))} W_{m_{11},n_{11}}(\delta)$ of ξ/ξ'_0.

Squaring, on units, multiplies small projective volumes by q^{-2e} (since it takes the i-pixel about 1 to the $(i+e)$-pixel for $i > e$). But it is $|H^0|$-to-one since there are $|H^0|$-many square roots of 1 in R, up to scaling by ± 1. Since the resolvent conditions are invariant under multiplying ξ' by a square root of 1, the volume of (ξ/ξ'_0) is

$$\frac{q^{-2e + \bar{s}/2 - v(N(\gamma))}}{|H^0|} W_{m_{11},n_{11}}(\delta).$$

Lastly, δ is a unit, so multiplying by it does not change volumes. Hence

$$\frac{q^{-2e+\bar{s}/2-v(N(\gamma))}}{|H^0|}\sum_{\delta\in\mathcal{L}_0} W_{m_{11},n_{11}}(\delta)$$

is the volume of the box $\mathbb{P}(\mathcal{O}_K^\times + B_{m_{11},n_c})$. Thus it suffices to prove that

$$\mu(\mathbb{P}(\mathcal{O}_K^\times + B_{m_{11},n_c})) = q^{-m_{11}-n_{11}+\bar{s}+\frac{d_0}{2}}.$$

Converting to affine volumes, with $\mu(R) = 1$,

$$\begin{aligned}\mu(\mathbb{P}(\mathcal{O}_K^\times + B_{m_{11},n_c})) &= \frac{1}{1-\frac{1}{q}}\mu(\mathcal{O}_K^\times + B_{m_{11},n_c}) \\ &= \mu(\mathcal{O}_K + B_{m_{11},n_c}) \\ &= q^i\end{aligned}$$

where i is the integer such that

$$\begin{aligned}\Lambda^3(\mathcal{O}_K + B_{m_{11},n_c}) &= \pi^i\Lambda^3\mathcal{O}_R \\ \Lambda^3(\mathcal{O}_{\bar{K}}\langle 1, \pi^{n_c}\theta_1, \pi_{11}^m\theta_2\rangle) &= \pi^i\Lambda^3\mathcal{O}_R \\ n_c + m_{11} &= i + \frac{d_0}{2}.\end{aligned}$$

So

$$\sum_{\delta\in\mathcal{L}_0} W_{m_{11},n_c}(\delta) = |H^0|\cdot q^{2e-\bar{s}/2+v(N(\gamma))}\cdot q^{-m_{11}-n_c+\frac{d_0}{2}} = |H^0|\cdot q^{2e-m_{11}-n_{11}+\bar{s}/2+d_0'+v(N(\gamma))}$$

as desired. ■

We tabulate:

spl.t.	h	$\xi_0' \sim$	$v(N(\gamma\gamma^{\odot}))$
ur	0	$(\pi^{s/2};1;1)$, s even	0
ur	1	$(\pi^{(s-1)/2};1;1)$, s odd	1/2
1^3	1	1	0
1^3	-1	π_R^2	-2

(169)

As shown, we obtain as a by-product that s determines h in unramified splitting types.

We now come to our main lemma, which computes $W_{m_{11},n_{11}}$ for large m_{11}.

21.2.1 Unramified

Lemma 21.4. *Suppose R is unramified over $K \supseteq \mathbb{Q}_2$. Let m_{11} and n_c be integers, $m_{11} > 2e \geq n_c > 0$. Let $\square_C = \min\{2\ell(\hat{\omega}_C)+1, e\}$ be the squareness of the $\delta = 1$ conic if s is even; let $\square_C = 0$ if s is odd. If s is even, let*

$$\tilde{n} = \left\lfloor \frac{2e - s - n_c + 2}{4} \right\rfloor = \left\lceil \frac{e - \frac{s}{2} - \lceil \frac{n_{11}}{2} \rceil}{2} \right\rceil.$$

Then $W_{m_{11},n_{11}}$ is given as follows:

(a) If $n_c > 2e$ (black zone), then

$$\begin{aligned} W_{m_{11},n_{11}} &= |H^0| q^{2e-m_{11}-n_c-\lfloor \frac{s}{2} \rfloor} F(e,\emptyset,\emptyset) \\ &= q^{2e-m_{11}-n_c-\lfloor \frac{s}{2} \rfloor}[F(e,0,0) + Fx(e,0,0) + Fxx(e,0,0)] \end{aligned}$$

(b) If $2e - s < n_c \leq 2e$ (purple zone), then

$$\begin{aligned} W_{m_{11},n_{11}} &= 2q^{e-m_{11}-\lceil \frac{n_c}{2} \rceil - \lfloor \frac{s}{2} \rfloor} F\left(\left\lfloor \frac{n_c}{2} \right\rfloor, e - \left\lfloor \frac{n_c}{2} \right\rfloor, \emptyset\right) \\ &= q^{e-m_{11}-\lceil \frac{n_c}{2} \rceil - \lfloor \frac{s}{2} \rfloor} \left[F\left(\left\lfloor \frac{n_c}{2} \right\rfloor, e - \left\lfloor \frac{n_c}{2} \right\rfloor, 0\right) + Fx\left(\left\lfloor \frac{n_c}{2} \right\rfloor, e - \left\lfloor \frac{n_c}{2} \right\rfloor, 0\right)\right] \end{aligned}$$

(c) *If* $2e - s - 2\square_C < n_c \le 2e - s$ *and* $n_c \ge \dfrac{2e-s}{3}$ *(blue zone), then* s *is even and*

$$W_{m_{11},n_{11}} = q^{-m_{11}+\lfloor \frac{2e-s-n_c}{4} \rfloor} F\left(\left\lfloor \frac{n_c}{2} \right\rfloor, e - \tilde{n} - \left\lfloor \frac{n_c}{2} \right\rfloor, \tilde{n}\right)$$

(d) *If* $\square_C < n_c \le 2e - s - 2\square_C$ *(green zone), then*

$$W_{m_{11},n_{11}} = q^{-m_{11}+\lceil \ell_C \rceil}(1+\varepsilon_C) F\left(\left\lfloor \frac{n_c}{2} \right\rfloor, \ell_C + \frac{s}{2} + \mathbf{1}_{2\nmid n_c}, e - \ell_C - \frac{s}{2} - \left\lceil \frac{n_c}{2} \right\rceil\right)$$

where $\ell_C = \frac{\square_C - 1}{2} \in \{-1/2\} \cup \mathbb{Z}_{\ge 0}$.

(e) *If* $n_c < \dfrac{2e-s}{3}$ *and* $n_c \le \square_C$ *(red zone), then* s *is even and*

$$W_{m_{11},n_{11}} = \sum_{\lfloor \frac{n_c}{2} \rfloor \le \ell < \tilde{n}} q^{-m_{11}+\ell}(1+\varepsilon_C) G^{\times}\left(\ell, \left\lceil \frac{n_c}{2} \right\rceil + \frac{s}{2}, e - \left\lceil \frac{n_c}{2} \right\rceil - \frac{s}{2} - \ell\right) + \\ + q^{-m_{11}+\lfloor \frac{2e-s-n_c}{4} \rfloor} G(\tilde{n}, e-2\tilde{n}, \tilde{n}).$$

Proof. First note that if $s \ge 2e$, then the blue, green, and red zones are empty, and if $s < 2e$ is odd, then since $\ell_0 = -1/2$, the blue and red zones are empty. This ensures that the answers are at least well defined.

By Lemma 18.4, the support of $W_{m_{11},n_{11}}$ consists of the classes $[\delta] = [\beta]$ in H^1 of elements β of the box

$$1 + B_{m_{11},n_c} = \{1 + y\pi^{n_c}\theta_1 + z\pi^{m_{11}}\theta_2, \quad x \in \mathcal{O}_K^{\times}, \quad y, z \in \mathcal{O}_K\}.$$

Since $m_{11} > 2e$, the z term has no effect on $[\beta]$, and we ignore it. In particular, the conic

$$\operatorname{coef}_{\theta_2}(\beta\xi^2) = 0, \quad \text{that is,} \quad \operatorname{tr}(\hat{\omega}_C \beta \xi^2) = 0$$

has a solution $\xi = 1$, so $\varepsilon_C(\beta) = \varepsilon(\hat{\omega}_C\beta) = 1$ for all β in the box.

Black zone. In the black zone, we have $\beta \equiv 1 \mod 4\pi$, so $[\beta] = 1$. Hence only $\delta = 1$ yields a nonzero volume, which is, by Lemma 21.3,

$$|H^0|q^{2e-m_{11}-n_c+\frac{d_0}{2}-(s/2-v(N(\gamma)))} = |H^0|q^{2e-m_{11}-n_c-\lfloor\frac{s}{2}\rfloor}.$$

For the remaining zones, let $W'_{m_{11},n_{11}}$ denote the claimed value of $W_{m_{11},n_{11}}$ in each case. Our proof method will consist of two steps:

- We prove that $W_{m_{11},n_{11}}(\delta) \leq W'_{m_{11},n_{11}}(\delta)$ for every δ (the *bounding step*).
- We check that

$$\sum_{\delta\in H^1} W'_{m_{11},n_{11}}(\delta) = |H^0|q^{2e-m_{11}-n_c} = \sum_{\delta\in H^1} W_{m_{11},n_{11}}(\delta)$$

  (the *summing step*), implying that equality must hold for every δ.

Purple zone. In the purple zone, $s > 0$ defines a splitting $R = K \times Q$. If we translate θ_1 so that $\theta_1^Q \equiv 0 \mod \pi^s$, then we get $\beta^Q \equiv 1 \mod 4\pi$. Also, $\beta \equiv 1 \bmod \pi^{n_c}$, and indeed, $\beta^{(K)}$ can achieve any value $\equiv 1 \mod \pi^{n_c}$, each congruence class modulo 4π achieved equally often. So $[\delta] = [\beta]$ ranges uniformly over $T\left(\lfloor\frac{n_c}{2}\rfloor, e-\lfloor\frac{n_c}{2}\rfloor, \emptyset\right)$, and for each class $[\delta]$ that is attained,

$$W_{m_{11},n_{11}}(\delta) = \frac{|H^0|q^{2e-m_{11}-n_c-\lfloor\frac{s}{2}\rfloor}}{|T\left(\lfloor\frac{n_c}{2}\rfloor, e-\lfloor\frac{n_c}{2}\rfloor, \emptyset\right)|} = \frac{|H^0|q^{2e-m_{11}-n_c-\lfloor\frac{s}{2}\rfloor}}{\frac{|H^0|}{2}q^{e-\lfloor\frac{n_c}{2}\rfloor}} = 2q^{e-m_{11}-\lceil\frac{n_c}{2}\rceil-\lfloor\frac{s}{2}\rfloor},$$

as claimed.

Blue zone. Note that $s < 2e$ and that s is even (as the bounds imply $\square_C > 0$). Our strategy is to note that

$$\beta \in 1 + B_{m_{11},n_c} \subseteq 1 + B_{m',n_c}$$

for some $m' \le m_{11}$ for which $[1 + B_{m',n_c}]$ is a boxgroup. Here, we find that the gray-blue condition (152) in Lemma 20.4 is the most stringent one, so we take

$$m' = \left\lceil \frac{n_c}{2} \right\rceil + e + \frac{s}{2}$$

and get

$$\begin{aligned}
\beta &\in \left[1 + B_{\theta_1}\left(\left\lceil \frac{n_c}{2} \right\rceil + e + \frac{s}{2}, n_c\right)\right] \\
&= T\left(\left\lfloor \frac{n_c}{2} \right\rfloor, \left\lfloor \frac{\left\lceil \frac{n_c}{2} \right\rceil + e + \frac{s}{2}}{2} \right\rfloor - \left\lfloor \frac{n_c}{2} \right\rfloor, e - \left\lfloor \frac{\left\lceil \frac{n_c}{2} \right\rceil + e + \frac{s}{2}}{2} \right\rfloor\right) \\
&= T\left(\left\lfloor \frac{n_c}{2} \right\rfloor, e - \tilde{n} - \left\lfloor \frac{n_c}{2} \right\rfloor, \tilde{n}\right).
\end{aligned}$$

For each such δ, the value of

$$W_{m_{11},n}(\delta)$$

is controlled by the conic via Lemma 19.9, once we know the level

$$\ell = \min\left\{\ell(\delta\hat{\omega}_C\diamondsuit\heartsuit), \left\lfloor \frac{e}{2} \right\rfloor\right\}.$$

We claim that all these conics are blue in the sense of Lemma 19.9; this requires

$$2\ell + 1 \stackrel{?}{\ge} e - n' = e - \left\lceil \frac{n_{11}}{2} \right\rceil = e - \left\lceil \frac{n_c + s}{2} \right\rceil,$$

that is,

$$\delta\hat{\omega}_C\diamondsuit\heartsuit \stackrel{?}{\in} \mathcal{L}_{\left\lceil \frac{e - \left\lceil \frac{n_c+s}{2} \right\rceil}{2} \right\rceil} = \mathcal{L}_{\left\lceil \frac{e - \left\lfloor \frac{n_c+s+1}{2} \right\rfloor}{2} \right\rceil} = \mathcal{L}_{\left\lceil \frac{2e-n_c-s-1}{4} \right\rceil}.$$

When $\delta = 1$, the required relation

$$\hat{\omega}_C\diamondsuit\heartsuit \in \mathcal{L}_{\left\lceil \frac{2e-n_c-s-1}{4} \right\rceil}$$

follows from the given inequality $n_c > 2e - s - 2\square_C$. So it suffices to show that

$$\beta \in \mathcal{L}_{\lceil \frac{2e-n_c-s-1}{4} \rceil}.$$

Since $\beta \equiv 1 \mod \pi^{n_c}$, it suffices to show that

$$\left\lfloor \frac{n_c}{2} \right\rfloor \stackrel{?}{\geq} \left\lceil \frac{2e - n_c - s - 1}{4} \right\rceil.$$

But the given red-blue inequality $n_c \geq \frac{2e-s}{3}$ gives

$$\frac{n_c - 1}{2} \geq \frac{2e - n_c - s - 1}{4},$$

from which the desired inequality follows by taking ceilings. So all conics are blue, and for every δ, $W_{\theta_1, m_{11}, n_{11}}(\delta) = q^{-m_{11} + \lfloor \frac{2e-s-n_c}{4} \rfloor}$ if nonzero. The summing step is now straightforward:

$$\begin{aligned}
\sum_{\delta \in H^1} W'_{m_{11}, n_{11}}(\delta) &= q^{-m_{11} + \lfloor \frac{2e-s-n_c}{4} \rfloor} \left| T\left(\left\lfloor \frac{n_c}{2} \right\rfloor, e - \tilde{n} - \left\lfloor \frac{n_c}{2} \right\rfloor, \tilde{n} \right) \right| \\
&= |H^0| \cdot q^{-m_{11} + \lfloor \frac{2e-s-n_c}{4} \rfloor + e - \tilde{n} - \lfloor \frac{n_c}{2} \rfloor + 2\tilde{n}} \\
&= |H^0| \cdot q^{-m_{11} + e - \lfloor \frac{n_c}{2} \rfloor + \lfloor \frac{2e-s-n_c}{4} \rfloor + \lfloor \frac{2e-s-n_c+2}{4} \rfloor} \\
&= |H^0| \cdot q^{-m_{11} + e - \lfloor \frac{n_c}{2} \rfloor + \lfloor \frac{2e-s-n_c}{2} \rfloor} \\
&= |H^0| \cdot q^{-m_{11} + e - \lfloor \frac{n_c}{2} \rfloor + e - \frac{s}{2} - n_c + \lfloor \frac{n_c}{2} \rfloor} \\
&= |H^0| \cdot q^{2e - m_{11} - n_c - \frac{s}{2}}.
\end{aligned}$$

This completes the proof, and in particular shows that $\varepsilon = 1$ identically on $\hat{\omega}_C \cdot T\left(\left\lfloor \frac{n_c}{2} \right\rfloor, e - \tilde{n} - \left\lfloor \frac{n_c}{2} \right\rfloor, \tilde{n} \right)$. This result will be important in proving the remaining zones.

Green zone. Again, we write

$$\beta \in 1 + B_{m_{11}, n_c} \subseteq 1 + B_{m', n_c}$$

where m' is as large as possible to make a boxgroup. This time, we find that the gray-green inequality (151) is the most stringent of the conditions in Lemma 20.4, so we take $m' = 2\left\lceil \frac{n_c}{2} \right\rceil + \square_C + s$ (noting that m' is an odd integer) and find that the support of $W_{m_{11},n_{11}}$ is contained in

$$\left[1 + B_{\theta_1}\left(2\left\lceil \frac{n_c}{2} \right\rceil + \square_C + s, n_c\right)\right] = T\left(\left\lfloor \frac{n_c}{2} \right\rfloor, \ell_C + \frac{s}{2} + \mathbf{1}_{2\nmid n_c}, e - \ell_C - \frac{s}{2} - \left\lceil \frac{n_c}{2} \right\rceil\right).$$

We claim all conics are green of the same squareness $\square_C$. The zone boundaries easily imply $\ell_C < \lfloor e/2 \rfloor$, so

$$[\hat{\omega}_C \diamondsuit \heartsuit] \in \mathcal{L}_{\lfloor \ell_C \rfloor} \setminus \mathcal{L}_{\lfloor \ell_C \rfloor + 1}.$$

We then note that $[\beta] \in \mathcal{L}_{\lfloor \ell_C \rfloor + 1}$, because $\beta \equiv 1 \mod \pi^{n_c}$ and we have the inequality $n_c > \square_C$. So $[\beta \hat{\omega}_C \diamondsuit \heartsuit]$ is also of exact level ℓ_C. Thus all conics are green of the same squareness, and by Lemmas 19.9 and 19.10, we have the bound

$$W_{m_{11},n_c} \leq 2q^{-m_{11}+\lceil \ell_C \rceil} T\left(\left\lfloor \frac{n_c}{2} \right\rfloor, \ell_C + \frac{s}{2} + \mathbf{1}_{2\nmid n_c}, e - \ell_C - \frac{s}{2} - \left\lceil \frac{n_c}{2} \right\rceil\right),$$

indeed

$$W_{m_{11},n_c} \leq q^{-m_{11}+\lceil \ell_C \rceil}(1 + \varepsilon_C) T\left(\left\lfloor \frac{n_c}{2} \right\rfloor, \ell_C + \frac{s}{2} + \mathbf{1}_{2\nmid n_c}, e - \ell_C - \frac{s}{2} - \left\lceil \frac{n_c}{2} \right\rceil\right).$$

where $\varepsilon_C(\delta) = \varepsilon(\hat{\omega}_C \delta)$. This completes the bounding step.

To perform the summing step, we need to compute the sum

$$q^{-m_{11}+\lceil \ell_C \rceil} \sum_{\delta \in T\left(\left\lfloor \frac{n_c}{2} \right\rfloor, \ell_C + \frac{s}{2} + \mathbf{1}_{2\nmid n_c}, e - \ell_C - \frac{s}{2} - \left\lceil \frac{n_c}{2} \right\rceil\right)} (1 + \varepsilon_C(\delta)).$$

The term 1 is found to sum to the desired total $|H^0| \cdot q^{2e - m_{11} - n_c - \left\lfloor \frac{s}{2} \right\rfloor}$. We claim that

$$\sum_{\delta \in T\left(\left\lfloor \frac{n_c}{2} \right\rfloor, \ell_C + \frac{s}{2} + \mathbf{1}_{2\nmid n_c}, e - \ell_C - \frac{s}{2} - \left\lceil \frac{n_c}{2} \right\rceil\right)} \varepsilon_C(\delta) = 0,$$

in other words that ε is *equidistributed* between 1 and -1 in this boxgroup. This follows from Lemma 20.13(b): because $\mathcal{L}_{\lfloor \ell_C \rfloor + 1} \neq \hat{\omega}_C \mathcal{L}_{\lfloor \ell_C \rfloor + 1}$ is an uncharmed coset, we have ε equidistributed on cosets of $\mathcal{L}_{e - \lfloor \ell_C \rfloor - 1}$.

Red zone. We first recenter. Changing θ_1 to the element $a + b\psi_C^{-1}\theta_1$ from Lemma 20.11, keeping the rest of the resolvent data fixed, gives us a new first vector problem $\mathfrak{P}'$ whose associated cubic ring C' has first extender vector $\theta_1' = \eta^2$ is a square. By Lemma 21.2, the ring-count function $W_{\mathfrak{P}}$ simply shifts by ψ_C. Note that all boxgroups $T(\ell_0, \ell_1, \ell_2)$ in claimed totals satisfy the gray-green inequality

$$\ell_1 \leq \frac{s + \square_C + 1}{2}$$

Since $\theta_1' \equiv \theta_1 \mod \pi^{s + \square_C}$, the replacement does not change any of the boxgroups, and their charmed cosets merely translate by $[\psi]$ along with the quadratic form $\varepsilon_{C'}(\delta) = \varepsilon_C(\psi\delta)$.

So it suffices to prove the result in the case that θ_1 is a square. Note that $[\hat{\omega}_C] \in \mathcal{L}_{\lfloor e/2 \rfloor}$ since $\omega_C \equiv \theta_1 \mod 2$.

