ON UNIT SIGNATURES AND NARROW CLASS GROUPS OF ODD ABELIAN NUMBER FIELDS: STRUCTURE AND HEURISTICS

BENJAMIN BREEN, ILA VARMA, AND JOHN VOIGHT
(APPENDIX WITH NOAM ELKIES)

Abstract. For an abelian number field of odd degree, we study the structure of its 2-Selmer group as a bilinear space and as a Galois module. We prove structural results and make predictions for the distribution of unit signature ranks and narrow class groups in families where the degree and Galois group are fixed.

Contents

1. Introduction

1.1. **Motivation.** Originating in the study of solutions to the negative Pell equation, the investigation of signatures of units in number rings dates back at least to Lagrange. While a considerable amount of progress has been made for quadratic fields [38, 21, 7], predictions for the distribution of narrow class groups and possible signs of units under real embeddings for certain families of higher degree number fields have only recently been developed [16, 14, 4].

In this paper, we study unit signatures and class groups of abelian number fields of odd degree. To illustrate and motivate our results, we begin with two special cases.

Conjecture 1.1.1 (Conjecture 6.3.3)**.** *As K varies over cyclic cubic number fields, the probability that K has a totally positive system of fundamental units is approximately* 3%.

For the conjectures presented in this paper, we sidestep the issue of ordering fields: we expect that any *fair* counting function in the terminology of Wood [41] should be allowed, for

Date: July 31, 2020.
2020 *Mathematics Subject Classification.* 11R29, 11R27, 11R45, 11Y40.

example ordering by conductor or by the norm of the product of ramified primes. We are led to Conjecture 1.1.1 by combining structural results established herein with a randomness hypothesis (H2) in the vein of the Cohen–Lenstra heuristics. This conjecture agrees well with computational evidence (see section 7.1); the following theorem provides additional theoretical support.

Theorem 1.1.2 (Theorem A.1.2, with Elkies)**.** *There exist infinitely many cyclic cubic fields with a totally positive system of fundamental units.*

The proof of Theorem 1.1.2 involves the study the integral points on a log K3 surface. The (infinite) family of *simplest cubic fields* of Shanks were each shown to have units of all possible signatures by Washington [40, p. 371], the case complementary to Theorem 1.1.2.

Our second illustrative conjecture is as follows.

Conjecture 1.1.3 (Conjecture 6.1.1)**.** *As K ranges over cyclic number fields of degree 7 with odd class number, the probability that the narrow class number is odd is $7/9$.*

This conjecture also matches computational evidence well (see section 7.2).

The predictions above are based on the philosophy underlying the Cohen–Lenstra heuristics, which predicts random behavior for arithmetic objects *as soon as* one accounts for all of the determined structure. Early examples of the need to account for structural properties, including genus theory and ranks of units, were already present in the original paper of Cohen–Lenstra [9]. It remains mysterious and important to understand how one must account for additional structure in generalizations following the Cohen–Lenstra heuristics. For example, what makes a prime *good* [11], and the interaction between p-parts of class groups and the presence of pth roots of unity [32, 33, 2], remain unresolved. On the other hand, some reflection principles like those of Scholz and Leopoldt [28], seem to be inherently compatible with the Cohen–Lenstra–Martinet conjectures [17, 26, 27].

In this paper, we propose a model for the distribution of 2-parts of narrow class groups and signatures of units in families of abelian number fields of fixed odd degree and Galois group. For such families, the Galois action and the presence of the 2nd roots of unity suggest additional, nontrivial structure to account for (as confirmed by computations and available function field analogues). The requirement that the degree is odd when $p = 2$ isolates the "roots of unity problem" from other obstructions to arithmetic randomness, including genus theory. Since the narrow class group is an extension of the class group by an abelian 2-group that measures signatures of units, our efforts are concentrated on 2-parts.

Our contributions are thus twofold. First, for these families we precisely identify and analyze relevant structure, including the relationship to reflection principles. Second, under the hypothesis that what remains behaves randomly, we make exact predictions for the behavior of units and class groups—with corroborating, computational evidence.

1.2. **Structure: class groups.** We now set up the structures we study and model in this paper. We build on work of Dummit–Voight [16], who make predictions for fields of odd degree n with Galois group S_n—here, we instead consider Galois extensions of odd degree.

Recall that the 2-Selmer group of a number field K is

$$\mathrm{Sel}_2(K) := \{\alpha \in K^\times : (\alpha) = \mathfrak{a}^2 \text{ for a fractional ideal } \mathfrak{a} \text{ of } K\}/(K^\times)^2.$$

Attached to K is a finite-dimensional $\mathbb{F}_2$-vector space $V_\infty(K) \boxplus V_2(K)$ equipped with a nondegenerate symmetric bilinear form and a homomorphism

$$\varphi_K \colon \mathrm{Sel}_2(K) \to V_\infty(K) \boxplus V_2(K)$$

called the 2-Selmer signature map. Dummit–Voight [16] showed that the image $S(K) := \mathrm{img}(\varphi_K)$ of φ_K is a maximal, totally isotropic subspace. If K is Galois over $\mathbb{Q}$ with Galois group G_K, then we observe that the above objects carry a G_K-action and in particular $S(K)$ is a G_K-invariant, maximal totally isotropic subspace (Corollary 3.1.3).

In preparation for stating our guiding result, we introduce a bit of notation. Let G be a finite abelian group of odd order and let χ be an $\overline{\mathbb{F}}_2$-character of G. Then every irreducible $\mathbb{F}_2[G]$-module is isomorphic to $\mathbb{F}_2(\chi)$, the value field of a $\overline{\mathbb{F}}_2$-character $\chi\colon G \to \overline{\mathbb{F}}_2^\times$ taking values in a (fixed) algebraic closure $\overline{\mathbb{F}}_2$ of $\mathbb{F}_2$. For a finitely generated $\mathbb{Z}[G]$-module M, write $\mathrm{rk}_\chi M$ for the multiplicity of the irreducible module $\mathbb{F}_2(\chi)$ in the $\mathbb{F}_2[G]$-module M/M^2, and let $\mathrm{rk}_2 M := \dim_{\mathbb{F}_2} M/M^2$. For an $\overline{\mathbb{F}}_2$-character χ of G, there is a noncanonical isomorphism $\mathrm{Hom}_{\mathbb{F}_2}(\mathbb{F}_2(\chi), \mathbb{F}_2) \simeq \mathbb{F}_2(\chi^{-1})$ (see Lemma 5.1.2 and the discussion preceding it), and we write $\chi^* := \chi^{-1}$ for the corresponding dual character. We say χ is self-dual if $\mathbb{F}_2(\chi^*) \simeq \mathbb{F}_2(\chi)$ as $\mathbb{F}_2[G]$-modules. For an $\overline{\mathbb{F}}_2$-character χ of G and V an $\mathbb{F}_2[G]$-module, we write V_χ for the $\mathbb{F}_2(\chi)$-isotypic component of V and $V_{\