We will actually prove something stronger:

$$W_{m_{11}, n_{11}} = \sum_{\lfloor \frac{n_c}{2} \rfloor \leq \ell < \tilde{n}_c} q^{-m_{11} + \ell}(1 + \varepsilon_C) F^{\times}\left(\ell, \left\lceil \frac{n_c}{2} \right\rceil + \frac{s}{2}, e - \left\lceil \frac{n_c}{2} \right\rceil - \frac{s}{2} - \ell\right) + q^{-m_{11} + \lfloor \frac{2e + s - n_c}{4} \rfloor} F(\tilde{n}, e - 2\tilde{n}, \tilde{n}), \tag{170}$$

in which we have replaced all G's by F's. We take a moment to realize why this is actually stronger. The claim that $T = T(\tilde{n}, e - 2\tilde{n}, \tilde{n})$ is in the support of $W_{m_{11}, n_{11}}$ implies the following:

- ε_C is identically 1 on T, and hence
- T is maximal isotropic for the Hilbert pairing, and also
- the identity coset T is charmed, so $F_T = G_T$, and
- the quadratic form ε_C is positively charmed.

All the remaining terms use F_V where $V \supseteq T$, so F is interchangeable with G there too. We now prove (170).

Begin with an arbitrary

$$\beta = 1 + \pi^{n_c} b\theta_1.$$

Assume first that $\pi^{n_c}b$ is *not* a square modulo $\pi^{e-\frac{s}{2}-\lceil\frac{n_c}{2}\rceil+1}$, and let k be the largest integer such that $\pi^{n_c}b$ is a square modulo π^{2k+1}. Note that $\left\lfloor\frac{n_c}{2}\right\rfloor \le k < \tilde{n}$. We may write

$$\pi^{n_c}b = \left(\pi^{\lceil\frac{n_c}{2}\rceil}a\right)^2 + \pi^{2k+1}c, \quad \pi \nmid c.$$

Let $\zeta = 1 + \pi^{\lceil\frac{n_c}{2}\rceil}a\eta$. We claim that

$$\frac{\beta}{\zeta^2} \in 1 + B_{\theta_1}\left(2\left\lceil\frac{n_c}{2}\right\rceil + s + 2k + 1, 2k + 1\right),$$

implying that $[\beta] \in T\left(k, \lceil\frac{n_c}{2}\rceil + \frac{s}{2}, e - \lceil\frac{n_c}{2}\rceil - \frac{s}{2} - k\right)$ (compare the kth term of the sum). Write

$$\begin{aligned}
\frac{\beta}{\zeta^2} &= \frac{1 + \left(\pi^{\lceil\frac{n_c}{2}\rceil}a\right)^2\theta_1 + \pi^{2k+1}c\theta_1}{\zeta^2} \\
&= \frac{\left[1 + \left(\pi^{\lceil\frac{n_c}{2}\rceil}a\right)^2\theta_1\right]\left(1 + \pi^{2k+1}c\theta_1\right) - \pi^{2\lceil\frac{n_c}{2}\rceil+2k+1}a^2c\theta_1^2}{\zeta^2} \\
&= \frac{\left[\left(1 + \pi^{\lceil\frac{n_c}{2}\rceil}a\eta\right)^2 - 2\pi^{\lceil\frac{n_c}{2}\rceil}a\eta\right]\left(1 + \pi^{2k+1}c\theta_1\right) - \pi^{2\lceil\frac{n_c}{2}\rceil+2k+1}a^2c{\theta_1}^2}{\zeta^2} \\
&= \frac{\left(\zeta^2 - 2\pi^{\lceil\frac{n_c}{2}\rceil}a\eta\right)\left(1 + \pi^{2k+1}c\theta_1\right) - \pi^{2\lceil\frac{n_c}{2}\rceil+2k+1}a^2c\theta_1^2}{\zeta^2}.
\end{aligned}$$

We first claim that the denominator ζ^2 belongs to $\mathcal{O}_K[\theta_1] = B_{\theta_1}(s, 0)$. Since

$$\zeta^2 = \left(1 + \pi^{\lceil\frac{n_c}{2}\rceil}a\eta\right)^2 = 1 + \pi^{2\lceil\frac{n_c}{2}\rceil}a^2\theta_1 + 2\pi^{\lceil\frac{n_c}{2}\rceil}a\eta,$$

only the last term is in question, and since $v_K\left(\mathrm{coef}_{\theta_2}\eta\right) \ge s/2$ (as we saw in Lemma 20.3), the inequality needed is

$$e + \left\lceil\frac{n_c}{2}\right\rceil + \frac{s}{2} \ge s,$$

a consequence of $s < 2e$.

Therefore the last term of β/ζ^2 is

$$\begin{aligned}\frac{-\pi^{2\left\lceil \frac{n_c}{2}\right\rceil+2k+1}a^2c\theta_1^2}{\zeta^2} &\in \pi^{2\left\lceil \frac{n_c}{2}\right\rceil+2k+1}\mathcal{O}_K[\theta_1] \\ &= B_{\theta_1}\left(2\left\lceil\frac{n_c}{2}\right\rceil+s+2k+1, n_c+2k+1\right) \\ &\subseteq B_{\theta_1}\left(2\left\lceil\frac{n_c}{2}\right\rceil+s+2k+1, 2k+1\right).\end{aligned}$$

Thus it is enough to prove that

$$\frac{\left(\zeta^2-2\pi^{\left\lceil \frac{n_c}{2}\right\rceil}a\eta\right)\left(1+\pi^{2k+1}c\theta_1\right)}{\zeta^2} \in 1+B_{\theta_1}(n_c+s+2k+1,2k+1) \subseteq 1+B_{\theta_1}\left(2\left\lceil\frac{n_c}{2}\right\rceil+s+2k+1,2k+1\right).$$

Since the right-hand side is a group and contains $1+\pi^{2k+1}c\theta_1$, it is enough to show that

$$\frac{\zeta^2-2\pi^{\left\lceil \frac{n_c}{2}\right\rceil}a\eta}{\zeta^2} \in 1+B_{\theta_1}(n_c+s+2k+1,2k+1),$$

that is,

$$\frac{2\pi^{\left\lceil \frac{n_c}{2}\right\rceil}a\eta}{\zeta^2} \in B_{\theta_1}(n_c+s+2k+1,2k+1).$$

But, since η belongs to the ring $B_{\theta_1}(s/2,0)$ and ζ^2 is a unit in that ring,

$$\begin{aligned}\frac{2\pi^{\left\lceil \frac{n_c}{2}\right\rceil}a\eta}{\zeta^2} &\in \pi^{e+\left\lceil \frac{n_c}{2}\right\rceil}B_{\theta_1}\left(\frac{s}{2},0\right) \\ &= B_{\theta_1}\left(e+\left\lceil\frac{n_c}{2}\right\rceil+\frac{s}{2}, e+\left\lceil\frac{n_c}{2}\right\rceil\right) \\ &\subseteq B_{\theta_1}(n_c+s+2k+1,2k+1),\end{aligned}$$

where the last step uses $k<\tilde{n}$. This establishes the claim that

$$[\beta] \in T\left(k, \left\lceil\frac{n_c}{2}\right\rceil+\frac{s}{2}, e-\left\lceil\frac{n_c}{2}\right\rceil-\frac{s}{2}-k\right).$$

To replace the T by $T^\times$, note that

$$\frac{\beta}{\zeta^2} \equiv 1 + \pi^{2k+1} c\theta_1 \mod \pi^{2k+2},$$

a generic unit of exact level k. Hence

$$\beta \in T^\times \left(k, \left\lceil \frac{n_c}{2} \right\rceil + \frac{s}{2}, e - \left\lceil \frac{n_c}{2} \right\rceil - \frac{s}{2} - k\right).$$

Also $\ell(\beta\hat{\omega}_C) = k$, so at $\delta = \beta$ there is a green conic of squareness k and

$$W_{m_{11},n_{11}}(\beta) = 2q^{-m_{11}+k}.$$

If it so happens that $b\pi^{n_c}$ *is* a square modulo $\pi^{e-\frac{s}{2}-\lceil\frac{n_c}{2}\rceil+1}$, then writing $\pi^{n_c}b = \left(\pi^{\lceil\frac{n_c}{2}\rceil}a\right)^2 + \pi^{2\tilde{n}}c$ and carrying out the above computations, *mutatis mutandis,* shows that

$$[\beta] \in T(\tilde{n}, e - 2\tilde{n}, \tilde{n})$$

and

$$\ell(\beta\hat{\omega}_C) \geq \tilde{n},$$

so there is a blue conic at β and

$$W_{m_{11},n_{11}} = q^{-m_{11}+\lfloor\frac{2e-s-n_c}{4}\rfloor}.$$

Overall,

$$W_{m_{11},n_{11}} \leq \sum_{\lfloor\frac{n_c}{2}\rfloor \leq \ell < \tilde{n}} q^{-m_{11}+\ell}(1+\varepsilon_C)F^\times\left(\ell, \left\lceil \frac{n_c}{2} \right\rceil + \frac{s}{2}, e - \left\lceil \frac{n_c}{2} \right\rceil - \frac{s}{2} - \ell\right) + q^{-m_{11}+\lfloor\frac{2e+s-n_c}{4}\rfloor} F(\tilde{n}, e-2\tilde{n}, \tilde{n})$$

This completes the bounding step. For the summing step, we note that $T^\times\left(\ell, \left\lceil \frac{n_c}{2} \right\rceil + \frac{s}{2}, e - \left\lceil \frac{n_c}{2} \right\rceil - \frac{s}{2} - \ell\right)$ is a union of cosets of $\mathcal{L}_{e-\ell-1}$ that do not lie in the charmed coset $\mathcal{L}_{\ell+1}$, so ε_C is equidistributed.

The summation then proceeds routinely. ■

Further remarks on the red zone. For general C, we end up proving that the coset $\psi_C^{-1}T$ is charmed for each $T = T(\ell_0, \ell_1, \ell_2)$ appearing (either positively or negatively) in the sum. Now $\psi_C \in 1 + B_{\theta_1}(\infty, \square_C)$, which, if

$$\ell_0 \leq \ell_C, \tag{171}$$

is contained in the box defining T. Thus the identity coset is charmed and we can replace G by F.

21.2.2 Splitting type 1^3

Lemma 21.5. *Suppose R has splitting type 1^3. Let m_{11} and n_{11} be rational numbers with*

$$m_{11} \in \mathbb{Z} - \frac{h}{3}, \quad n_{11} \in \mathbb{Z} + \frac{h}{3}, \quad m_{11} > 2e \geq n_{11} > 0.$$

Write

$$m^{\triangle} = m_{11} - \frac{2h}{3} \in \mathbb{Z}, \quad n^{\triangle} = n_{11} + \frac{2h}{3} \in \mathbb{Z}.$$

Let $\square_C = \min\{2\lfloor \ell(\hat{\omega}_C)/2 \rfloor + 1, e\}$ be the squareness of the $\delta = 1$ conic. Also let

$$\tilde{n} = \left\lfloor \frac{2e - n^{\triangle} + 2 + 2h}{4} \right\rfloor.$$

Then $W_{m_{11},n_{11}}$ is given as follows:

(a) *If $n_{11} > 2e$ (black zone), then*

$$W_{m_{11},n_{11}} = q^{2e-m_{11}-n_{11}+1} F(e, 0, 0).$$

(b) *If $2e - 2\square_C + 2 + \frac{4h}{3} \leq n_{11} \leq 2e$ and $n_{11} \geq \frac{2e}{3}$ (blue zone), then*

$$W_{m_{11},n_{11}} = q^{-m^{\triangle}+1-h+\left\lfloor \frac{2e-n^{\triangle}+2h}{4} \right\rfloor} F_h\left(\left\lfloor \frac{n^{\triangle}}{2} \right\rfloor, e - \left\lfloor \frac{n^{\triangle}}{2} \right\rfloor - \tilde{n}, \tilde{n} \right)$$

(c) *If* $\square_C + 1 - \dfrac{2h}{3} \le n_{11} \le 2e - 2\square_C + \dfrac{4h}{3}$ *(green zone), then*

$$W_{m_{11},n_{11}} = q^{-m^\triangle + \ell_C + 1 - h}(1+\varepsilon_C) F_h\left(\left\lfloor \frac{n^\triangle}{2} \right\rfloor, \ell_C - h + \mathbf{1}_{2\nmid n^\triangle}, e - \left\lceil \frac{n^\triangle}{2} \right\rceil - \ell_C + h\right)$$

where $\ell_C = \frac{\square_C - 1}{2} \in \mathbb{Z}_{\ge 0}$.

(d) *If* $n_{11} < \dfrac{2e}{3}$ *and* $n_{11} \le \square_C - \dfrac{2h}{3}$ *(red zone), then*

$$\begin{aligned} W_{m_{11},n_{11}} = &\sum_{\left\lfloor \frac{n^\triangle}{2} \right\rfloor \le \ell < \tilde{n}} q^{-m^\triangle + 1 - h + \ell}(1+\varepsilon_C) G_h^\times\left(\ell, \left\lceil \frac{n^\triangle}{2} \right\rceil - h, e - \left\lceil \frac{n^\triangle}{2} \right\rceil - \ell + h\right) + \\ &+ q^{-m^\triangle + 1 - h + \left\lfloor \frac{2e - n^\triangle + 2h}{4} \right\rfloor} G_h(\tilde{n}, e - 2\tilde{n}, \tilde{n}) \end{aligned}$$

Proof. By Lemma 18.4, the support of $W_{m_{11},n_{11}}$ consists of the classes $[\delta] = [\beta]$ in H^1 of elements β of the box

$$1 + B_{m_{11},n_{11}} = \{1 + y\pi^{n_{11}}\theta_1 + z\pi^{m_{11}}\theta_2, \quad x \in \mathcal{O}_K^\times, \quad y, z \in \mathcal{O}_K\}.$$

Since $m_{11} > 2e$, the z term has no effect on $[\beta]$, and we ignore it. In particular, the conic

$$\operatorname{coef}_{\theta_2}(\beta\xi^2) = 0, \quad \text{that is,} \quad \operatorname{tr}(\hat{\omega}_C \beta \xi^2) = 0$$

has a solution $\xi = 1$, so $\varepsilon(\hat{\omega}_C\beta) = 1$ for all β in the box.

In this case, Lemma 21.3 yields

$$\sum_{\delta \in \mathcal{L}_0} W_{m_{11},n_{11}}(\delta) = q^{2e - m_{11} - n_{11} + 1},$$

in particular verifying the total in the black zone.

Again, let $W'_{m_{11},n_{11}}$ denote the claimed value of $W_{m_{11},n_{11}}$ in each case. Our proof method will consist of bounding and summing, as in the preceding splitting types.

Blue zone. Our strategy is to note that

$$\beta \in 1 + B_{m_{11},n_{11}} \subseteq 1 + B_{m',n_{11}}$$

for some $m' \le m_{11}$ for which $[1 + B_{m',n_{11}}]$ is a boxgroup. Here, we find that the gray-blue condition (161) in Lemma 20.9 is the most stringent one, so we take

$$m'^{\triangle} = \left\lceil \frac{n^{\triangle} + 1}{2} \right\rceil + e - h \quad \text{and} \quad m' = m'^{\triangle} + \frac{2h}{3}$$

We easily verify that

$$e - \left\lfloor \frac{m^{\triangle}}{2} \right\rfloor = \tilde{n},$$

so $[1 + B_{\theta_1}(m', n_{11})]$ is exactly the support of $W'_{m_{11},n_{11}}$. We claim all conics are blue. This requires that the squareness

$$\square = \min\left\{ 2 \left\lfloor \frac{\ell(\beta\hat{\omega}_C)}{2} \right\rfloor + 1, e \right\}$$

satisfy

$$\square \overset{?}{\ge} e - n' = e - \left\lceil \frac{n^{\triangle}}{2} \right\rceil + h,$$

which simplifies to

$$\beta\hat{\omega}_C \in \mathcal{L}_{\left\lfloor \frac{2e - n^{\triangle} + 2h}{4} \right\rfloor}.$$

When $\beta = 1$, we have $\ell = \ell_C$, and the required relation follows from the given blue-green inequality $n_{11} \ge 2e - 2\square_C + 1 + \dfrac{4h}{3}$. So it suffices to show that

$$\beta \in \mathcal{L}_{\left\lfloor \frac{2e - n^{\triangle} + 2h}{4} \right\rfloor}.$$

Using the known relation $\ell(\beta) \geq 2\left\lfloor n^{\triangle}/2 \right\rfloor$ and the blue-red inequality $n_{11} \geq 2e/3$, this is not hard to prove. So all conics are blue, and the only possible nonzero value of $W_{m_{11},n_{11}}(\delta)$ is

$$q^{-m_{11}^{\odot}+\left\lfloor \frac{e-n'_{11}}{2} \right\rfloor} = q^{-m^{\triangle}+\left\lfloor \frac{2e-n^{\triangle}+2h}{4} \right\rfloor}.$$

This completes the bounding step. The summing step is routine.

This completes the proof, and in particular shows that $\varepsilon = 1$ identically on boxgroups of the shape in the lemma. This result will be important in proving the remaining zones.

Green zone. Again, we write

$$\beta \in 1 + B_{m_{11},n_{11}} \subseteq 1 + B_{m',n_{11}}$$

where m' is as large as possible to make a boxgroup. This time, we find that the gray-green inequality (160) is the most stringent of the conditions in Lemma 20.9, so we take $m' = n_{11} + \square_C - \frac{2h}{3}$, that is,

$$m'^{\triangle} = m_{11} - \frac{2h}{3} = n^{\triangle} + \square_C - 2h \in \mathbb{Z}.$$

and find that the support of $W_{m_{11},n_{11}}$ is contained in

$$[1 + B_{\theta_1}(m', n_{11})] = T_h\left(\left\lfloor \frac{n^{\triangle}}{2} \right\rfloor, \ell_C - h + \mathbf{1}_{2\nmid n^{\triangle}}, e - \left\lceil \frac{n^{\triangle}}{2} \right\rceil - \ell_C + h\right)$$

We claim all conics are green of the same squareness $\square_C$. It is easy to prove that $\square_C < e - 1$ in this zone, so

$$[\hat{\omega}_C \diamondsuit \heartsuit] \in \mathcal{L}_{2\ell_C} \setminus \mathcal{L}_{2\ell_C+2}.$$

We then note that $[\beta] \in \mathcal{L}_{2\ell_C+2}$, because $[\beta] \in \mathcal{L}_{2\lfloor n^{\triangle}/2 \rfloor}$ and we have the inequality $n^{\triangle} \geq 2\ell_C + 2$. So $[\beta\hat{\omega}_C \diamondsuit \heartsuit]$ is also of exact level $2\ell_C$ or $2\ell_C + 1$. Thus all conics are green of the same squareness,

and by Lemmas 19.9 and 19.10, we have the bound

$$W_{m_{11},n_{11}} \leq 2q^{-m^{\triangle}+1-h+\ell_C} F_h\left(\left\lfloor \frac{n^{\triangle}}{2} \right\rfloor, \ell_C - h + \mathbf{1}_{2\nmid n^{\triangle}}, e - \left\lceil \frac{n^{\triangle}}{2} \right\rceil - \ell_C + h\right),$$

indeed

$$W_{m_{11},n_{11}} \leq q^{-m^{\triangle}+1-h+\ell_C}(1+\varepsilon_C) F_h\left(\left\lfloor \frac{n^{\triangle}}{2} \right\rfloor, \ell_C - h + \mathbf{1}_{2\nmid n^{\triangle}}, e - \left\lceil \frac{n^{\triangle}}{2} \right\rceil - \ell_C + h\right).$$

This completes the bounding step.

To perform the summing step, we need to compute the sum of $q^{-m^{\triangle}+\ell_C}(1+\varepsilon_C)$ over the stated boxgroup. The term 1 is found to sum to the desired total $|H^0| \cdot q^{2e-m_{11}-n_{11}+h}$. We claim that

$$\sum_{\delta \in T\left(2\left\lfloor \frac{n^{\triangle}}{2} \right\rfloor + \frac{1-h}{2}, 2\ell_C - 1 - h + \mathbf{1}_{2\nmid n^{\triangle}}, 2e - 2\ell_C - 2\left\lceil \frac{n^{\triangle}}{2} \right\rceil + \frac{3h+1}{2}\right)} \varepsilon_C(\delta) = 0,$$

in other words that ε is equidistributed between 1 and -1 in this boxgroup. This follows from Lemma 20.13(b): because $\mathcal{L}_{2\ell_C+2} \neq \hat{\omega}_C \mathcal{L}_{2\ell_C+2}$ is an uncharmed coset, we have ε equidistributed on cosets of $\mathcal{L}_{2e-2\lfloor \ell_C \rfloor - 2}$, of which the boxgroup in question is a union by the green-blue inequality.

Red zone. Considerations of space prevent us from writing out the proof, which is like that in the unramified splitting types with the following changes:

- We reduce to the case that $\theta_1 = \eta^2$ is a square using Lemma 20.12, and there we will prove the result with the G's replaced by F's. We begin with an arbitrary

$$\beta = 1 + \pi^{n_{11}} b\theta_1 = 1 + \pi^{n^{\triangle}} b \cdot \pi^{-2h/3}\theta_1, \quad b \in \mathcal{O}_K.$$

- We assume first that $\pi^{n^{\triangle}} b$ is *not* a square modulo $\pi^{e-\left\lceil \frac{n^{\triangle}}{2} \right\rceil + 1 + h}$, and let k be the largest

integer such that $\pi^{n^\triangle} b$ is a square modulo π^{2k+1}. We find that

$$[\beta] \in T^\times \left(\ell, \left\lceil \frac{n^\triangle}{2} \right\rceil - h, e - \left\lceil \frac{n^\triangle}{2} \right\rceil - \ell + h \right)$$

is in the support of the kth term of the claimed answer and that there is a green conic of level k there.

- If $\pi^{n^\triangle} b$ in fact *is* a square modulo $\pi^{e - \lceil \frac{n_{11}}{2} \rceil + 1 + h}$, then we find that $[\beta]$ is in the support of the last term of the claimed answer and that there is a blue conic there.

The rest of the proof, including the summing step, is completely like the unramified splitting types.

■

The G's can be replaced by F's when the index k is at most ℓ_C, for reasons just like those named above. Another corollary is the following.

21.2.3 The level parity lemma

Note that in ramified splitting type, conics of given squareness $k < \lfloor e/2 \rfloor$ occur for $[\delta^\odot]$ of exactly two levels: $2k$ and $2k+1$. The following lemma tells when each occurs, at least when $\delta = 1$.

Lemma 21.6. *Take $\delta = 1$. If $[\delta^\odot] \notin \mathcal{L}_e$, then either*

- *$\delta^\odot$ has even level and $b_1 \in \mathbb{Z} + 1/3$, or*
- *$\delta^\odot$ has odd level and $b_1 \in \mathbb{Z} - 1/3$.*

Proof. Consider the first vector problem $\mathfrak{P}$ with the given θ_1, with $m_{11} > 2e$ and with $\mathcal{N}_{11}$ as minimally active as can be:

$$n_{11} = \begin{cases} 1/3, & b_1 \in \mathbb{Z} + 1/3 \\ 2/3, & b_1 \in \mathbb{Z} - 1/3. \end{cases}$$

This lies in the red zone, and we get an answer of the form (using ellipses to mark unimportant

portions)

$$W_{m_{11},n_{11}} = \sum_{0\le\ell<\lceil e/2\rceil} (\cdots)G_h^{\times}(\ell,\ldots) + (\cdots)G_h\left(\left\lceil\frac{e}{2}\right\rceil, -\mathbf{1}_{2\nmid e}, \left\lceil\frac{e}{2}\right\rceil\right).$$

Since $\ell(\delta^{\odot}) < e$, the black-red comparison shows that $\delta = 1$ lies in the support of the kth summand, $k = \ell_C = \lfloor \ell(\delta^{\odot})/2 \rfloor$. Now simply note that the kth summand consists entirely of elements of exact level $2k$ (for $h = 1$) or $2k+1$ (for $h = -1$). ■

21.3 The zones when $\mathcal{N}_{11}$ is weakly active (brown and yellow)

We now turn our attention to first vector problems such that N_{11} is weakly active and $m_{11} > 2e$. Here we use a significantly different framework. Note that $\bar{s} > 0$ induces a distinguished splitting $R = K \times Q$. The resolvent conditions $\mathcal{M}_{11}$ and $\mathcal{N}_{11}$ simplify to

$$\begin{aligned}\mathcal{M}_{11}\colon \operatorname{tr}(\xi_1^2) &\equiv 0 \mod \pi^{m_{11}}\\ \mathcal{N}_{11}\colon \quad \xi_1^{(K)} &\equiv 0 \mod \pi^{n_{11}/2}\end{aligned}$$

For ξ_1 to satisfy this, its two Q-components must be units. Under the transformation of Lemma 19.3, the conditions can also be written as

$$\begin{aligned}\mathcal{M}_{11}\colon \operatorname{tr}(\delta^{\odot}{\xi_1^{\odot}}^2) &\equiv 0 \mod \pi^{m_{11}^{\odot}}\\ \mathcal{N}_{11}\colon \qquad \xi_1^{\odot(K)} &\equiv 0 \mod \pi^{\frac{n_{11}}{2}-v^{(K)}(\gamma\gamma^{\odot})}\\ \iff \qquad \xi_1^{\odot(K)} &\equiv 0 \mod \pi^{\left\lceil\frac{n_{11}}{2}-v^{(K)}(\gamma\gamma^{\odot})\right\rceil}.\end{aligned}$$

For simplicity we let

$$n_{11}^{\odot} = \left\lceil \frac{n_{11}}{2} - v^{(K)}(\gamma\gamma^{\odot})\right\rceil,$$

which sometimes differs slightly from the $n^{\odot}$ of Lemma 19.18.

In each of the three applicable splitting types, we will find a *brown zone* where n_{11} is so high that $\xi_1^{\odot(K)}$ can be taken to be 0, so the only $\delta^{\odot}$ for which there is a solution are those where $\delta^{(Q)}$

is the class of an element on the traceless line of Q. Let $\clubsuit$ be such an element of the form

$$\clubsuit = (\alpha + \bar{\alpha}; \alpha - \bar{\alpha}; \bar{\alpha} - \alpha)$$

where α is a generator for $\mathcal{O}_Q$ as an $\mathcal{O}_K$-module. Remarks are in order:

- In splitting type (111), we can take $\clubsuit = (1; 1; -1)$.
- In splitting type (12), we can take $\alpha = (1 + \sqrt{D_0})/2$, giving $\clubsuit = (1; \bar{\zeta}_2\sqrt{D_0})$.

Denote by $Y_{\mathfrak{P}}(\delta^{\clubsuit})$ the volume of ξ_1' satisfying the $\mathcal{M}_{11}$ and $\mathcal{N}_{11}$ conditions when

$$[\delta^{\clubsuit}] = [\hat{\omega}_C \clubsuit \delta],$$

that is,

$$Y_{\mathfrak{P}}(\delta^{\clubsuit}) = W_{\mathfrak{P}}\left(\hat{\omega}_C \clubsuit \delta^{\clubsuit}\right).$$

Observe that the dependence on θ_1 has been nullified and, if $m_{11}^{\odot} > 2e$, that $Y_{\mathfrak{P}}$ is supported on the vanishing locus of the quadratic form

$$\varepsilon^{\clubsuit}(\delta^{\clubsuit}) \coloneqq \varepsilon(\clubsuit \delta^{\clubsuit}).$$

Let $Y_{\mathfrak{P}}^{\odot}$ be the corresponding volume of $\xi_1^{\odot}$.

As in the strong zones, we need a summation lemma.

Lemma 21.7. *We have*

$$\sum_{\delta^{\clubsuit} \in \delta_0^{\clubsuit} \mathcal{L}_0} Y_{\mathfrak{P}}(\delta^{\clubsuit}) = |H^0| q^{2e - m_{11}^{\odot} - n_{11}^{\odot} + 2v_K\left(\delta^{\odot}(Q)\right)},$$

where $m_{11}^{\odot}$, γ, and $\delta^{\odot}$ are given by Lemma 19.3 and depend only on the class $\delta^{\clubsuit}\mathcal{L}_0 \in H^1/\mathcal{L}_0$.

Proof. Since $\xi_1^{(Q)}$ must be a unit, $\xi_1^{\odot(Q)}$ has fixed valuation

$$v^{(Q))}\left(\xi_1^{\odot}\right) = -v^{(Q)}\left(\gamma\gamma^{\odot}\right) =: r.$$

Meanwhile, $v\left(\xi_1^{\odot(K)}\right) \geq n_{11}^{\odot}$ can vary. For $i \geq n_{11}^{\odot}$, let $Y_{\mathfrak{P}}^{(i)}(\delta^{\clubsuit})$ denote the volume of $\xi_1^{\odot}$ satisfying the first vector problem $\mathfrak{P}$ and having $v_K(\xi^{\odot(K)}) = i$. We have

$$Y_{\mathfrak{P}} = \sum_{i=i_0}^{\infty} Y_{\mathfrak{P}}^{(i)},$$

since only the measure-zero set where $\xi^{\odot(K)} = 0$ has been dropped. Let

$$\beta = \delta^{\odot}{\xi^{\odot}}^2 \cdot \pi^{2r} \tag{172}$$

Observe that $2r$ is an integer (by reference to (134)) so $\beta \in R$. Moreover, as we vary $[\delta^{\clubsuit}] \in \delta^{\clubsuit}\mathcal{L}_0$ and $\xi_1^{\odot}$ in the set whose volume is $Y_{m_{11},n_{11}}^{(i)}$, we get that β varies in the region of primitive members of $\mathcal{O}_R$ such that

$$\begin{aligned} v_K(\beta^{(K)}) &= v_K\left(\delta^{\odot(K)}\right) + 2i - 2r \\ v_K(\beta^{Q}) &= 0 \\ \lambda^{\diamondsuit}(\beta) &\equiv 0 \mod \pi^{m_{11}^{\odot}+2r}. \end{aligned}$$

Conditions of the form $\beta^{(K)} \equiv 0 \mod \pi^{n_{11}}$ and $\lambda^{\diamondsuit}(\beta) \equiv 0 \mod \pi^{m_{11}}$ cut out a box of volume $q^{-m_{11}-n_{11}}$; so the volume of β is

$$\begin{aligned} &\left(1 - \frac{1}{q}\right) q^{-\left(v_K\left(\delta^{\odot(K)}\right)+2i+2r\right)-\left(m_{11}^{\odot}-2r\right)} \\ &= \left(1 - \frac{1}{q}\right) q^{-2i-m_{11}^{\odot}-v_K\left(\delta^{\odot(K)}\right)+4r}. \end{aligned}$$

Consider the sequence

$$\xi' \longmapsto \frac{\xi'}{\left(\pi^i;\pi_Q^{2r}\right)} \longmapsto \frac{\xi'^2}{\left(\pi^{2i};\pi_Q^{4r}\right)} \longmapsto \frac{\delta^{\odot}\xi'^2}{\pi^{2r}} = \beta.$$

Every term is a primitive vector in $\mathcal{O}_R$, so we can consider projective volumes. The linear map of dividing by $\left(\pi^i;\pi_Q^{2r}\right)$ scales volumes by q^{i+2r}. Squaring by units scales volumes by $1/\left(|H^0|\cdot q^{2e}\right)$ on regions symmetric under multiplication by $R^{\times}[2]$, as we noted above in the proof of Lemma 21.3. Finally, multiplication by

$$\frac{\delta^{\odot}\cdot\left(\pi^{2i};\pi_Q^{4r}\right)}{\pi^{2r}}$$

scales volumes by

$$q^{-v_K\left(\delta^{\odot(K)}\right)-2v_K\left(\delta^{\odot(Q)}\right)-2i+2r}.$$

So overall, a volume $Y_{\mathfrak{P}}^{(i)}(\delta)$ of ξ' transforms to a volume of

$$\frac{1}{|H^0|}q^{-2e-i-v_K\left(\delta^{\odot(K)}\right)-2v_K\left(\delta^{\odot(Q)}\right)+4r}Y_{\mathfrak{P}}^{(i)}(\delta).$$

Summing over $[\delta]\in\delta_0\mathcal{L}_0$,

$$\frac{1}{|H^0|}q^{-2e-i-v_K\left(\delta^{\odot(K)}\right)-2v_K\left(\delta^{\odot(Q)}\right)+4r}\sum_{\delta\in\delta_0\mathcal{L}_0}Y_{\mathfrak{P}}^{(i)}(\delta)=\left(1-\frac{1}{q}\right)q^{-2i-m_{11}^{\odot}-v_K\left(\delta^{\odot(K)}\right)+4r},$$

that is,

$$\sum_{\delta\in\delta_0\mathcal{L}_0}Y_{\mathfrak{P}}^{(i)}(\delta)=\left(1-\frac{1}{q}\right)q^{2e-i-m_{11}^{\odot}+2v_K\left(\delta^{\odot(Q)}\right)}.$$

Summing over $i\geq n_{11}^{\odot}$, the right-hand side becomes a geometric series and we get

$$\sum_{\delta\in\delta_0\mathcal{L}_0}Y_{\mathfrak{P}}(\delta)=q^{2e-m_{11}^{\odot}-n_{11}^{\odot}+2v_K\left(\delta^{\odot(Q)}\right)},$$

as desired. ■

We now use this to power the summing step in each splitting type.

21.3.1 Unramified

Here $\clubsuit = (1; \bar{\zeta}_2\sqrt{D_0})$, where D_0 is scaled so that $D_0 \equiv 1 \mod 4$. Observe that $\clubsuit^Q$ is traceless.

Lemma 21.8. *There is an $\alpha_0 \in \mathcal{O}_Q$ such that*

$$\ker\left(\mathrm{tr}_{\mathcal{O}_R/\mathcal{O}_K}\right) = \left\langle \clubsuit(0;1), \clubsuit(1;\alpha_0^2)\right\rangle$$

as $\mathcal{O}_K$-modules.

Proof. This is a notable example of a lemma of simple form that can be proved using the machinery we have got. (Incidentally, if R is totally split, the choice $\alpha_0 = (0;1)$ works, so we're really only concerned about splitting type (12): but we have no need to separate the splitting types here.)

The conic

$$\mathcal{A}(\xi) = \mathrm{tr}(\clubsuit\xi^2)$$

has determinant 1. Since $\clubsuit \equiv 1 \mod 2$, $\mathcal{A}$ has maximal squareness $\lfloor e/2 \rfloor$. It has Brauer class $\varepsilon(\mathcal{A}) = 1$, since $\xi = (0;1)$ is a solution. Hence, by Lemma 19.9, not all the $\mathcal{O}_K$-points of $\mathcal{A}$ lie in a single 1-pixel. The reduction of $\mathcal{A}$ modulo π consists of $(q+1)$-many 1-pixels, only one of which has vanishing K-coordinate. Hence there is a solution $\xi = (a;\alpha)$ with $\pi \nmid a$. Rescaling, we can take $a = 1$. ∎

Lemma 21.9. *In splitting types* 111 *and* 12. *If $h_1 = 0$, let*

$$\tilde{n} = \left\lfloor \frac{2e - n_{11} + 2}{4} \right\rfloor = \left\lceil \frac{e - n_{11}^{\odot}}{2} \right\rceil.$$

Then $Y_{\mathfrak{P}}$ is given in terms of $n_{11} = n_{11}$ and as follows:

(a) If $n_{11} > 2e$ (brown zone), then

$$Y_{\mathfrak{P}} = \begin{cases} 2q^{e-m_{11}-n_{11}^{\odot}} F\left(0, e, \emptyset\right) & [\delta_0^{\clubsuit}] \in \mathcal{L}_0 \\ 2q^{e-m_{11}-n_{11}^{\odot}} xF\left(0, e, \emptyset\right) & [\delta_0^{\clubsuit}] \in (1;\pi;\pi)\mathcal{L}_0 \end{cases}$$

(*b*) *If* $0 < n_{11} \leq 2e$ *(yellow zone), then*

$$Y_{\mathfrak{P}} = \begin{cases} \displaystyle\sum_{0 \leq \ell < \tilde{n}} q^{-m_{11}+\ell}(1+\varepsilon^{\clubsuit})F^{\times}\left(\ell, n_{11}^{\odot}, e - n_{11}^{\odot} - \ell\right) + q^{-m_{11}+\left\lfloor \frac{2e-n_{11}}{4} \right\rfloor} F(\tilde{n}, e-2\tilde{n}, \tilde{n}), & h_1 = 0 \\ q^{-m_{11}}(1+\varepsilon^{\clubsuit})xF\left(0, n_{11}^{\odot}, e - n_{11}^{\odot}\right) & h_1 = 1. \end{cases}$$

Proof. In the brown zone, the conditions imply that

$$(\delta^{\odot}\xi^{\odot 2})^{Q} \equiv a^{\clubsuit} \mod \pi^{2e+1}$$

for some $a \in \mathcal{O}_K$, necessarily in $\mathcal{O}_K^{\times}$. So $[\delta^{\odot}] \in {}^{\clubsuit}\iota(K) = {}^{\clubsuit}T(\emptyset, e, \emptyset)$. It's easy to see that all values occur, and the solution volume is constant within the appropriate coarse coset, because the K-coordinate of $\beta = \delta^{\odot}\xi^{\odot 2}/\pi^{h_1}$ can range over all of $\pi^n\mathcal{O}_K^{\times}$ (for $n \geq 2n_{11}^{\odot} - h_1$ of the correct parity) while $\beta^{(Q)} \equiv {}^{\clubsuit}(Q) \mod \pi^{2e+1}$ remains of constant class. So

$$Y_{\mathfrak{P}}(\delta^{\clubsuit}) = 2q^{e-m_{11}-n_{11}^{\odot}}$$

for each $\delta^{\clubsuit}$ in the support, as desired.

In particular, $T(\emptyset, e, \emptyset)$ is charmed for $\varepsilon^{\clubsuit}$.

In the yellow zone, the conditions imply that

$$\beta^{Q} \equiv a^{\clubsuit} \mod \pi^{2n_{11}^{\odot}+h_1}$$

for some a in $\mathcal{O}_K$, necessarily in $\mathcal{O}_K^{\times}$. Hence

$$[\delta^{\clubsuit}] \in \begin{cases} \varepsilon^{\clubsuit -1}(1) \cap T^{\times}\left(\emptyset, n_{11}^{\odot}, e - n_{11}^{\odot}\right) & h_1 = 1 \\ \varepsilon^{\clubsuit -1}(1) \cap T\left(0, n_{11}^{\odot}, e - n_{11}^{\odot}\right) & h_1 = 0. \end{cases}$$

Note that the boxgroups have $\ell_1 = n_{11}^{\odot} \leq \lceil s/2 \rceil$, so they are well defined. Also, $F = G$ in the answer, because everything contains $\iota(K^{\times}) \cdot \mathcal{L}_e$, which is charmed for $\varepsilon^{\clubsuit}$.

In the case $h_1 = 1$, the conics are all tiny and green, and we get the bound

$$Y_{\mathfrak{P}} \leq q^{-m_{11}}(1+\varepsilon^{\clubsuit})xF\left(0, n_{11}^{\odot}, e - n_{11}^{\odot}\right),$$

which is exactly as desired. The summing step precedes routinely, noting that $\varepsilon^{\clubsuit}$ is equidistributed because everything is contained in a non-charmed coarse coset.

In the case $h_1 = 0$, that is, $[\delta^{\odot}] \in \mathcal{L}_0$, some further analysis must be done to narrow the support. By Lemma 19.6, we can assume that $\mathcal{M}_{11}$ is an equality on the nose and also that the K-component of ξ' is not *exactly* 0 (to allow recovery of $[\delta^{\clubsuit}] = [\delta^{\odot} \diamondsuit \clubsuit \xi'^2]$). Then $\mathrm{tr}(\delta^{\odot}\xi'^2) = 0$, so there are $u \in \mathcal{O}_K^{\times}$, $b \in \mathcal{O}_K$ such that

$$\delta^{\clubsuit}\xi'^2 = u(0;1) + b\pi^{2n'}(1;\alpha_0^2).$$

Hence we are curious about the H^1-class of the right-hand side. Since scaling by $K^{\times}$ preserves H^1-class, we may assume that $u = 1$. We have $b \neq 0$.

Assume first that b is *not* a square modulo $\pi^{v_K(b)+2\tilde{n}}$. Write

$$b = a^2(1+\pi^{2k+1}c), \quad \pi \nmid c, \quad 0 \leq k < \tilde{n}.$$

We will show that $[\delta^{\clubsuit}]$ lies in the kth term

$$T^{\times}\left(k, n_{11}^{\odot}, e - n_{11}^{\odot} - k\right).$$

We compute:

$$\begin{aligned}
[\delta^{\clubsuit}] &= [(0;1) + b\pi^{2n_{11}^{\odot}}(1;\alpha_0^2)] \\
&= [(b; 1 + b\pi^{2n_{11}^{\odot}}\alpha_0^2)] \\
&= [1 + c\pi^{2k+1}; 1 + a^2\pi^{2n_{11}^{\odot}}\alpha_0^2 + a^2 c\pi^{2n_{11}^{\odot}+2k+1}\alpha_0^2] \\
&\equiv [1 + c\pi^{2k+1}; 1 + a^2\pi^{2n_{11}^{\odot}}\alpha_0^2] \mod \mathcal{L}_{k+n_{11}^{\odot}} \\
&\equiv [1 + c\pi^{2k+1}; (1 + a\pi^{n_{11}^{\odot}}\alpha_0)^2] \mod \mathcal{L}_{\lceil (e+n_{11}^{\odot})/2 \rceil} \subseteq \mathcal{L}_{k+n_{11}^{\odot}} \\
&= [1 + c\pi^{2k+1}; 1] \\
&\in T^{\times}\left(k, n_{11}^{\odot}, e - n_{11}^{\odot} - k\right).
\end{aligned}$$

Also, the conics here are green of squareness k. Likewise, if b *is* a square modulo $\pi^{v_K(b)+2\tilde{n}}$, the same computation shows that $[\delta^{\clubsuit}] \in S(\tilde{n}, e-2\tilde{n}, \tilde{n})$. Here the conics are blue, and we have the bounding step.

For the summing step, we note that ε is equidistributed on each support $T^{\times}(\ell, n_{11}^{\odot}, e - n_{11}^{\odot} - \ell)$, since it is a union of cosets of $\mathcal{L}_{e-\ell-1}$ inside a non-charmed coset of $\mathcal{L}_{\ell+1}$. The sum is then easy to compute and compare against the total of Lemma 21.7. ■

When we translate back to W's counting the volumes by the value of δ, the answers change but slightly. In the brown zone, the support is contained in $\hat{\omega}_C \clubsuit \iota(K)$, but using $s > 2e$ (or the black-brown comparison, when the chosen coarse coset is $\mathcal{L}_0$), this coset is the identity. Intersecting this with the two possible coarse cosets yields the answers

$$W_{\mathfrak{P}} = \begin{cases}
2q^{e-m_{11}-\lceil n_{11}/2 \rceil} F(0, e, \emptyset) & [\delta] \in \mathcal{L}_0, & s \text{ even} \\
2q^{e-m_{11}-\lceil n_{11}/2 \rceil} xF(0, e, \emptyset) & [\delta] \in (1;\pi;\pi)\mathcal{L}_0, & s \text{ odd} \\
2q^{e-m_{11}-\lfloor n_{11}/2 \rfloor} F(0, e, \emptyset) & [\delta] \in \mathcal{L}_0, & s \text{ odd} \\
2q^{e-m_{11}-\lfloor n_{11}/2 \rfloor} xF(0, e, \emptyset) & [\delta] \in (1;\pi;\pi)\mathcal{L}_0, & s \text{ even}
\end{cases}$$

Further remarks on the yellow zone. In the "long" yellow zone answer ($h_1 = 0$), the F's can be changed to G's, because the answer implies that $T(\tilde{n}, e - 2\tilde{n}, \tilde{n})$ is charmed. When translating from Y back to W, we keep these G's, switching quadratic forms from $\varepsilon^{\clubsuit}$ to ε_C. However, some of these G's and xG's admit simplifications that are of importance to us.

- If $h = 1$ and s is odd, the fact that $\delta = 1$ yields a nonzero ring volume implies that the xG simplifies to F:

$$W_{m_{11},n_{11}} = q^{-m_{11}}(1 + \varepsilon_C)F\left(0, \left\lfloor \frac{n_{11}}{2} \right\rfloor, e - \left\lfloor \frac{n_{11}}{2} \right\rfloor\right)$$

- Still assuming $h = 1$ and s is odd, in the very special case that $n_{11} = 2e$ (on the yellow-brown border), the term

$$\varepsilon_C F(0, e, 0)$$

  admits a curious simplification. Since the charmed coset of $T(0, e, 0)$ is $T^{\times}(\emptyset, e, 0)$, we have

$$G(0, e, 0) = xF(0, e, 0).$$

  Taking Fourier transforms of both sides,

$$\varepsilon_C F(0, e, 0) = Fx(0, e, 0).$$

  This accounts for the "Fx-yellow-special" zone in the code.

- If $h = 1$ and s is even, we claim that the xG simplifies to xF. Note that $\hat{\omega}_C$ is constrained by s: we have $\theta_1 \equiv (1; 0; 0) \mod \pi^s$, so $\omega \equiv (0; \clubsuit^Q) \mod \pi^s$ and

$$[\hat{\omega}_C \clubsuit] \in \iota(K^{\times}) \cdot (1 + \pi^s \mathcal{O}_R) \subseteq \cdot(1 + \pi^{n_{11}} \mathcal{O}_R) = T\left(\emptyset, \left\lfloor \frac{n_{11}}{2} \right\rfloor, e - \left\lfloor \frac{n_{11}}{2} \right\rfloor\right).$$

  So the regions in which $\delta^{\clubsuit}$ lay are also good for δ.

- If $h = 0$ and s is even, then $\delta = 1$ must also lie in some term of the sum. Which term it is can

be determined using the levels of the conics. If

$$\ell_C \geq \tilde{n},$$

then $\delta = 1$ lies in the last term and all G's can be made F's. Otherwise, the terms for

$$\ell \leq \ell_C$$

so simplify.

21.4 The beige zone

21.4.1 Unramified

The following is immediate from Lemmas 19.9, 19.10, and 19.14.

Lemma 21.10. *In unramified splitting type, if $m_{11} > 2e$ but $\mathcal{N}_{11}$ is inactive (beige zone), then the ring volume for ξ_1' is given by*

$$W_{m_{11},0} = \begin{cases} q^{-m_{11}} \left[(1+\varepsilon_C) \sum_{0 \leq \ell \leq \lfloor \frac{e}{2} \rfloor - 1} q^{\ell} G^{\times\times}(\ell, 0, e-\ell) + (\textit{core}) \right] & [\delta^{\odot}] \in \mathcal{L}_0 \\ q^{-m_{11}}(1+\varepsilon_C)\big(xG(0,0,e) + xxG(0,0,e)\big) & [\delta^{\odot}] \notin \mathcal{L}_0 \end{cases}$$

where

$$(\textit{core}) = \begin{cases} q^{\frac{e}{2}} \left(1 + \frac{1}{q}\right) G\left(\frac{e}{2}, 0, \frac{e}{2}\right) & e \text{ even} \\ q^{\frac{e-1}{2}} (1+\varepsilon_C) G\left(\frac{e-1}{2}, 0, \frac{e+1}{2}\right) & e \text{ odd} \end{cases}$$

Further remarks on the beige zone. In the unramified $h = 1$ case, the answer would more strictly be written as a restriction to the particular coarse coset specified by the discrete data, but we do not do so, as all $(|H^0| - 1)$-many non-charmed coarse cosets admit the same extender indices

and will be immediately summed. We know which coset of $\mathcal{L}_0$ is charmed, and hence:

$$xG(0,0,e) + xxG(0,0,e) = \begin{cases} xF(0,0,e) + xxF(0,0,e) & s \text{ even} \\ F(0,0,e) + xxF(0,0,e) & s \text{ odd.} \end{cases}$$

21.4.2 Splitting type 1^3

Here, a little more care is required to deal with the restrictions on the valuation of $\xi^{\odot}$ that remain active in the beige zone.

We first use a summation lemma. (We could have proved a summation lemma in the unramified splitting type, but it was unnecessary for finding the answers.)

Lemma 21.11. *In splitting type 1^3, let $m_{11} > 0$. Then*

$$\sum_{\delta \in H^1} W_{m_{11},0} = q^{2e + \frac{h-1}{2} - m_{11}^{\triangle}}.$$

Proof. Analogous to Lemma 21.3, map each $\xi' \in \mathcal{O}_R^{\times}$ in the solution set to a corresponding $\beta = \delta^{\odot}\xi'^2$. The $\mathcal{M}_{11}$-condition restricts β to a space of volume $q^{\frac{h-1}{2} - m_{11}^{\triangle}}$, and the squaring multiplies projective volumes by q^{-2e}, establishing the result. ∎

Lemma 21.12. *In splitting type 1^3, a first vector problem with $m_{11} > 2e$ and $n_{11} \leq 0$ (beige zone) has the answer, for $h_1 = 1$,*

$$W_{m_{11},0} = q^{-m_{11}^{\triangle}}(1+\varepsilon_C) \sum_{k=0}^{\lceil e/2 \rceil - 1} q^k \big(G_1(k,0,e-k) - G_1(k+1,-1,e-k) \big) + \\ + q^{-m_{11}^{\triangle} + \lceil e/2 \rceil} G_1\left(\left\lceil \frac{e}{2} \right\rceil, -\mathbf{1}_{2\nmid e}, \left\lceil \frac{e}{2} \right\rceil \right)$$

and, for $h_1 = -1$,

$$W_{m_{11},0} = q^{-m_{11}^{\triangle}+2}(1+\varepsilon_C) \sum_{k=0}^{\lfloor e/2 \rfloor - 1} q^k \big(G_{-1}(k,1,e-k-1) - G_{-1}(k+1,0,e-k-1) \big) + \\ + q^{-m_{11}^{\triangle}+2+\lfloor e/2 \rfloor} G_{-1}\left(\left\lfloor \frac{e}{2} \right\rfloor, \mathbf{1}_{2\nmid e}, \left\lfloor \frac{e}{2} \right\rfloor \right).$$

Proof. Since $\mathcal{L}_e$ is charmed for ε, all of the G's can be viewed as selectors for the coset of the indicated boxgroup containing $[\hat{\omega}_C]$.

For each $[\delta^\odot] = [\delta\hat{\omega}_C]$ with $\varepsilon(\delta^\odot) = 1$, the conic $\mathcal{M}_{\delta^\odot} : \lambda^\diamondsuit(\delta^\odot {\xi^\odot}^2)$ has *some* rational point $\xi^\odot$. Let h' be the value of h_1 to which $\xi^\odot$ contributes to the beige-zone answer:

$$h' = \begin{cases} 1 & \xi^\odot \sim 1 \text{ (here } \xi^\odot \text{ lies in a } \textit{generic} \text{ 1-pixel)} \\ -1 & \xi^\odot \sim \pi_R^2 \text{ (here } \xi^\odot \text{ lies in the } \textit{special} \text{ 1-pixel)} \end{cases}$$

(A potential third case $\xi^\odot \sim \pi_R$ does not satisfy $\mathcal{M}_{\delta^\odot}$ even mod π.) Then let $\theta_1' \in \bar{\zeta}_3^{h'} R$ whose associated traceless $\omega_{\theta_1'}$ is the known

$$\omega' = \frac{\diamondsuit \delta^\odot {\xi^\odot}^2}{\pi^{4+2h}}$$

When $[\delta^\odot] = [\delta\hat{\omega}_C] \notin \mathcal{L}_{2\lfloor e/2 \rfloor}$, the corresponding conic $\mathcal{M}_{\delta^\odot}$ has squareness $k < \lfloor e/2 \rfloor$. The solutions to the conic lie in a single 1-pixel, which must be either generic or special. By the level parity result in Lemma 21.6 applied to θ_1', values with $\ell(\delta^\odot)$ even and odd give the generic and special pixels respectively. This establishes the claimed result when $[\delta^\odot] \notin \mathcal{L}_{2\lfloor e/2 \rfloor}$, which corresponds to the terms $k \leq \lfloor e/2 \rfloor - 1$ of each sum.

We now turn to the case that $[\delta^\odot] \in \mathcal{L}_{2\lfloor e/2 \rfloor}$, so the conic has squareness $\lfloor e/2 \rfloor$. Refer to Lemma 19.9 for the analysis of conics. If e is even, the conic has solutions in $(q+1)$-many 1-pixels. These form the line in $\mathbb{P}(\mathcal{O}_R/\pi\mathcal{O}_R)$ given by reducing the conic mod π; they are q generic and 1 special. Because the conic has equal volume in each 1-pixel, the volume can be computed explicitly and contributes

$$q^{-m_{11}^{\triangle} + e/2} G_1\left(\frac{e}{2}, 0, \frac{e}{2}\right)$$

to the $h_1 = 1$ case and q times as much to the $h_1 = -1$ case (the special pixel gets inflated by q in the $\xi^\odot \mapsto \xi'$ transition), as desired.

If e is odd, the conic has solutions in two 1-pixels and we need to know whether one of them is special. For $\delta^\odot$ of *exact* level $e-1$, we know, again by Lemma 21.6, that both pixels are generic. For

$\delta^{\odot} \in \mathcal{L}_e$, we get *at least* one generic pixel and *at most* one special pixel, leading to the inequalities

$$\begin{aligned} W^{h_1=1}_{m_{11},0}\big|_{\hat{\omega}_C\mathcal{L}_{e-1}} &\geq q^{-m_{11}^{\triangle}+(e-1)/2}(1+\varepsilon_C)\left(G_{-1}\left(\frac{e-1}{2},0,\frac{e+1}{2}\right)-\frac{1}{2}G_{-1}\left(\frac{e-1}{2},1,\frac{e-1}{2}\right)\right) \\ &= q^{-m_{11}^{\triangle}+(e-1)/2}(1+\varepsilon_C)\left(G_{-1}\left(\frac{e-1}{2},0,\frac{e+1}{2}\right)-G_{-1}\left(\frac{e-1}{2},1,\frac{e-1}{2}\right)\right)+ \\ &\quad + q^{-m_{11}^{\triangle}+(e-1)/2}G_{-1}\left(\frac{e-1}{2},1,\frac{e-1}{2}\right) \end{aligned}$$

and

$$W^{h_1=-1}_{m_{11},0}\big|_{\hat{\omega}_C\mathcal{L}_{e-1}} \leq q^{-m_{11}^{\triangle}+2+(e-1)/2}G_{-1}\left(\frac{e-1}{2},1,\frac{e-1}{2}\right).$$

Then, summing and comparing against Lemma 21.11, we find that equality must hold. ∎

21.5 Orthogonality

Before proceeding to first-vector problems with $m_{11} \leq 2e$, we prove the following result, which will enable us to compute Fourier transforms of ring totals.

Lemma 21.13. *For any boxgroup $T_{\theta_1}(\ell_0,\ell_1,\ell_2)$, its orthogonal complement is given by $T_{\theta_1}(\ell_2,\ell_1,\ell_0)$.*

Remark 21.14. This is an example of an *explicit reciprocity law*, that is, a formula for the Hilbert symbol in a certain region. There is a wide literature on explicit reciprocity laws, but we suspect that this one is new. In our proof, the only fact we use about the Hilbert pairing is that it is the associated bilinear form to ε (and ε_C). This enables us to use various facts about ε gleaned in the preceding sections. We will be concocting various values of the resolvent datum θ_1 and of the discrete datum n_{11} to plug into the lemmas regarding the ring volumes.

Proof of Lemma 21.13. We carry out the proof in the unramified splitting type only, the proof in the other types being very similar.

We first note that if any of ℓ_0,ℓ_1,ℓ_2 is the symbol $\emptyset$, the result follows easily from the self-orthogonality of $\iota(K^{\times})$ (if applicable), as mentioned above. So we can assume that the ℓ_i are

integers. By definition, they must satisfy

$$\ell_0 + \ell_1 + \ell_2 = e \tag{173}$$

$$\ell_1 \leq \ell_0 + \frac{s}{2} + 1 \qquad \text{(the gray-red inequality)} \tag{174}$$

$$\ell_1 \leq \frac{s + \square_C + 1}{2} \qquad \text{(the gray-green inequality)} \tag{175}$$

$$\ell_1 \leq \ell_2 + \frac{s}{2} + 1, \qquad \text{(the gray-blue inequality)} \tag{176}$$

We first reduce to the case $\square_C = e$. If s is even, this is accomplished, as in the proof of the red zone, by replacing θ_1 by $\theta_1' = \eta^2$ and noting that, by the gray-green inequality, the boxgroups $T_{\theta_1}(\cdots) = T_{\theta_1'}(\cdots)$ are unchanged. If s is odd, we simply replace θ_1 by a $\theta_1' \equiv (1;0;0) \mod \pi^{\max\{2e+1,s\}}$ whose corresponding $\hat{\omega}_{C'}$ is in $\mathcal{L}_{\lfloor e/2 \rfloor}$. (For example, $\theta_1' = (1; 8\pi^{2s}\bar{\zeta}_2\sqrt{D_0}))$ is found to work.) Then since $\theta_1' \equiv \theta_1 \mod \pi^s$ and all boxgroups satisfy the gray-green inequality $\ell_1 \leq (s+1)/2$, the boxgroups are unchanged. Incidentally, we can also assume as a result of this reduction that s is even.

Now the gray-green inequality is subsumed by the gray-blue and gray-red ones. Using $\mathcal{L}_i^\perp = \mathcal{L}_{e-i}$, the truth of the lemma for a triple (ℓ_0, ℓ_1, ℓ_2), $\ell_1 \geq 1$, implies its truth for the triples $(\ell_0+1, \ell_1-1, \ell_2)$ and $(\ell_0, \ell_1 - 1, \ell_2 + 1)$. Hence we can run these reductions backward, increasing ℓ_1 until we reach an obstruction. This usually happens if either the gray-blue or the gray-red inequality becomes an equality, but it can also happen in two special cases, which we dispatch now:

- $\ell_0 = \ell_2 = 0$. Here $s \geq 2e - 2$, and the self-orthogonality of $T(0, e, 0)$ follows from that of $T(\emptyset, e, \emptyset) = \iota(K^\times)$, unless $e = 1$ and $s = 0$, in which case the gray-blue and gray-red inequalities are also equalities.

- Both the gray-blue and gray-red inequalities are 1 away from equality, that is,

$$(\ell_0, \ell_1, \ell_2) = \left(\frac{2e - s}{6}, \frac{e + s}{3}, \frac{2e - s}{6} \right).$$

  As we see, this is only possible if $2e \equiv s \mod 3$. This space shows up as the support in the

blue zone for the first vector problem

$$m_{11} = 2e + 1, \quad n_{11} - s = \frac{2e - s}{3},$$

right on the blue-red boundary. It is therefore isotropic and, by virtue of its size, maximal isotropic.

So we are left with the case that, without loss of generality, the gray-blue inequality is an equality

$$\ell_1 = \ell_2 + \frac{s}{2} + 1.$$

We thus have

$$(\ell_0, \ell_1, \ell_2) = \left(e - 2\ell_2 - \frac{s}{2} - 1, \ell_2 + \frac{s}{2} + 1, \ell_2\right).$$

Let $V = T(\ell_0, \ell_1, \ell_2)$ and $W = T(\ell_2, \ell_1, \ell_0)$ be the claimed orthogonals. By the gray-red inequality, $\ell_0 \geq \ell_2$ and $V \subseteq W$.

If $\ell_0 = \ell_2$, we again have a unique group

$$(\ell_0, \ell_1, \ell_2) = \left(\frac{2e - s - 2}{6}, \frac{e + s + 2}{3}, \frac{2e - s - 2}{6}\right)$$

which shows up as the support in the blue zone for the first vector problem

$$m_{11} = 2e + 1, \quad n_c = \frac{2e - s - 2}{3},$$

right on the blue-red boundary. It is therefore isotropic and, by virtue of its size, maximal isotropic.

So we may assume that $\ell_0 > \ell_2$ and $V \subsetneq W$. The space V shows up as the blue-zone support for the first vector problem

$$m_{11} = 2e + 1, \quad n_c = 2e - 4\ell_2 - 1.$$

Hence V is isotropic. Also, the first vector problem

$$m_{11} = 2e + 1, \quad n_c = 2\ell_2 + 1$$

lies in the red zone. The first term of its answer is a positive multiple of

$$(1 + \varepsilon_C)G^\times(W),$$

but since $\square_C = e$, the G can be replaced by F. Our strategy is as follows. Since $W^\times = T^\times(\ell_2, \ell_1, \ell_0)$ generates W as a group, it's enough to show that any $\alpha \in W^\times$ and $\beta \in V$ are orthogonal. We may write

$$\begin{aligned}\langle \alpha, \beta \rangle &= \varepsilon_C(1)\varepsilon_C(\beta)\varepsilon_C(\alpha)\varepsilon_C(\alpha\beta) \\ &= \varepsilon_C(\alpha)\varepsilon_C(\alpha\beta).\end{aligned}$$

So if α and β are *not* orthogonal, then, applying the transformation $\alpha \mapsto \alpha\beta$ if need be, we may assume

$$\varepsilon_C(\alpha) = 1 \quad \text{and} \quad \varepsilon_C(\alpha\beta) = -1.$$

Since $\varepsilon_C(\alpha) = 1$, α is in the support of the red-zone answer $W_{m_{11}=2e+1, n_c=2\ell_2+1}$. So there is a ψ in the box $1 + B_{\theta_1}(\infty, 2\ell_2 + 1)$ representing the class $[\alpha] \in H^1$. Recenter, using Lemma 21.2, and consider the $\mathfrak{P}'$ with $\theta_1' = \psi^{-1}\theta_1$, $m_{11}' = 2e + 1$, and

$$n_c' = 2e - 4\ell_2 - 1.$$

Since

$$\ell_{\mathfrak{P}'} = \ell(\alpha) = \ell_2,$$

this problem is still in the blue zone (right on the blue-green boundary), and we get that $\varepsilon_{C'} = 1$

on the boxgroup

$$1 + B_{\theta_1'}(\ell_0, \ell_1, \ell_2).$$

Since $\theta_1' \equiv \theta_1 \mod \pi^{2\ell_2+1}\mathcal{O}_K[\theta_1]$, the subscript can be changed from θ_1' to θ_1 without changing the boxgroup. So

$$1 = \varepsilon_{\mathfrak{P}'}(\beta) = \varepsilon_{\mathfrak{P}}(\alpha\beta),$$

a contradiction. This completes the proof in the unramified splitting types. ■

21.5.1 E-forms of the long answers

In the red, yellow, and beige zones when $h = 0$, the answer, as announced in 21.4, 21.9, and 21.10, is a sum of G and $\varepsilon_C G$ terms. It is capable of a simplification.

Definition 21.15. If $T(\ell_0, \ell_1, \ell_2)$ is defined, define

$$E(\ell_0, \ell_1, \ell_2) = \widehat{\varepsilon_C F}(\ell_0, \ell_1, \ell_2)$$

Note that if the ℓ_i are integers, we have

$$E(\ell_0, \ell_1, \ell_2) = \begin{cases} G(\ell_0, \ell_1, \ell_2), & \ell_0 \le \ell_2 \\ q^{\ell_2 - \ell_0}\varepsilon_C G(\ell_2, \ell_1, \ell_0), & \ell_2 \le \ell_0. \end{cases}$$

Lemma 21.16. (*a*) *A sum of the form*

$$\sum_{\ell=a}^{\lceil b/2\rceil - 1} q^\ell (1+\varepsilon_C) G^\times(\ell, e-b, b-\ell) + q^{-\lfloor b/2\rfloor} G^\times\left(\left\lceil \frac{b}{2}\right\rceil, e - 2\left\lceil \frac{b}{2}\right\rceil, \left\lceil \frac{b}{2}\right\rceil\right),$$

where $b \ge 2a$, can be rewritten as

$$\sum_{\ell=a}^{b-a} q^\ell E(\ell, e-b, b-\ell) - \sum_{\ell=a}^{b-a-1} q^\ell E(\ell+1, e-b-1, b-\ell).$$

(*b*) *In unramified splitting types, a sum of the form*

$$(1+\varepsilon_C)\sum_{a\le\ell\le\lfloor\frac{e}{2}\rfloor-1} q^\ell G^{\times\times}(\ell,0,e-\ell)+(core),$$

where (*core*) *denotes the beige-zone core (see Lemma 21.10) and* $a<\lfloor e/2\rfloor$*, can be rewritten as*

$$\sum_{\ell=a}^{e-a} q^\ell E(\ell,0,e-\ell)-\sum_{\ell=a+1}^{e-a-1} q^{\ell-1}E(\ell,0,e-\ell)$$

where the second sum may be empty or may have to be interpreted according to the natural convention

$$\sum_{\ell=1}^{-1} x_i=-x_0.$$

Proof. The proof is straightforward, converting each G and $\varepsilon_C G$ into an E and merging the ranges of summation. ■

Corollary 21.17. *For unramified splitting type, we get in the red zone:*

$$\begin{aligned}W_{m_{11},n_{11}}=&\sum_{\ell=\lfloor\frac{n_C}{2}\rfloor}^{e-n_{11}+\frac{s}{2}} q^{-m_{11}+\ell}E\left(\ell,\left\lceil\frac{n_{11}}{2}\right\rceil,e-\left\lceil\frac{n_{11}}{2}\right\rceil-\ell\right)\\&-\sum_{\ell=\lfloor\frac{n_C}{2}\rfloor}^{e-n_{11}+\frac{s}{2}-1} q^{-m_{11}+\ell}E\left(\ell+1,\left\lceil\frac{n_{11}}{2}\right\rceil-1,e-\left\lceil\frac{n_{11}}{2}\right\rceil-\ell\right),\end{aligned}$$

and in the yellow zone:

$$\begin{aligned}W_{m_{11},n_{11}}=&\sum_{\ell=0}^{e-\lceil n_{11}/2\rceil} q^{-m_{11}+\ell}E\left(\ell,\left\lceil\frac{n_{11}}{2}\right\rceil,e-\left\lceil\frac{n_{11}}{2}\right\rceil-\ell\right)\\&-\sum_{\ell=0}^{e-\lceil n_{11}/2\rceil-1} q^{-m_{11}+\ell}E\left(\ell+1,\left\lceil\frac{n_{11}}{2}\right\rceil-1,e-\left\lceil\frac{n_{11}}{2}\right\rceil-\ell\right),\end{aligned}$$

and in the beige zone:

$$W_{m_{11}}=\sum_{\ell=0}^{e} q^{-m_{11}+\ell}E(k,0,e-k)-\sum_{\ell=1}^{e-1} q^{-m_{11}+k-1}E(k,0,e-k).$$

For splitting type 1^3, we get in the red zone:

$$W_{m_{11},n_{11}} = \sum_{\ell=\left\lfloor \frac{n^\triangle}{2} \right\rfloor}^{e-n^\triangle+h} q^{-m^\triangle+1-h+\ell} E_h\left(\ell, \left\lceil \frac{n^\triangle}{2} \right\rceil - h, e - \left\lceil \frac{n^\triangle}{2} \right\rceil - \ell + h\right) - \sum_{\ell=\left\lfloor \frac{n^\triangle}{2} \right\rfloor}^{e-n^\triangle+h} q^{-m^\triangle+1-h+\ell} E_h\left(\ell+1, \left\lceil \frac{n^\triangle}{2} \right\rceil - h - 1, e - \left\lceil \frac{n^\triangle}{2} \right\rceil - \ell + h\right),$$

and in the beige zone ($h_1 = 1$):

$$W_{m_{11}} = \sum_{\ell=0}^{e} q^{-m^\triangle+\ell} E_1(k, 0, e-k) - \sum_{\ell=0}^{e-1} q^{-m^\triangle+\ell} E_1(k+1, -1, e-k)$$

and in the beige zone ($h_1 = -1$):

$$W_{m_{11}} = \sum_{\ell=0}^{e-1} q^{-m^\triangle+2+\ell} E_{-1}(k, 1, e-k-1) - \sum_{\ell=0}^{e-2} q^{-m^\triangle+2+\ell} E_{-1}(k+1, 0, e-k-1).$$

The following are to be kept in mind when manipulating terms $E(\ell_0, \ell_1, \ell_2)$:

- When $\ell_0 \leq \ell_C$ and $\ell_0 \leq \ell_2$, the E came from a $G(\ell_0, \ell_1, \ell_2)$ with $\ell_0 \leq \ell_C$. As we observed in the "Further remarks" sections following the red, yellow, and beige zones, such a G is interconvertible with an F. Hence such an E will be changed to F if it appears in the final answer (after smearing and applying the ξ_2 restrictions: see below).

- When $\ell_2 \leq \ell_C$ and $\ell_2 < \ell_0$, the E came from an $\varepsilon_C G(\ell_2, \ell_1, \ell_0)$ with $\ell_2 \leq \ell_C$. Such an $\varepsilon_C G$ is interconvertible with $\varepsilon_C F$ and hence is its own Fourier transform, up to the inevitable factor of q^e. We annotate it as E_{bal} ("bal" for "balanced"). The same can happen to $\varepsilon_C Fx$ and $\varepsilon_C Fxx$ terms, which we accordingly notate as $E_{bal}x$ and $E_{bal}xx$.

- When $\ell_C < \ell_0$ and $\ell_C < \ell_2$, the above transformations do not apply. We annotate the E as E_{side} and note that, for reflection to hold, either

  - The E_{side} pairs with its Fourier transform, an $\varepsilon_C F$ from the green zone, or

  - The E_{side} cancels with a like term for a different value of the discrete data. Indeed, we

notice that increasing n_{11} by 2 in the red or yellow zone causes most of the positive terms to reappear with a negative sign.

21.6 Smeared answers

It is now necessary to compute $\mathfrak{S}_r(W)$ to solve first vector problems with small m_{11}.

It is convenient to express as much as possible in terms of *sparks* that vanish suddenly as the smear index r, or equivalently m_{11}, is decreased.

Definition 21.18. A function $W : H^1 \to \mathbb{C}$ is a *spark of level* r_0 if for all r, $0 \leq r \leq e' + 1$,

$$\mathfrak{S}_r(W) = \begin{cases} W & r \geq r_0 \\ \\ 0 & r < r_0. \end{cases}$$

Lemma 21.19. *Let $0 \leq r_0 \leq e' + 1$. A function W is a spark of level r_0 if and only if its Fourier transform $\widehat{W}$ is supported on the set $\mathcal{L}_{e'-r_0} \backslash \mathcal{L}_{e'-r_0+1}$ of elements of exact level r_0 (or $-1/2$, in the case $r_0 = e' + 1$).*

Proof. Using the familiar Fourier duality between multiplication and convolution, we have the relation

$$\mathfrak{S}_r(W) = \left(\mathbf{1}_{\mathcal{L}_{e'-r}} \cdot \widehat{W} \right)\widehat{\ }. \tag{177}$$

So W is a spark of level r_0 if and only if

$$\mathbf{1}_{\mathcal{L}_\ell} \cdot \widehat{W} = \begin{cases} \widehat{W} & \ell \leq e' - r_0 \\ \\ 0 & \ell > e' - r_0. \end{cases}$$

This evidently happens exactly when $\widehat{W}$ is supported on $\mathcal{L}_{e'-r_0} \backslash \mathcal{L}_{e'-r_0+1}$, as desired. ∎

Drawing on the repertory of Fourier transforms we computed in Lemma 20.14, as well as the definition of E-functions, we get the following.

Lemma 21.20. *Let $\mathfrak{r}(\ell)$ be the minimal level of elements in a boxgroup denoted $T(\ell, \ell_1, \ell_2)$; to wit,*

- $\mathfrak{r}(\ell) = \ell$ *in unramified splitting type*
- $\mathfrak{r}(\ell) = 2\ell$ *in splitting type* 1^3 *if* $h = 1$
- $\mathfrak{r}(\ell) = 2\ell + 1$ *in splitting type* 1^3 *if* $h = -1$

The following functions are sparks of the indicated levels.

(*a*) *If* $T(\ell_0, \ell_1, \ell_2)$ *is defined and* $\ell_0, \ell_2 \geq \ell_C + 1$, *then*

$$W = \varepsilon_C F(\ell_0, \ell_1, \ell_2)$$

is a spark of level $e' - \mathfrak{r}(\ell_C)$. *This will be used in the green zone.*

(*b*) *If both terms are defined and* $\ell_1 \geq 1$, *then*

$$W = q \cdot E(\ell_0, \ell_1, \ell_2) - E(\ell_0, \ell_1 - 1, \ell_2 + 1)$$

is a spark of level $\mathfrak{r}(e - \ell_2)$. *This will be used in the red and yellow zones, as well as the beige zone in ramified splitting types.*

(*c*) *In unramified splitting type, if both terms are defined, then*

$$W = q^2 \cdot E(\ell_0, 0, \ell_2) - E(\ell_0 + 1, 0, \ell_2 - 1)$$

is a spark of level $\mathfrak{r}(\ell_0)$. *This will be used in the beige zone.*

(*d*) *Expressions of the form*

$$W = Gx(), \quad xGx(), \qquad \text{and} \quad Gxx()$$

are sparks of level $e' + 1$.

Although a single F is not generally a spark, we do have the relation $\mathcal{L}_{e'-\mathfrak{r}(\ell_2)} \subseteq T(\ell_0, \ell_1, \ell_2)$, from which $F(\ell_0, \ell_1, \ell_2)$ and $G(\ell_0, \ell_1, \ell_2)$ are stable under smears of levels $r \geq e' - \mathfrak{r}(\ell_2)$.

We are now ready to compute explicit answers for the smear. Note that we do *not* try to write $W_{m_{11},n_{11}}$ for each value of m_{11} and n_{11}. Instead, we express $W_{m_{11},n_{11}}$ for m_{11} large as a sum of sparks and stable terms whose appearance and disappearance can be coded simply.

One region that we do *not* have to work out is the *gray zone* where m_{11} is so low as to satisfy all the conditions of Lemma 20.4, resp. 20.9, for the defining of boxgroups. There the zone total is simply

$$W_{m_{11},n_{11}} = \frac{|H^0|q^{2e-m_{11}-n_c+\frac{d_0}{2}-(s/2-v(N(\gamma)))}}{|T(\ell_0,\ell_1,\ell_2)|} \cdot F(\ell_0,\ell_1,\ell_2)), \tag{178}$$

where $T(\ell_0,\ell_1,\ell_2)$ is the corresponding boxgroup.

We now consider each zone in turn:

- The black and brown zones need no smear, as $m_{11} \geq n_{11} > 2e$ automatically in them.
- The purple and blue zones have as answer a single F. It is stable as long as m_{11} is above the gray zone, since we computed the support by relaxing $\mathcal{M}_{11}$ until we hit the gray zone.
- The green-zone answer is a sum of type $F + \varepsilon_C F$. The F is stable, as we got it by relaxing $\mathcal{M}_{11}$ until we hit the gray zone. The $\varepsilon_C F$ is a spark by Lemma 21.20(a).
- In the red, yellow, and beige zones in the charmed coarse coset, the answer is a difference of two series of E's. The E's pair up to form sparks of the types in 21.20, leaving one singleton (two in the beige zone), a mostly stable F. In the yellow and beige zones, if the positive sum gets cut down to 1 or 0 terms respectively, the negative sum has -1 term and must be coded up in a *special zone*. This happens in a few cases, as shown in the code.

21.7 The average value of a quadratic character on a box

The results in this subsection, coupled with the strong-zone answers in Section 21.2, yield a quick solution to a problem that, at first glance, is unrelated to the topic of this paper.

Theorem 21.21. *Let $K \supseteq \mathbb{Q}_2$ be a finite extension, and let $R \supset K$ be a tamely ramified étale extension of degree 3. In other words, R is one of the following:*

- $K \times K \times K$
- $K \times Q$, *where* Q *is the unramified quadratic extension field*
- *the unramified cubic extension field*
- *a totally ramified cubic extension field.*

Let

$$\chi : R^\times \to \{\pm 1\}$$

be a character, that is, a group homomorphism, such that $\chi(a) = 1$ *for all* $a \in K^\times$. *(All such characters can be put in the form*

$$\chi_\alpha(\xi) = \left\langle \alpha \cdot N_{R/K}(\alpha), \xi \right\rangle,$$

where $\alpha \in R^\times$ *and* $\langle \bullet, \bullet \rangle$ *is the Hilbert symbol.) Let* B *be an* $\mathcal{O}_K$*-sublattice contained in the Jacobson radical of* $\mathcal{O}_R$. *(That is,* B *is a subgroup of* $\mathcal{O}_R$ *of finite index closed under multiplication by* $\mathcal{O}_K$*, and all elements of* B *have positive valuation at every field factor of* R.*) Then the average value*

$$\frac{1}{\int_B 1} \int_B \chi(1+\xi)\, \mathrm{d}\xi$$

takes on one of the following values:

- 0
- 1
- q^{-i} *for some* i, $1 \le i \le e$. *(Here* $q = |k_K|$, *and* $e = v_K(2)$ *is the absolute ramification index.)*

Proof. We may assume that B contains $\pi\mathcal{O}_K$, as enlarging $1 + B$ to $(1 + \pi\mathcal{O}_K)(1 + B)$ does not change the average of a character that vanishes on $K^\times$. Now we can take a reduced basis

$$B = \pi\mathcal{O}_K + \pi^n\theta_1 + \pi^m\theta_2,$$

and observe that B is one of the boxes that came up in Lemma 18.4. The strong-zone total $W_{m,n}(\delta)$ that we have computed in Section 21.2 can also be interpreted (up to scaling) as the volume of $\beta \in B$ of class δ. Hence the average in question is

$$I(\chi) = \frac{\sum_\delta \chi(\delta) W_{m,n}(\delta)}{\sum_\delta W_{m,n}(\delta)} = \frac{\widehat{W}_{m,n}(\chi)}{\widehat{W}_{m,n}(1)}.$$

We wish to understand the possible values of this as χ ranges over H^1. In view of the smearing lemma (Lemma 21.1), increasing m only makes the theorem stronger, so we can assume that we are in the case of Lemma 21.4 or 21.5.

In the black, purple, and blue zones, $W_{m,n}(\delta) = c \cdot F(T)$ for some subgroup $T \subseteq H_1$, so I takes the value 1 or 0 according as $\chi(T) = 1$ or not.

In the green zone,

$$W_{m,n}(\delta) = c(F(T) + \varepsilon_C F(T))$$

for some boxgroup $T = T(\ell_0, \ell_1, \ell_2)$ on which ε_C is equidistributed, so

$$I = \begin{cases} F(T^\perp) + G(T^\perp), & T^\perp \supseteq T \\ F(T^\perp) + \varepsilon_C \dfrac{\sqrt{|V|}}{|T|} G(T), & T^\perp \subsetneq T. \end{cases}$$

In either case, the identity coset T is uncharmed, so the two terms have disjoint supports. In the first case, I is either 1 or 0. In the second case, we can additionally get a value of

$$\varepsilon_C \frac{\sqrt{|V|}}{|T|} = \pm q^{\ell_0 - \ell_2}.$$

The value of $i = \ell_2 - \ell_0$ evidently satisfies $1 \le i \le e$ by our setup of boxgroups.

Finally, in the red zone, the Fourier transform is easier to compute using the E-form (Corollary 21.17), which is of the form

$$W_{m,n} = \sum_{\ell=a}^{b-a} q^{c+\ell} E(\ell, e-b, b-\ell) - \sum_{\ell=a}^{b-a-1} q^{c-\ell} E(\ell+1, e-b-1, b-\ell).$$

The Fourier transform, by definition of E, is

$$\widehat{W}_{m,n} = c\varepsilon_C \cdot \left(\sum_{\ell=a}^{b-a} q^{b-\ell} F(b-\ell, e-b, \ell) - \sum_{\ell=a}^{b-a-1} q^{b-\ell-1} F(b-\ell, e-b-1, \ell+1) \right).$$

Scaling by $\widehat{W}_{m,n}(1) = cq^{b-a}$, we get

$$I = \varepsilon_C \left(\sum_{\ell=a}^{b-a} q^{a-\ell} F(b-\ell, e-b, \ell) - \sum_{\ell=a}^{b-a-1} q^{a-\ell-1} F(b-\ell, e-b-1, \ell+1) \right).$$

The boxgroups on which the terms are supported form a nested chain

$$T(b-a, e-b, a) \subset T(b-a, e-b-1, a+1) \subset T(b-a-1, e-b, a+1) \subset \cdots \subset T(a, e-b, a)$$

that appear alternately with positive and negative coefficients. So there are two types of behavior upon plugging in any individual χ:

- χ lies in an even number of boxgroups in the chain, and they cancel in pairs to yield $I = 0$.
- χ lies in an odd number of boxgroups in the chain, and only the smallest one yields a contribution $I = \pm q^{a-\ell}$. The negative of the exponent satisfies

$$0 \leq \ell - a \leq b - a \leq e.$$

We must exclude the possibility that $I = -1$. This can be done by noting that I is the average value of a character that takes only the values 1 and -1, and that in a small neighborhood of $1 \in 1 + B$, χ is identically 1 (continuity of χ is automatic, because all values near 1 are squares). ■

22 Ring volumes for ξ_2'

Fix ξ_1 and all the data leading up to it. By Lemma 18.2, there are only three possibilities for $\bar{\xi}_2$: either it is unrestricted, in which case the volume is given by the white-zone answer in Lemma 18.6,

or it is restricted by $\mathcal{M}_{12}$ or $\mathcal{M}_{22}$.

22.1 $\mathcal{M}_{12}$

Lemma 22.1. *Assume that R is tamely ramified and $\mathcal{M}_{12}$ is active. Fix ξ_1 satisfying the $\mathcal{M}_{11}$, $\mathcal{N}_{11}$ conditions, and normalize γ_2 as in Lemma 18.5. Then $\mathcal{M}_{12}$ is equivalent to a relation of the form*

$$\lambda^{\diamondsuit}(\alpha_1 \xi_2') \equiv 0 \mod \pi^{\lfloor m_{12} \rfloor}$$

where $\alpha_1 \in \mathcal{O}_R$ is primitive.

Proof. The $\mathcal{M}_{12}$ condition says that

$$\operatorname{tr}(\xi_1 \xi_2) \equiv 0 \mod \pi^{m_{12}}.$$

We have

$$\operatorname{tr}(\xi_1 \xi_2) = \operatorname{tr}(\xi_1 \gamma_2 \xi_2') = \lambda^{\diamondsuit}(\diamondsuit \xi_1 \gamma_2 \xi_2').$$

Observe that

$$\diamondsuit \xi_1 \gamma_2 \in \pi^{-a_1' - a_2'} R.$$

Let $r_{12} \in a_1' + a_2' + \mathbb{Z}$ be the unique value such that

$$\alpha_0 = \pi^{r_{12}} \diamondsuit \xi_1 \gamma_2$$

is a primitive vector in $\mathcal{O}_R$. Then

$$\mathcal{M}_{12} : \lambda^{\diamondsuit}(\alpha_1 \xi_2') \equiv 0 \mod \pi^{m_{12} + r_{12}},$$

and the exponent is seen to be an integer. To show that it is $\lfloor m_{12} \rfloor$, it's enough to prove that

$$-1 < r_{12} \leq 0.$$

We examine the cases.

- If R is unramified and $[\delta\hat{\omega}_C] \in \mathcal{L}_0$, then $\diamondsuit$, γ_2 are units and ξ_1 is primitive, so $r_{12} = 0$.
- If R is unramified and $[\delta\hat{\omega}_C] \in (1;\pi;\pi)\mathcal{L}_0$, then $\diamondsuit$ is a unit. Since $\mathcal{M}_{11}$ is satisfied, we have $j_0 \neq 1$ and (with respect to the naïve choice of γ_1 from Lemma 18.5, which differs from how we actually found the ring volume for ξ_1), $\gamma_1 \sim (\sqrt{\pi};1;1)$, $(\xi_1')^Q$ is primitive. There are then two subcases, $j_0 = 2$ and $j_0 = 3$. In both cases we find that the scaling of α_0 is controlled by the Q-components and $r_{12} = -1/2$ or 0 respectively.
- If R is totally ramified, then $\diamondsuit \sim \pi_R^2$, $\xi_1 \sim 1$, $\gamma_2 \sim 1$. According as the product $\diamondsuit\xi_1\gamma_2$ lies in R, $\bar{\zeta}_3 R$, or $\bar{\zeta}_3^2 R$, we must take $r_{12} = 0$, $-2/3$, or $-1/3$ respectively.

Thus in all cases $-1 < r_{12} \leq 0$, as desired. ■

This allows us to compute the ring volume for ξ_2:

Lemma 22.2. *If $\mathcal{M}_{12}$ is active, the solution volume for ξ_2' is*

$$q^{-\lfloor m_{12} \rfloor},$$

except when $m_{12} \in \mathbb{Z}$ in splitting type 1^3, in which case $\mathcal{M}_{12}$ has no solutions.

Proof. By Lemma 22.1, the $\mathcal{M}_{12}$-condition is given by one of the form

$$\lambda^{\diamondsuit}(\alpha_1\xi_2') \equiv 0 \mod \pi^{\lfloor m_{12} \rfloor}.$$

Here α_1 is primitive, so we have a linear relation modulo $\pi^{\lfloor m_{12} \rfloor}$ which yields a solution volume of $(1+1/q)q^{-\lfloor m_{12} \rfloor}$. The solutions must be further whittled down using the restrictions on ξ_2' in Lemma 18.5 as well as the condition that ξ_1 and ξ_2 be linearly independent mod $\mathfrak{m}_{\bar{K}}$. Here it's important to note that the solutions to $\mathcal{M}_{12}$ are distributed equally among $(q+1)$-many 1-pixels.

- If R is unramified and $[\delta\hat{\omega}_C] \in \mathcal{L}_0$, then $a_1' \in \mathbb{Z}$. One of the 1-pixels is that of ξ_1, which violates the linear independence, so we eliminate it.

- If R is unramified, $[\delta\hat{\omega}_C] \in (1;\pi;\pi)\mathcal{L}_0$, and

$$(a_1, a_2, a_3) \equiv \left(\frac{1}{2}, 0, \frac{1}{2}\right) \mod 1,$$

then $m_{12} \in \mathbb{Z}+1/2$, and the condition that $\pi \nmid (\xi_2')^{(K)}$ eliminates one 1-pixel (no more, because $(\xi_1')^Q$ is primitive).

- If R is unramified, $[\delta\hat{\omega}_C] \in (1;\pi;\pi)\mathcal{L}_0$, and

$$(a_1, a_2, a_3) \equiv \left(\frac{1}{2}, \frac{1}{2}, 0\right) \mod 1,$$

then $m_{12} \in \mathbb{Z}$ and $\gamma_1 = \gamma_2 \sim (\sqrt{\pi}; 1; 1)$. When the $\mathcal{M}_{12}$-condition

$$\mathrm{tr}(\gamma_1^2 \xi_1' \xi_2') \equiv 0 \mod \pi^{m_{12}}$$

is looked at mod π, it uniquely determines $\xi_2'^Q \equiv \xi_1'^Q \mod \pi$ (by $\mathcal{M}_{11}$, the value $\xi_2' = \xi_1'$ is a solution). But then $\xi_2 \equiv \xi_1 \mod \sqrt{\pi}$, violating linear independence. So $\mathcal{M}_{12}$ is unsatisfiable in this case.

- If R is totally ramified, then the condition that ξ_2' be a unit eliminates one 1-pixel, unless all its solutions are non-units. This happens exactly when $\alpha_1 \sim \pi_R^2$, which is seen to be equivalent to $m_{12} \in \mathbb{Z}$.

Thus, in all but the stated exceptional case, we eliminate one 1-pixel, leaving a ring volume of $q^{-\lfloor m_{12} \rfloor}$. ■

22.2 $\mathcal{M}_{22}$

When $\mathcal{M}_{22}$ is active, of course $\mathcal{M}_{11}$ is also, and we normalize both γ_1 and γ_2 (that is, ξ_1' and ξ_2') according to Lemma 19.3. In tame splitting types, we find that the conic

$$\mathcal{M} : \lambda^{\diamondsuit}(\delta^{\odot}\xi_i'^2) \equiv 0 \mod m_{ii}'$$

is actually the same conic, but that the ξ_i' cannot even lie in the same 1-pixel. The following two lemmas detail when this can happen.

Lemma 22.3. *Let $\mathcal{A}$ be a conic of determinant 1 on a lattice Λ over $\mathcal{O}_K$, and let m be an integer, $1 \leq m \leq e$. Then there are coprimitive $\vec{x}_1, \vec{x}_2 \in \mathbb{P}(\Lambda)$ satisfying*

$$\mathcal{A}(\vec{x}_1) \equiv \mathcal{A}(\vec{x}_2) \equiv 0 \mod \pi^m \tag{179}$$

if and only if the squareness $\square(\mathcal{A})$ satisfies

$$\square(\mathcal{A}) \geq m.$$

Moreover, if $\square(\mathcal{A}) + 1 \geq m$, then for fixed $\vec{x}_1$, the volume of $\vec{x}_2$ satisfying (179) *and coprimitive to $\vec{x}_1$ is $q^{-\lceil m/2 \rceil}$, split evenly among q-many 1-pixels.*

Proof. If coprimitive $\vec{x}_1, \vec{x}_2$ satisfy (179), we can complete them to a basis $(\vec{x}_1, \vec{x}_2, \vec{x}_3)$ of Λ. Note that $\pi \nmid \mathcal{A}(\vec{x}_3)$, or else the determinant could not be 1. So we may scale so that $\mathcal{A}(\vec{x}_3) = 1$, and now we see that $\mathcal{A}$ is a square modulo π^m.

Conversely, suppose that $\mathcal{A}$ is a square λ^2 of a linear form modulo π^m. Then for $\vec{x} \in \mathbb{P}(\Lambda)$,

$$\begin{aligned} & \mathcal{A}(\vec{x}) \equiv 0 \mod \pi^m \\ \iff & \lambda(\vec{x})^2 \equiv 0 \mod \pi^m \\ \iff & \lambda(\vec{x}) \equiv 0 \mod \pi^{\lceil m/2 \rceil}. \end{aligned}$$

Since $\lambda \not\equiv 0 \mod \pi$, this has solution volume $(1 + 1/q)q^{-\lceil m/2 \rceil}$, split evenly among $(q+1)$-many 1-pixels. If $\vec{x}_1$ is given, then $\vec{x}_2$ can occupy any 1-pixel except the one containing $\vec{x}_1$. ∎

The following lemma limits m_{22}:

Lemma 22.4. *The conditions on ξ_2' can be satisfied only if $m_{22} \leq e$ and $m_{22}^{\odot} \leq e$.*

Proof. For the first part, note that if $m_{22} > e$, then

$$m_{12} = \frac{m_{11} + m_{22}}{2} - e + t > \frac{e+e}{2} - e = 0,$$

so $\mathcal{M}_{12}$ is active, contradicting Lemma 18.2. In unramified splitting type, this is the entire content of the lemma, since $m_{22}^{\odot} = m_{22}$. In splitting type 1^3, note that

$$m_{11}^{\odot} = m_{11} - \frac{2h_1}{3} \quad \text{and} \quad m_{22}^{\odot} = m_{22} - \frac{2h_2}{3}$$

satisfy $m_{11}^{\odot} + m_{22}^{\odot} = m_{11} + m_{22}$, since $\{h_1, h_2\} = \{1, -1\}$. Also, $m_{11}^{\odot} > m_{22}^{\odot}$ since $m_{11} - m_{22} = 2(a_2 - a_1) \geq 2/3$. So if $m_{22}^{\odot} > e$, then $m_{11}^{\odot} > e$ and $\mathcal{M}_{12}$ is active as above. ■

This enables us to compute the ring volume for ξ_2'.

Lemma 22.5. *Let R be tamely ramified. Fix the discrete data of a quartic ring and a ξ_1' satisfying its conditions. The $\mathcal{M}_{22}$-condition is solvable for ξ_2' if and only if the following conditions are satisfied:*

- $[\delta\hat{\omega}_C] \in \mathcal{L}_0$*;*
- *the value of a_2 mod $\mathbb{Z}$ allows for a γ_2 and $m_{22}^{\odot}$ according to Lemma 19.3, and*
- $m_{22}^{\odot} \leq \min\{2\ell(\mathcal{M}) + 1, e\}$.

In such cases, the volume of ξ_2' is

- $q^{1-\lceil m_{22}^{\odot}/2 \rceil}$ *if R is totally ramified, $h_1 = 1$ and $h_2 = -1$,*
- $q^{-\lceil m_{22}^{\odot}/2 \rceil}$ *otherwise.*

Proof. The necessity of the restrictions on $m_{22}^{\odot}$ is shown by the foregoing lemmas. If they are satisfied, then $\mathcal{M}_{22}$ transforms to a linear condition with solution volume $(1 + 1/q)q^{-\lceil m_{22}^{\odot}/2 \rceil}$, distributed equally among $(q+1)$-many 1-pixels. We must check its solutions against the other restrictions on ξ_2':

- If R is unramified and $[\delta\hat{\omega}_C] \in \mathcal{L}_0$, then ξ_1', ξ_2' are required to be coprimitive, eliminating one of the 1-pixels.

- If R is unramified and $[\delta\hat{\omega}_C] \in (1;\pi;\pi)\mathcal{L}_0$ then j_0 must be 3 in order for both γ_1 and γ_2 to exist. Then since $m_{22}^{\odot} = m_{22} \geq 1$, we must have two solutions ξ_1', ξ_2' to the transformed conic $\mathcal{M}$ modulo π whose Q-components are coprimitive. But $\mathcal{M}(\xi')\mod \pi$ only depends on the Q-component and has only a unique solution in $\mathbb{P}(\mathcal{O}_Q/\pi\mathcal{O}_Q)$, so $\mathcal{M}_{22}$ is unsatisfiable if active.

- If R has splitting type 1^3, then for γ_1, γ_2 to exist, we must have $\{h_1, h_2\} = \{1, -1\}$. Here, coprimitivity between the ξ_i is subsumed by the condition that each $\xi_i^{\odot}$ lie in its correct domain

$$\xi_i^{\odot} \sim \pi_R^{1-h_i}.$$

  As we noted in the proof of Lemma 20.7, the solutions to $\mathcal{M}$ mod π comprise q-many 1-pixels of $\xi^{\odot} \sim 1$ and one 1-pixel of $\xi^{\odot} \sim \pi_R^2$. Hence if $h_1 = -1$ and $h_2 = 1$, we retain q of the $(q+1)$-many 1-pixels, getting a volume $q^{-\lceil m_{22}^{\odot}/2 \rceil}$. But if $h_1 = 1$ and $h_2 = -1$, then $\xi_2^{\odot}$ is restricted to one 1-pixel. This gives a volume of $q^{-1-\lceil m_{22}^{\odot}/2 \rceil}$, but we multiply back by q^2 since $\xi_2' = \pi_R^{-2}\xi_2^{\odot}$. ■

Of the conditions, only

$$m_{22}^{\odot} \leq \min\{2\ell(\mathcal{M}) + 1, e\} \tag{180}$$

is not trivial to verify. The following solves it:

Lemma 22.6. *Suppose that the discrete data is fixed in such a way that*

- $\mathcal{M}_{22}$ *is active,*
- $[\delta\hat{\omega}_C] \in \mathcal{L}_0$ *(so the conic has determinant* 1*),*
- *the value of* $a_2 \mod \mathbb{Z}$ *allows for a* γ_2 *and* $m_{22}^{\odot}$ *according to Lemma 19.3.*

Also suppose that ξ_1 *is fixed, satisfying the conditions* $\mathcal{M}_{11}$, $\mathcal{N}_{11}$ *governing it. Then the remaining condition* (180) *can be checked as follows:*

- *In the black, purple, and blue zones, it is automatic.*

- *In the green zone, it is equivalent to*

$$m_{22}^{\odot} \leq \square_C$$

- *In the red, yellow, and beige zones, it restricts the sum to only use terms* $G^{\times}(\ell_0, \ell_1, \ell_2)$ *with*

$$m_{22}^{\odot} \leq 2\ell_0 + 1.$$

Proof. When the conic $\mathcal{M}$ is green, its level was computed as part of the finding of the zone total for ξ_1'. So it remains to prove that if the conic is black or blue, (180) is satisfied. That the conic is black or blue implies that

$$n_{11} \geq 2e - 4\ell(\mathcal{M}) - 1.$$

We already know $m_{22} \leq e$. Suppose that

$$m_{22} \geq 2\ell(\mathcal{M}) + 2.$$

Since m_{12} is inactive,

$$m_{11} = 2m_{12} - m_{22} + 2e - 2t \leq 2e - 2\ell(\mathcal{M}) - 2.$$

But then

$$n_{22} = m_{22} - m_{11} + n_{11} \geq 3,$$

so $\mathcal{N}_{22}$ is active and we have a contradiction. ■

Remark 22.7. In the code, o_2 and h_2 are defined by

$$o_2 = 3(b_2 \bmod 1) \in \{0, 1, 2\}, \quad h_2 = 2o_2 - 3 \in \{-3, -1, 1\}.$$

The condition

$$m_{22}^{\triangle} \leq 2k+1$$

(where $k = \ell_C$ in the green zone, or k is the index of summation in the red zone) is coded as

$$2k + \frac{1}{3} - m_{22} + \frac{2o_2}{3} \geq 0.$$

One verifies that this is the same thing when $o_1 \in \{1,2\}$, while when $o_1 = 0$, it reduces to $m_{22} \leq 0$, as desired, since $\mathcal{M}_{22}$ is unsatisfiable if active.

23 Further remarks on the code

In the attached code, we use the computer programs SAGE and LattE to compute the generating function of rings. First we count "zone tuples" consisting of integer values of the following variables:

- e, t, b_1, b_2, s.
- $\texttt{a1f} = \lfloor a_1 \rfloor, \texttt{a2f} = \lfloor a_2 \rfloor, o_1, o_2, o_3$. Here we've decomposed

$$a_i = \lfloor a_i \rfloor + \frac{o_i}{o},$$

where

$$o = \begin{cases} 1 & \text{in splitting types (111), (12), and (3)} \\ 3 & \text{in splitting type } (1^3) \end{cases}.$$

The o_i belong to one of a finite number of "flavors" coding the classes of the a_i and b_i mod $\mathbb{Z}$. Note that $\lfloor a_3 \rfloor$ is missing from the variable list, as its value is uniquely determined by the discriminant identity (Lemma 18.1)

- $$\texttt{lCf} = \begin{cases} -1, & \square_C = 0 \\ \ell_C, & 0 < \square_C < e \\ \left\lfloor \frac{e}{2} \right\rfloor, & \square_C = e. \end{cases}$$

  This unambiguously determines $\square_C$. We note that in our answers, $\square_C$ only appears in the answer and bounds of the green zone. When $\square_C = e$, there is no green zone and its bounds are far from being achieved, so we can equate $\lfloor \ell_C \rfloor$ with `lCf` without changing anything.

- k, an index of summation needed to input the answers in the red, yellow, and beige zones.

- If $\lfloor m_{11}/2 \rfloor$ appears in a zone answer, we add a variable `m11fl` and impose one of the equations

$$m_{11} = 2 \cdot \texttt{m11fl} \quad \text{or} \quad m_{11} = 2 \cdot \texttt{m11fl} + 1.$$

  Similarly we treat $\lfloor n_{11}/2 \rfloor$, $\lfloor n_c/2 \rfloor$, $\tilde{n}$, $\lfloor m_{22}/2 \rfloor$, $\lfloor e/2 \rfloor$, $\lfloor s/2 \rfloor$.

The result comes out as a rational function in $\texttt{RRR} = \mathbb{Z}((E, T, B_1, B_2, S, \texttt{A1F}, \ldots))$, Here we use the convention that the value of a lowercase variable appears as an exponent of the corresponding uppercase variable. For instance, the generating function of the three lattice points on the line segment $y = 2x$, $0 \leq x \leq 2$ is

$$1 + XY^2 + X^2Y^4.$$

Because each variable is bounded below in terms of the preceding variables, the power series is formally convergent. Because each zone is delimited by finitely many linear inequalities with $\mathbb{Z}$-coefficients, the generating function is a rational function, computed by Barvinok's algorithm as implemented in LattE. We then encode ring totals as substitutions that land us in a common ring

$$\texttt{RINGS_RING} = \mathbb{Z}[[\texttt{E_}, \texttt{T_}, \texttt{LCF_}, \texttt{SFL_}, \texttt{B1_}, \texttt{B2_}, q, \texttt{L0}, \texttt{L2}]].$$

The trailing underscores are to prevent the computer from confounding certain elements of `RRR` and

RINGS_RING, although the reader can think of them as identified. Two new variables L0, L2, whose exponents are the ℓ_0 and ℓ_2 of a boxgroup, complete the description of a ring total, along with a string Ftype that tells the kind of weighting (F, Fxx, E_{bal}, etc.).

Part VIII

Unanswered questions

24 Doubly traced quartic rings

It is an open question to classify, analogously to Theorem 11.1, the lattices in the space V_K of pairs of ternary quadratic forms over K invariant under $\mathrm{GL}_2(\mathcal{O}_K) \times \mathrm{GL}_3(\mathcal{O}_K)$. This problem is not quite the most relevant to us because the factor $\mathrm{GL}_2(\mathcal{O}_K)$, which changes the coordinates of the resolvent, is not relevant when we count rings with a *fixed* resolvent, as we have done in this paper. We therefore look at lattices invariant under $\mathrm{GL}_3(\mathcal{O}_K)$ alone. By inspection we find the following examples, which we conjecture exhaust all of them:

Conjecture 24.1. *Let K be a number field, and let $\mathcal{V}(\mathcal{O}_K)$ be the lattice of pairs of ternary quadratic forms over $\mathcal{O}_K$. A primitive, $\mathrm{GL}_3(\mathcal{O}_K)$-invariant lattice L in $\mathcal{V}(\mathcal{O}_K)$ is $\mathrm{GL}_2(\mathcal{O}_K)$-equivalent to one whose completions $L_\mathfrak{p}$ are as follows:*

(a) For $\mathfrak{p}|2$, the lattices $L_{\mathfrak{p},t,s}$ of $(\mathfrak{p}^t, \mathfrak{p}^s)$-traced pairs of ternary quadratics

$$L_{t,s} = L_{\mathfrak{p},t,s} = \left\{ \left(\sum_{1 \le i \le j \le 3} a_{ij} x_i x_j, \sum_{1 \le i \le j \le 3} b_{ij} x_i x_j \right) : a_{ij} \equiv 0 \bmod \mathfrak{p}^t, b_{ij} \equiv 0 \bmod \mathfrak{p}^s \ (i < j) \right\}$$

for $0 \le t \le s \le e = v_p(2)$;

(b) For all other $\mathfrak{p}$, the maximal lattice $V_{\mathcal{O}_{K,\mathfrak{p}}}$ only.

In other words, they are of the form

$$L_{\mathfrak{t},\mathfrak{s}} = \bigcap_{\mathfrak{p}|2} L_{\mathfrak{p},\mathfrak{t}_\mathfrak{p},\mathfrak{s}_\mathfrak{p}} = \left\{ \left(\sum_{1\le i\le j\le 3} a_{ij}x_ix_j, \sum_{1\le i\le j\le 3} b_{ij}x_ix_j \right) : a_{ij} \equiv 0 \bmod \mathfrak{t}, b_{ij} \equiv 0 \bmod \mathfrak{s}\,(i<j) \right\}$$

for ideals $(1) \supseteq \mathfrak{t} \supseteq \mathfrak{s} \supseteq (2)$.

As in the cubic case, the same lattices $L_{\mathfrak{t},\mathfrak{s}}$ necessarily appear in the analogues of $\mathcal{V}(\mathcal{O}_K)$ with any Steinitz class $\mathfrak{a}$, appropriately adjusting the ideals that the a_{ij}, b_{ij} must lie in.

For now, we look at the (2-adic) local case $K/\mathbb{Q}_2$. An element of $L_{t,s}$ can be visualized as a pair of symmetric matrices

$$(\mathcal{A},\mathcal{B}) = \left(\begin{bmatrix} a_{11} & \frac{1}{2}a_{12} & \frac{1}{2}a_{13} \\ \frac{1}{2}a_{12} & a_{22} & \frac{1}{2}a_{23} \\ \frac{1}{2}a_{13} & \frac{1}{2}a_{23} & a_{33} \end{bmatrix}, \begin{bmatrix} b_{11} & \frac{1}{2}b_{12} & \frac{1}{2}b_{13} \\ \frac{1}{2}b_{12} & b_{22} & \frac{1}{2}b_{23} \\ \frac{1}{2}b_{13} & \frac{1}{2}b_{23} & b_{33} \end{bmatrix} \right)$$

with diagonal entries $a_{ii}, b_{ii} \in \mathcal{O}_K$ and off-diagonal entries $a_{ij} \in 2^{-1}\pi_K^t\mathcal{O}_K$, $b_{ij} \in 2^{-1}\pi_K^s\mathcal{O}_K$. It is easy to check that the cubic resolvent $f(x,y) = 4\det(\mathcal{A}x - \mathcal{B}y)$ has the form

$$f(x,y) = \pi^{2s}ax^3 + \pi^{2s}bx^2y + \pi^{2t}cxy^2 + \pi^{2t}dy^3$$

with discriminant $D \in \pi^{4t+4s}$. Now (A,B) parametrizes a quartic ring with a resolvent $\Phi : \mathcal{O} \to C$, and $f(x,y)$ is the index form of C. The divisibility conditions on $f(x,y)$ can be interpreted as a non-maximality condition on C: since $t \le s$,

$$\frac{f(\pi^{-t}x, \pi^{-t}y)}{\pi^{-2t}} = \pi^{2s-2t}ax^3 + \pi^{2s-2t}bx^2y + cxy^2 + dy^3$$

and

$$\frac{f(\pi^{-t}x, \pi^{-s}y)}{\pi^{-t-s}} = ax^3 + \pi^{s-t}bx^2y + cxy^2 + \pi^{s-t}dy^3$$

are integral and thus are the index forms of certain overrings C_1, C_2 which we call the *reduced*

resolvent and the *reduced coresolvent*. Appropriately lifting the basis $\langle \bar{\xi}, \bar{\eta} \rangle$ of $C/\mathcal{O}_K$ in which (A, B) and hence f are written, we have $C = \langle 1, \xi, \eta \rangle$, $C_1 = \langle 1, \pi^{-t}\xi, \pi^{-t}\eta \rangle$, and $C_2 = \langle 1, \pi^{-t}\xi, \pi^{-s}\eta \rangle$. Note that C_1 is a subring of C_2 of index π^{s-t} and moreover is a *unidirectional* subring in the sense that $C_1/C_2 \cong \mathcal{O}_K/\pi^{s-t}$ is generated by one element. The integrality properties of A and B translate readily into relations between the resolvent and the rings C_1 and C_2.

Definition 24.2. Let $\mathcal{O}_K$ be a Dedekind domain, and let L/K be a quartic algebra over its field of fractions with resolvent $\Phi : L \to R$. Let $C_1 \subseteq C_2 \subseteq R$ be a pair of subrings with $C_2/C_1 \cong \mathcal{O}_K/\mathfrak{d}$ for some divisor $\mathfrak{d}$ of 2 in $\mathcal{O}_K$. Let $\mathfrak{t}$ be a divisor of $2\mathfrak{d}^{-1}$ and let $\mathfrak{s} = \mathfrak{t}\mathfrak{d}$.

An order $\mathcal{O} \subseteq L$ is $(\mathfrak{t}, \mathfrak{s})$-*traced with reduced resolvent* C_1 *and reduced coresolvent* C_2 if

(a) $C = \mathcal{O}_K + \mathfrak{t}^2 C_1$ is a resolvent for $\mathcal{O}$, that is, $\operatorname{disc} \mathcal{O} = \operatorname{disc} C$ and $\Phi(\mathcal{O}) \subseteq C$;

(b) The associated bilinear form

$$\tilde{\Phi}(x, y) = \Phi(x + y) - \Phi(x) - \Phi(y) = xy' + x'y + x''y''' + x'''y''$$

maps $\mathcal{O} \times \mathcal{O}$ into $\mathcal{O}_K + \mathfrak{t}^3\mathfrak{s}C_2$.

If C has a basis $\langle 1, \xi, \eta \rangle$ for which $C_1 = \langle 1, \mathfrak{t}^{-1}\xi, \mathfrak{t}^{-1}\eta \rangle$ and $C_2 = \langle 1, \mathfrak{t}^{-1}\xi, \mathfrak{s}^{-1}\eta \rangle$, as always happens when $\mathcal{O}_K$ is a PID, then this is easily seen to be equivalent to the condition that $\Phi : \mathcal{O} \to C$ is a resolvent whose matrix under this basis is in $L_{\mathfrak{t},\mathfrak{s}}$.

The functional equation for the Shintani zeta functions on $V_{\mathbb{Z}}$ was stated and proved by Sato and Shintani ([48]). It relates pairs of integer-coefficient ternary quadratic forms (over $\mathbb{Z}$) with pairs of integer-matrix forms, that is, $L_{(1),(1)}$ to $L_{(2),(2)}$ in our notation. In contrast to the lattice of cubic forms, there is no $\mathrm{SL}_3(K)$-invariant inner product in V_K: as a representation of $\mathrm{SL}_3(K)$, V_K is not isomorphic to its dual. However, V_K *is* isomorphic to its dual twisted by the automorphism of $\mathrm{SL}_3(K)$ given by inverse transpose, and under this duality, it is easy to see that $L_{\mathfrak{t},\mathfrak{s}}$ is interchanged with $L_{2\mathfrak{s}^{-1},2\mathfrak{t}^{-1}}$. Therefore, it is a pretty conjecture that the corresponding composed varieties are naturally dual.

Conjecture 24.3. *Let K be a 2-adic local field and $0 \le t \le s \le e = v_K(2)$ be integers. Let $C_1 \subseteq C_2$ be orders in a cubic K-algebra R such that $C_2/C_1 \cong \mathcal{O}_K/\pi^{s-t}$ is an $\mathcal{O}_K$-module with one generator. For each quartic K-algebra L with resolvent R, denote by $g(L, C_1, C_2, t, s)$ the number of (t,s)-traced quartic rings in L with reduced resolvent and coresolvent C_1 and C_2, respectively. Then the dual of $g(L, C_1, C_2, t, s)$, considered as a function of L, is*

$$\hat{g}(L, C_1, C_2, t, s) = q^{t+s} g(L, C_1, C_2, e-s, e-t) \tag{181}$$

where $q = |k_K|$ is the order of the residue field.

Note that the quartic rings counted on either side of (181) actually have resolvents $\mathcal{O}_K + \pi^t C_1$ and $\mathcal{O}_K + \pi^{e-s} C_1$ and discriminants $\pi^{2t} \operatorname{disc} C_1$ and $\pi^{2e-2s} \operatorname{disc} C_1$, respectively. If $t + s = e$, this conjecture asserts the self-duality (up to the correct scaling) of the indicated local weighting.

If this conjecture is true, then by our reflection engine, we immediately get the following corresponding global result.

Conjecture 24.4. *Let K be a number field. Let $C_1 \subseteq C_2$ be orders in a cubic K-algebra R such that $C_2/C_1 \cong \mathcal{O}_K/\mathfrak{d}$ is an $\mathcal{O}_K$-module with one generator. Let $\mathfrak{t}, \mathfrak{s} \subseteq \mathcal{O}_K$ be ideals such that $\mathfrak{s} = \mathfrak{d}\mathfrak{t} \mid (2)$. Let $h(C_1, C_2, \mathfrak{t}, \mathfrak{s})$ count the number of $(\mathfrak{t}, \mathfrak{s})$-traced quartic rings with reduced resolvent and coresolvent C_1 and C_2, respectively, each weighted by the reciprocal of its number of resolvent-preserving automorphisms. Let $h^{\mathrm{ntc}}(C_1, C_2, \mathfrak{t}, \mathfrak{s})$ count the subset of the foregoing that are ntc, weighted in the same way. Then*

$$h(C_1, C_2, \mathfrak{t}, \mathfrak{s}) = \frac{N(\mathfrak{t}\mathfrak{s})}{2^{r_\infty}} \cdot h^{\mathrm{ntc}}(C_1, C_2, 2\mathfrak{s}^{-1}, 2\mathfrak{t}^{-1}),$$

where r_∞ is the number of real places of K over which R is not totally real plus twice the number of complex places of K.

25 Reflection for $2 \times n \times n$ boxes

We close with a conjectural generalization to pairs of symmetric matrices $(\mathcal{A}, \mathcal{B})$ of any odd order n. These play an important role in understanding 2-torsion in n-ic rings, owing to a parametrization of Wood [60] as well as the Selmer groups of hyperelliptic curves of genus $(n-1)/2$ (see [6]). The connection to quartic rings, on the other hand, has no known analogue.

Let K be a field, $\operatorname{char} K \neq 2$ and n be an odd integer. The group $\Gamma = \mathrm{SL}_n$ acts on the space V of pairs of symmetric matrices $(\mathcal{A}, \mathcal{B})$ over K, preserving the resolvent

$$f(x, y) = 2^{n-1} \det(\mathcal{A}x - \mathcal{B}y).$$

The point stabilizer of an orbit with resolvent f is isomorphic to $\mathcal{C}_2^{n-1}$, with Galois action permuting a hyperbasis as it permutes the roots of f, and the variety (V_f, Γ) of pairs with fixed resolvent is a composed variety (closely related to the "third representation" of SO_n in [7]). If $\mathcal{O}_K \subseteq K$ is a Dedekind subring with fraction field K, there are integral forms $(\mathcal{V}_{\mathfrak{a},\mathfrak{t},\mathfrak{s}}, \mathcal{G}_{\mathfrak{a}})$ of V for each $[\mathfrak{a}] \in \mathrm{Cl}(\mathcal{O}_K)$ and all ideals $(1) \supseteq \mathfrak{t} \supseteq \mathfrak{s} \supseteq (2)$, defined by a straightforward extension of the $2 \times 3 \times 3$ case. For simplicity we look only at the case when $[\mathfrak{a}] = [1]$, $\mathfrak{t} = (\tau) = \mathfrak{s}$ are principal:

$$\mathcal{V}_\tau(\mathcal{O}_K) = \left\{ [a_{ij}, b_{ij}] : a_{ij}, b_{ij} \in (2^{-1}\tau)^{\mathbf{1}_{i \neq j}} \mathcal{O}_K \right\}.$$

Note that the resolvent f of such a box is divisible by τ^{n-1}, since

$$f(x, y) = \tau^{n-1} \cdot 2^{-1}\tau \det\left(2\tau^{-1}(\mathcal{A}x - \mathcal{B}y)\right),$$

and the argument to the determinant is an $\mathcal{O}_K$-integral matrix that is skew-symmetric, hence singular (being of odd order), modulo $2\tau^{-1}$.

Conjecture 25.1 (**Local O-N for $2 \times n \times n$ boxes**). *If K is a local field,* $\operatorname{char} K \neq 2$, *then*

$$\mathcal{V}_{\tau, \tau^{n-1} f} \quad \textit{and} \quad \mathcal{V}_{2\tau^{-1}, (2\tau^{-1})^{n-1} f}$$

are naturally dual with duality constant $q^{(n-1)v_K(\tau)}$; in order words, for every binary n-ic form f, the associated local orbit counters

$$g_{\tau,f} : H^1(K, M_f) \to \mathbb{N}$$

satisfy the local reflection theorem

$$\hat{g}_{\tau,f} = |\mathcal{O}_K/\tau\mathcal{O}_K|^{n-1} \cdot g_{2\tau^{-1},4f}.$$

If this conjecture is true, our local-to-global reflection engine yields the following.

Conjecture 25.2 (**O-N for $2 \times n \times n$ boxes**). *Let K be a number field, and let τ be a divisor of 2 in $\mathcal{O}_K$. Denote by $h_\tau(f)$ the number of $\Gamma(\mathcal{O}_K) = \mathrm{SL}_n(\mathcal{O}_K)$-orbits of pairs $(\mathcal{A}, \mathcal{B})$ of $n \times n$ symmetric matrices whose on- and off-diagonal elements belong to $\mathcal{O}_K$ and $2^{-1}\tau\mathcal{O}_K$ respectively, each $(\mathcal{A}, \mathcal{B})$ weighted by the reciprocal of the order of its stabilizer in $\Gamma(\mathcal{O}_K)$. Denote by $h_\tau^{\mathrm{ntc}}(f)$ the count (by the same weighting) of the subset of orbits whose corresponding self-balanced ideal (R_f, I, δ) has $\delta > 0$ at every real place of K. Then we have a global reflection theorem*

$$h_\tau(\tau^{n-1} f) = \frac{N(\mathfrak{t})^2}{2^{r_\infty}} \cdot h_{2\tau^{-1}}^{\mathrm{ntc}}\left((2\tau^{-1})^{n-1}\right),$$

where $r_\infty \in \mathbb{Z}$ depends only on the splitting type of f at each of the real places of K.

While some low-discriminant cases of this conjecture can be verified using the known structure of self-balanced ideals, the general case—which involves the Igusa zeta function of an intersection of two quadrics in $\mathbb{P}^{n-1}$—is quite far from solvable using the techniques in this paper. If true, it furnishes a more satisfactory answer to the question addressed by Cohen–Rubinstein-Salzedo–Thorne [12], namely the production of a family of O-N-like reflection theorems for representations whose dimensions go to infinity.

Part IX

Appendices

A The Grothendieck-Witt ring and the proof of Lemma 19.11

In this section we prove Lemma 19.11, which is of a different character than the other results in this paper.

To prove this lemma, we must recall some facts about the Grothendieck-Witt ring of a local field. The nondegenerate quadratic forms over a field K ($\operatorname{char} K \neq 2$), up to isomorphism, form a semiring under the operations of orthogonal direct sum $\perp$ and tensor product $\otimes$; it is cancellative (the so-called *Witt cancellation theorem*), and the ring obtained by adjoining formal additive inverses is called the *Grothendieck-Witt ring* $GW(K)$ of K. In the case that K is a local field, a form is determined (see O'Meara [46], Theorem 63:20) by three invariants: its dimension $n \in \mathbb{Z}_{\geq 0}$, its determinant $D \in K^\times/(K^\times)^2$, and one other bit of information, the *Hasse symbol* $\varepsilon \in \{\pm 1\}$. For a diagonal form $a_1x_1^2 + \cdots + a_nx_n^2$, the determinant is given by $D = a_1 \cdots a_n$ and the Hasse symbol by

$$\varepsilon = \prod_{i<j} \langle a_i, a_j \rangle_K .$$

(The determinant is also called the *discriminant*; our choice of terminology is influenced partly by the clash in sign with the discriminant of a binary quadratic form.)

Every combination of dimension, determinant, and Hasse symbol determines a unique element of $GW(K)$. For dimension at least 3, all elements are actually realized by a quadratic form; in dimension 3, the Hasse symbol carries the same information as the class in the Brauer group of the associated conic. The structure of $GW(K)$ in terms of these invariants is easily computed by

reducing to the case of diagonal forms; the formulas are here recorded, as they will be useful to us.

$$\dim(f \perp g) = \dim f + \dim g \tag{182}$$

$$\det(f \perp g) = \det f \det g \tag{183}$$

$$\varepsilon(f \perp g) = \varepsilon(f)\varepsilon(g) \langle \det f, \det g \rangle_K \tag{184}$$

$$\dim(f \otimes g) = \dim f \dim g \tag{185}$$

$$\det(f \otimes g) = (\det f)^{\dim g} (\det g)^{\dim f} \tag{186}$$

$$\varepsilon(f \otimes g) = \varepsilon(f)^{\dim g} \varepsilon(g)^{\dim f} \langle \det f, -1 \rangle_K^{\binom{\dim g}{2}} \langle \det g, -1 \rangle_K^{\binom{\dim f}{2}} \langle \det f, \det g \rangle_K^{\dim f \dim g - 1}. \tag{187}$$

We denote by Ell_K the unique class in $GW(K)$ of dimension 0, determinant 1, and Hasse symbol -1 (the "elliptic class"). Note that if f and g are nonisomorphic quadratic forms over K with the same dimension and determinant, then $[f] = [g] + \mathrm{Ell}_K$ in $GW(K)$.

Suppose that L/K is a field extension. If $q : W \to L$ is a quadratic form over L, we can view W as a K-vector space and postcompose with the trace $\mathrm{tr}_{L/K}$ to get a quadratic form $\mathrm{tr}_{L/K} q$. Since $\mathrm{tr}_{L/K}$ respects orthogonal direct sums, it induces a group homomorphism (though not a ring homomorphism) from $GW(L)$ to $GW(K)$ (the opposite direction to the more familiar extension-of-scalars morphism). We easily compute that

$$\dim \mathrm{tr}_{L/K} q = [L : K] \cdot \dim q \quad \text{and} \quad \det \mathrm{tr}_{L/K} q = (\mathrm{disc}(L/K))^{\dim q} \cdot N_{L/K}(\det q).$$

We wish to understand how $\varepsilon(\mathrm{tr}_{L/K} q)$ behaves. The following is the most important result needed.

Lemma A.1. *For any extension L/K of local fields not of characteristic 2,*

$$\mathrm{tr}_{L/K} \mathrm{Ell}_L = \mathrm{Ell}_K.$$

In other words, $\mathrm{tr}_{L/K} : GW(L) \to GW(K)$ preserves the Hasse symbol on classes of dimension 0 and determinant 1.

Proof. We may assume that L/K is a *primitive* extension, that is, has no nontrivial intermediate extensions, since $\mathrm{tr}_{E/K} \circ \mathrm{tr}_{L/E} = \mathrm{tr}_{L/K}$ for a tower $L/E/K$.

Since $\mathrm{tr}_{L/K}\,\mathrm{Ell}_L$ is of dimension 0 and determinant 1, the only other possibility is that $\mathrm{tr}_{L/K}\,\mathrm{Ell}_L = 0$. We prove that this cannot hold.

Let $a \in K^\times$ be an element that does not become a square in L. Such an a exists because L/K is primitive; if not, then L/K would contain both an unramified and a ramified quadratic extension. Then choose $\theta \in L$ such that $\langle a, \theta\rangle_L = -1$. We also have $\langle a, N_{L/K}(\theta)\rangle_K = -1$ by the standard relation $\langle a, \theta\rangle_L = \langle a, N_{L/K}(\theta)\rangle_K$ ($a \in K$, $\theta \in L$). Consider the following quadratic forms over L:

$$f(x,y) = x^2 - \theta y^2, \quad g(x,y) = ax^2 - a\theta y^2.$$

In other words, $f = q_1 \perp q_{-\theta}$ and $g = q_a + q_{-a\theta}$ where $q_a(x) = ax^2$. Both f and g have dimension 2 and discriminant $-\theta$, but their Hasse symbols are 1 and $\langle a, -a\theta\rangle = -1$, respectively. Hence $[f] = [g] + \mathrm{Ell}_L$. But $g = af$, so $\mathrm{tr}_{L/K}(g) = a\,\mathrm{tr}_{L/K}(f) = q_a \otimes \mathrm{tr}_{L/K}(f)$. So by the formula (187) for the Hasse symbol of a tensor product,

$$\begin{aligned}
\varepsilon(\mathrm{tr}_{L/K}\, g) &= \varepsilon(q_a \otimes \mathrm{tr}_{L/K}\, f) \\
&= \varepsilon(q_a)^{2[L:K]} \cdot \varepsilon(\mathrm{tr}_{L/K}\, f)^1 \cdot \langle \det q_a, -1\rangle^{\binom{2[L:K]}{2}} \cdot \langle \det \mathrm{tr}_{L/K}\, f, -1\rangle^{\binom{1}{2}} \cdot \langle \det q_a, \det \mathrm{tr}_{L/K}\, f\rangle^{4[L:K]-1} \\
&= \varepsilon(\mathrm{tr}_{L/K}\, f) \cdot \langle a, -1\rangle^{[L:K]} \cdot \langle a, (\mathrm{disc}(L/K))^2 \cdot N_{L/K}(\det f)\rangle^{4[L:K]-1} \\
&= \varepsilon(\mathrm{tr}_{L/K}\, f) \cdot \langle a, -1\rangle^{[L:K]} \cdot \langle a, N_{L/K}(-\theta)\rangle \\
&= \varepsilon(\mathrm{tr}_{L/K}\, f) \cdot \langle a, N_{L/K}(\theta)\rangle \\
&= -\varepsilon(\mathrm{tr}_{L/K}\, f),
\end{aligned}$$

So $[\mathrm{tr}_{L/K}\, f] = [\mathrm{tr}_{L/K}\, g] + \mathrm{Ell}_K$, yielding the desired conclusion. ∎

Proof of Lemma 19.11. We now relate $\varepsilon(\alpha)$ to Hasse symbols. Denote by $q_{R,\alpha}$ the quadratic form

$$q_{R,\alpha}(\xi) = \alpha\xi^2$$

over R. Then $\varepsilon(\alpha) = 1$ if and only if the form $\mathrm{tr}_{R/K}(q_{R,\alpha})$ is isotropic, where $\mathrm{tr}_{R/K}$ is to be interpreted in the obvious way if R is not a field. Given $\alpha, \beta \in R^\times$ of norm 1, the forms

$$f = q_{R,1} \perp q_{R,\alpha\beta} \quad \text{and} \quad g = q_{R,\alpha} \perp q_{R,\beta}$$

have dimension 2 and determinant $\alpha\beta$ over R, and in $GW(K)$,

$$\varepsilon(1)\varepsilon(\alpha)\varepsilon(\beta)\varepsilon(\alpha\beta) = \varepsilon([\mathrm{tr}_{R/K}\, f] - [\mathrm{tr}_{R/K}\, g]).$$

Decompose $R = \prod_{i=1}^r R_i$ into its field factors ($1 \le r \le 3$), and let $\alpha = (\alpha_1; \ldots; \alpha_r)$ and $\beta = (\beta_1; \ldots; \beta_r)$. Then

$$[\mathrm{tr}_{R/K}\, f] - [\mathrm{tr}_{R/K}\, g] = \sum_{i=1}^{r} \mathrm{tr}_{R_i/K}([q_{R_i,\alpha_i\beta_i}] - [q_{R_i,\alpha_i}] - [q_{R_i,\beta_i}] + [q_{R_i,1}]).$$

Since the invariants of each $q_{R_i,\gamma}$ are known, the invariants of the class in parentheses can be computed by repeated application of (182)–(184). We find that it has dimension 0, determinant 1 and Hasse symbol $\langle \alpha_i, \beta_i \rangle_{R_i}$. By the preceding lemma, its trace has the same invariants. Hence the whole sum has Hasse symbol

$$\prod_i \langle \alpha_i, \beta_i \rangle_{R_i} = \langle \alpha, \beta \rangle_R \,,$$

as desired. ■

B Examples of zone totals

The following tables serve to illustrate some of the totals computed in Section 21.

The following are valid in the unramified splitting types (111, 12, and 3): more specifically, the first table (with $s = 0$) applies to all three, the remaining ones to splitting types 111 and 12.

For brevity, the following conventions have been observed:

- In the red zone, the answer (which is independent of ℓ_C) is the sum of the red-colored entries

of the corresponding row.

- In the other color zones, the answer is the single entry corresponding to the appropriate values of ℓ_C and n_{11}.

- The invariable factor of $q^{-m_{11}}$ has been omitted.

For $e = 8, s = 0$ (similar results hold whenever $s = 0$):

$\ell_C \to$	0	1	2	3	4
$n_{11} = 16$	$q^0F(8,0,0)$	$q^0F(8,0,0)$	$q^0F(8,0,0)$	$q^0F(8,0,0)$	$q^0F(8,0,0)$
15	$q^0F(7,1,0)$	$q^0F(7,1,0)$	$q^0F(7,1,0)$	$q^0F(7,1,0)$	$q^0F(7,1,0)$
14	$(1+\varepsilon_C)q^0F(7,0,1)$	$q^0F(7,0,1)$	$q^0F(7,0,1)$	$q^0F(7,0,1)$	$q^0F(7,0,1)$
13	$(1+\varepsilon_C)q^0F(6,1,1)$	$q^0F(6,1,1)$	$q^0F(6,1,1)$	$q^0F(6,1,1)$	$q^0F(6,1,1)$
12	$(1+\varepsilon_C)q^0F(6,0,2)$	$q^1F(6,1,1)$	$q^1F(6,1,1)$	$q^1F(6,1,1)$	$q^1F(6,1,1)$
11	$(1+\varepsilon_C)q^0F(5,1,2)$	$q^1F(5,2,1)$	$q^1F(5,2,1)$	$q^1F(5,2,1)$	$q^1F(5,2,1)$
10	$(1+\varepsilon_C)q^0F(5,0,3)$	$(1+\varepsilon_C)q^1F(5,1,2)$	$q^1F(5,1,2)$	$q^1F(5,1,2)$	$q^1F(5,1,2)$
9	$(1+\varepsilon_C)q^0F(4,1,3)$	$(1+\varepsilon_C)q^1F(4,2,2)$	$q^1F(4,2,2)$	$q^1F(4,2,2)$	$q^1F(4,2,2)$
8	$(1+\varepsilon_C)q^0F(4,0,4)$	$(1+\varepsilon_C)q^1F(4,1,3)$	$q^2F(4,2,2)$	$q^2F(4,2,2)$	$q^2F(4,2,2)$
7	$(1+\varepsilon_C)q^0F(3,1,4)$	$(1+\varepsilon_C)q^1F(3,2,3)$	$q^2F(3,3,2)$	$q^2F(3,3,2)$	$q^2F(3,3,2)$
6	$(1+\varepsilon_C)q^0F(3,0,5)$	$(1+\varepsilon_C)q^1F(3,1,4)$	$(1+\varepsilon_C)q^2F(3,2,3)$	$q^2F(3,2,3)$	$q^2F(3,2,3)$
5	$(1+\varepsilon_C)q^0F(2,1,5)$	$(1+\varepsilon_C)q^1F(2,2,4)$	$(1+\varepsilon_C)q^2G^\times(2,3,3)$	$q^2G(3,2,3)$	—
4	$(1+\varepsilon_C)q^0F(2,0,6)$	$(1+\varepsilon_C)q^1F(2,1,5)$	$(1+\varepsilon_C)q^2G^\times(2,2,4)$	$q^3G(3,2,3)$	—
3	$(1+\varepsilon_C)q^0F(1,1,6)$	$(1+\varepsilon_C)q^1G^\times(1,2,5)$	$(1+\varepsilon_C)q^2G^\times(2,2,4)$	$q^3G(3,2,3)$	—
2	$(1+\varepsilon_C)q^0F(1,0,7)$	$(1+\varepsilon_C)q^1G^\times(1,1,6)$	$(1+\varepsilon_C)q^2G^\times(2,1,5)$	$(1+\varepsilon_C)q^3G^\times(3,1,4)$	$q^3G(4,0,4)$
1	$(1+\varepsilon_C)q^0G^\times(0,1,7)$	$(1+\varepsilon_C)q^1G^\times(1,1,6)$	$(1+\varepsilon_C)q^2G^\times(2,1,5)$	$(1+\varepsilon_C)q^3G^\times(3,1,4)$	$q^3G(4,0,4)$

For $e = 6, s = 14$ (similar results hold whenever $s \geq 2e$):

$\ell_C \to$	any
$n_{11} = 12$	$2q^0F(6,0,\emptyset)$
11	$2q^0F(5,1,\emptyset)$
10	$2q^1F(5,1,\emptyset)$
9	$2q^1F(4,2,\emptyset)$
8	$2q^2F(4,2,\emptyset)$
7	$2q^2F(3,3,\emptyset)$
6	$2q^3F(3,3,\emptyset)$
5	$2q^3F(2,4,\emptyset)$
4	$2q^4F(2,4,\emptyset)$
3	$2q^4F(1,5,\emptyset)$
2	$2q^5F(1,5,\emptyset)$
1	$2q^5F(0,6,\emptyset)$

For $e = 11, s = 7$ (similar results hold whenever $s < 2e$ is odd):

$\ell_C \to$	3
$n_{11} = 22$	$2q^0F(11,0,\emptyset)$
21	$2q^0F(10,1,\emptyset)$
20	$2q^1F(10,1,\emptyset)$
19	$2q^1F(9,2,\emptyset)$
18	$2q^2F(9,2,\emptyset)$
17	$2q^2F(8,3,\emptyset)$
16	$2q^3F(8,3,\emptyset)$
15	$(1+\varepsilon_C)q^3F(7,4,0)$
14	$(1+\varepsilon_C)q^3F(7,3,1)$
13	$(1+\varepsilon_C)q^3F(6,4,1)$
12	$(1+\varepsilon_C)q^3F(6,3,2)$
11	$(1+\varepsilon_C)q^3F(5,4,2)$
10	$(1+\varepsilon_C)q^3F(5,3,3)$
9	$(1+\varepsilon_C)q^3F(4,4,3)$
8	$(1+\varepsilon_C)q^3F(4,3,4)$
7	$(1+\varepsilon_C)q^3F(3,4,4)$
6	$(1+\varepsilon_C)q^3F(3,3,5)$
5	$(1+\varepsilon_C)q^3F(2,4,5)$
4	$(1+\varepsilon_C)q^3F(2,3,6)$
3	$(1+\varepsilon_C)q^3F(1,4,6)$
2	$(1+\varepsilon_C)q^3F(1,3,7)$
1	$(1+\varepsilon_C)q^3F(0,4,7)$

For $e = 10, s = 4$ (similar results hold whenever $s < 2e$ is even):

$\ell_C \to$	0	1	2	3	≥ 4
$n_{11} = 20$	$2q^0F(10,0,\emptyset)$	$2q^0F(10,0,\emptyset)$	$2q^0F(10,0,\emptyset)$	$2q^0F(10,0,\emptyset)$	$2q^0F(10,0,\emptyset)$
19	$2q^0F(9,1,\emptyset)$	$2q^0F(9,1,\emptyset)$	$2q^0F(9,1,\emptyset)$	$2q^0F(9,1,\emptyset)$	$2q^0F(9,1,\emptyset)$
18	$2q^1F(9,1,\emptyset)$	$2q^1F(9,1,\emptyset)$	$2q^1F(9,1,\emptyset)$	$2q^1F(9,1,\emptyset)$	$2q^1F(9,1,\emptyset)$
17	$2q^1F(8,2,\emptyset)$	$2q^1F(8,2,\emptyset)$	$2q^1F(8,2,\emptyset)$	$2q^1F(8,2,\emptyset)$	$2q^1F(8,2,\emptyset)$
16	$q^2F(8,2,0)$	$q^2F(8,2,0)$	$q^2F(8,2,0)$	$q^2F(8,2,0)$	$q^2F(8,2,0)$
15	$q^2F(7,3,0)$	$q^2F(7,3,0)$	$q^2F(7,3,0)$	$q^2F(7,3,0)$	$q^2F(7,3,0)$
14	$(1+\varepsilon_C)q^2F(7,2,1)$	$q^2F(7,2,1)$	$q^2F(7,2,1)$	$q^2F(7,2,1)$	$q^2F(7,2,1)$
13	$(1+\varepsilon_C)q^2F(6,3,1)$	$q^2F(6,3,1)$	$q^2F(6,3,1)$	$q^2F(6,3,1)$	$q^2F(6,3,1)$
12	$(1+\varepsilon_C)q^2F(6,2,2)$	$q^3F(6,3,1)$	$q^3F(6,3,1)$	$q^3F(6,3,1)$	$q^3F(6,3,1)$
11	$(1+\varepsilon_C)q^2F(5,3,2)$	$q^3F(5,4,1)$	$q^3F(5,4,1)$	$q^3F(5,4,1)$	$q^3F(5,4,1)$
10	$(1+\varepsilon_C)q^2F(5,2,3)$	$(1+\varepsilon_C)q^3F(5,3,2)$	$q^3F(5,3,2)$	$q^3F(5,3,2)$	$q^3F(5,3,2)$
9	$(1+\varepsilon_C)q^2F(4,3,3)$	$(1+\varepsilon_C)q^3F(4,4,2)$	$q^3F(4,4,2)$	$q^3F(4,4,2)$	$q^3F(4,4,2)$
8	$(1+\varepsilon_C)q^2F(4,2,4)$	$(1+\varepsilon_C)q^3F(4,3,3)$	$q^4F(4,4,2)$	$q^4F(4,4,2)$	$q^4F(4,4,2)$
7	$(1+\varepsilon_C)q^2F(3,3,4)$	$(1+\varepsilon_C)q^3F(3,4,3)$	$q^4F(3,5,2)$	$q^4F(3,5,2)$	$q^4F(3,5,2)$
6	$(1+\varepsilon_C)q^2F(3,2,5)$	$(1+\varepsilon_C)q^3F(3,3,4)$	$(1+\varepsilon_C)q^4F(3,4,3)$	$q^4F(3,4,3)$	$q^4F(3,4,3)$
5	$(1+\varepsilon_C)q^2F(2,3,5)$	$(1+\varepsilon_C)q^3F(2,4,4)$	$(1+\varepsilon_C)q^4G^\times(2,5,3)$	$q^4G(3,4,3)$	—
4	$(1+\varepsilon_C)q^2F(2,2,6)$	$(1+\varepsilon_C)q^3F(2,3,5)$	$(1+\varepsilon_C)q^4G^\times(2,4,4)$	$q^5G(3,4,3)$	—
3	$(1+\varepsilon_C)q^2F(1,3,6)$	$(1+\varepsilon_C)q^3G^\times(1,4,5)$	$(1+\varepsilon_C)q^4G^\times(2,4,4)$	$q^5G(3,4,3)$	—
2	$(1+\varepsilon_C)q^2F(1,2,7)$	$(1+\varepsilon_C)q^3G^\times(1,3,6)$	$(1+\varepsilon_C)q^4G^\times(2,3,5)$	$(1+\varepsilon_C)q^5G^\times(3,3,4)$	$q^5G(4,2,4)$
1	$(1+\varepsilon_C)q^2G^\times(0,3,7)$	$(1+\varepsilon_C)q^3G^\times(1,3,6)$	$(1+\varepsilon_C)q^4G^\times(2,3,5)$	$(1+\varepsilon_C)q^5G^\times(3,3,4)$	$q^5G(4,2,4)$

References

[1] Salim Ali Altuğ, Arul Shankar, Ila Varma, and Kevin H. Wilson. The number of quartic D_4-fields ordered by conductor. Preprint (2017), available at `arxiv.org/abs/1704.01729`.

[2] Manjul Bhargava. Higher composition laws. I. A new view on Gauss composition, and quadratic generalizations. *Ann. of Math. (2)*, 159(1):217–250, 2004.

[3] Manjul Bhargava. Higher composition laws. II. On cubic analogues of Gauss composition. *Ann. of Math. (2)*, 159(2):865–886, 2004.

[4] Manjul Bhargava. Higher composition laws. III. The parametrization of quartic rings. *Ann. of Math. (2)*, 159(3):1329–1360, 2004.

[5] Manjul Bhargava. Higher composition laws. IV. The parametrization of quintic rings. *Ann. of Math. (2)*, 167(1):53–94, 2008.

[6] Manjul Bhargava. Most hyperelliptic curves over $\mathbb{Q}$ have no rational points, 2013. Preprint, available at `arxiv.org/abs/1308.0395`.

[7] Manjul Bhargava and Benedict H. Gross. Arithmetic invariant theory. In *Symmetry: representation theory and its applications*, volume 257 of *Progr. Math.*, pages 33–54. Birkhäuser/Springer, New York, 2014.

[8] Manjul Bhargava, Arul Shankar, and Jacob Tsimerman. On the Davenport-Heilbronn theorems and second order terms. *Invent. Math.*, 193(2):439–499, 2013.

[9] Manjul Bhargava and Ariel Shnidman. On the number of cubic orders of bounded discriminant having automorphism group C_3, and related problems. *Algebra Number Theory*, 8(1):53–88, 2014.

[10] Owen Biesel. *Galois closures for rings*. ProQuest LLC, Ann Arbor, MI, 2013. Thesis (Ph.D.)–Princeton University.

[11] Owen Biesel. Galois closure data for extensions of rings. *Transform. Groups*, 23(1):41–69, 2018.

[12] Henri Cohen, Simon Rubinstein-Salzedo, and Frank Thorne. Identities for field extensions generalizing the Ohno-Nakagawa relations. *Compos. Math.*, 151(11):2059–2075, 2015.

[13] Ilaria Del Corso and Roberto Dvornicich. The compositum of wild extensions of local fields of prime degree. *Monatsh. Math.*, 150(4):271–288, 2007.

[14] David A. Cox. *Primes of the form $x^2 + ny^2$: Fermat, class field theory, and complex multiplication*. Pure and Applied Mathematics (Hoboken). John Wiley & Sons, Inc., Hoboken, NJ, second edition, 2013.

[15] J. E. Cremona. Reduction of binary cubic and quartic forms. *LMS J. Comput. Math.*, 2:64–94, 1999. Available (with corrections) at `https://homepages.warwick.ac.uk/staff/J.E.Cremona/papers/r34jcm.pdf`.

[16] J. E. Cremona. Corrigendum: "Reduction of binary cubic and quartic forms" [LMS J. Comput. Math. **2** (1999), 64–94]. *LMS J. Comput. Math.*, 4:73, 2001.

[17] Henri Darmon, Fred Diamond, and Richard Taylor. Fermat's last theorem. In *Current Developments in Mathematics*, 1994.

[18] Boris Datskovsky and David J. Wright. The adelic zeta function associated to the space of binary cubic forms. II. Local theory. *J. reine angew. Math.*, 367:27–75, 1986.

[19] B. N. Delone and D. K. Faddeev. *The theory of irrationalities of the third degree*. Translations of Mathematical Monographs, Vol. 10. American Mathematical Society, Providence, R.I., 1964.

[20] Jorge Dioses. *Generalizing the theorem of Nakagawa on binary cubic forms to number fields*. ProQuest LLC, Ann Arbor, MI, 2012. Thesis (Ph.D.)–Oklahoma State University. Available at `http://gateway.proquest.com/openurl?url_ver=Z39.88-2004&rft_val_fmt=info:ofi/fmt:kev:mtx:dissertation&res_dat=xri:pqm&rft_dat=xri:pqdiss:3524491`.

[21] Jordan S. Ellenberg and Akshay Venkatesh. Reflection principles and bounds for class group torsion. *Int. Math. Res. Not.*, 2007. Article rnm002, 18 pp. `https://doi.org/10.1093/imrn/rnm002`.

[22] Xia Gao. On the Ohno-Nakagawa theorem. *J. Number Theory*, 189:186–210, 2018.

[23] Georges Gras. Théorèmes de réflexion. *J. Théor. Nombres Bordeaux*, 10(2):399–499, 1998.

[24] Benedict H. Gross and Mark W. Lucianovic. On cubic rings and quaternion rings. *J. Number Theory*, 129(6):1468–1478, 2009.

[25] Fabian Gundlach. *Parametrizing Extensions with Fixed Galois Group*. ProQuest LLC, Ann Arbor, MI, 2019. Thesis (Ph.D.)–Princeton University. Available at `https://fabiangundlach.org/phd-thesis.pdf`.

[26] Helmut Hasse. Arithmetische Theorie der kubischen Zahlkörper auf klassenkörpertheoretischer Grundlage. *Math. Zeits.*, 31(1):565–582, 1930.

[27] Osamu Hyodo. Wild ramification in the imperfect residue field case. In *Galois representations and arithmetic algebraic geometry (Kyoto, 1985/Tokyo, 1986)*, volume 12 of *Adv. Stud. Pure Math.*, pages 287–314. North-Holland, Amsterdam, 1987.

[28] John W. Jones and David P. Roberts. A database of number fields. *LMS Journal of Computation and Mathematics*, 17(1):595–618, 2014.

[29] Andrei Jorza. Math 160c Spring 2013 Caltech. Applications of global class field theory. Course notes. Available at `https://www3.nd.edu/~ajorza/courses/m160c-s2013/overview/m160c-s2013.pdf`.

[30] Max-Albert Knus and Jean-Pierre Tignol. Quartic exercises. *Int. J. Math. Math. Sci.*, 2003. Article ID 284672, 61 pages, `http://dx.doi.org/10.1155/S0161171203203458`.

[31] H. W. Leopoldt. Über Einheitengruppe und Klassenzahl reeller abelscher Zahlkörper. *Abh. Deutsch. Akad. Wiss. Berlin. Kl. Math. Nat.*, 1953(2):48 pp., 1953.

[32] Friedrich Wilhelm Levi. Kubische Zahlkörper und binäre kubische Formenklassen [Cubic number fields and cubic form classes]. *Leipz. Ber.*, 66:26–37, 1914.

[33] Monica Marinescu. A dual description of integral binary cubic forms and the Ohno-Nakagawa identities, 2015. Senior thesis, Princeton University.

[34] Preda Mihăilescu. Reflection, Bernoulli numbers and the proof of Catalan's conjecture. In *European Congress of Mathematics*, pages 325–340. Eur. Math. Soc., Zürich, 2005.

[35] James S. Milne. Fields and Galois theory (v4.30), 2012. Available at www.jmilne.org/math/.

[36] Jin Nakagawa. A conjecture on the zeta functions of pairs of ternary quadratic forms. Preprint (2017), available at `https://arxiv.org/abs/1707.00789`.

[37] Jin Nakagawa. Orders of a quartic field. *Mem. Amer. Math. Soc.*, 122(583):viii+75, 1996.

[38] Jin Nakagawa. On the relations among the class numbers of binary cubic forms. *Invent. Math.*, 134(1):101–138, 1998.

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

[40] Jürgen Neukirch, Alexander Schmidt, and Kay Wingberg. *Cohomology of number fields*, volume 323 of *Grundlehren der Mathematischen Wissenschaften [Fundamental Principles of Mathematical Sciences]*. Springer-Verlag, Berlin, 2000.

[41] Thong Nguyen-Quang-Do. Filtration de K^*/K^{*p} et ramification sauvage. *Acta Arith.*, 30(4):323–340, 1976.

[42] Evan M. O'Dorney. Rings of small rank over a Dedekind domain and their ideals. *Res. Math. Sci.*, 3(8), 2016.

[43] Evan M. O'Dorney. On a remarkable identity in class numbers of cubic rings. *Journal of Number Theory*, 176:302–332, 2017.

[44] Yasuo Ohno. A conjecture on coincidence among the zeta functions associated with the space of binary cubic forms. *Amer. J. Math.*, 119(5):1083–1094, 1997.

[45] Yasuo Ohno and Takashi Taniguchi. Relations among Dirichlet series whose coefficients are class numbers of binary cubic forms II. *Math. Res. Lett.*, 21(2):363–378, 2014.

[46] O. Timothy O'Meara. *Introduction to quadratic forms*. Classics in Mathematics. Springer-Verlag, Berlin, 2000. Reprint of the 1973 edition.

[47] Charles A. Osborne. $GL_2(O_K)$-invariant lattices in the space of binary cubic forms with coefficients in the number field K. *Proc. Amer. Math. Soc.*, 142(7):2313–2325, 2014.

[48] Mikio Sato and Takuro Shintani. On zeta functions associated with prehomogeneous vector spaces. *Ann. of Math. (2)*, 100:131–170, 1974.

[49] Arnold Scholz. Über die Beziehung der Klassenzahlen quadratischer Körper zueinander. *J. reine angew. Math.*, 166:201–203, 1932.

[50] I. Schur. Elementarer Beweis eines Satzes von L. Stickelberger. *Math. Zeits.*, 29:464–465, 1929.

[51] Jean-Pierre Serre. *Local fields*, volume 67 of *Graduate Texts in Mathematics*. Springer-Verlag, New York-Berlin, 1979. Translated from the French by Marvin Jay Greenberg.

[52] Takuro Shintani. On Dirichlet series whose coefficients are class numbers of integral binary cubic forms. *J. Math. Soc. Japan*, 24:132–188, 1972.

[53] Takashi Taniguchi and Frank Thorne. Orbital exponential sums for prehomogeneous vector spaces. Preprint (2016), available at `https://arxiv.org/abs/1607.07827`.

[54] Takashi Taniguchi and Frank Thorne. Secondary terms in counting functions for cubic fields. *Duke Math. J.*, 162(13):2451–2508, 2013.

[55] J. T. Tate. Fourier analysis in number fields, and Hecke's zeta-functions. In J. W. S. Cassels and A. Fröhlich, editors, *Algebraic Number Theory (Proc. Instructional Conf., Brighton, 1965)*, pages 305–347. Thompson, Washington, D.C., 1967.

[56] Frank Thorne. Shintani's zeta function is not a finite sum of Euler products. *Proc. Amer. Math. Soc.*, 142(6):1943–1952, 2014.

[57] Melanie Matchett Wood. Gauss composition over an arbitrary base. *Adv. Math.*, 226(2):1756–1771, 2011.

[58] Melanie Matchett Wood. Parametrizing quartic algebras over an arbitrary base. *Algebra Number Theory*, 5(8):1069–1094, 2011.

[59] Melanie Matchett Wood. Quartic rings associated to binary quartic forms. *Int. Math. Res. Not.*, 2012(6):1300–1320, 2012.

[60] Melanie Matchett Wood. Parametrization of ideal classes in rings associated to binary forms. *J. reine angew. Math.*, 689:169–199, 2014.

[61] Liang Xiao and Igor Zhukov. Ramification of higher local fields, approaches and questions. *Algebra i Analiz*, 26:1–63, 2014.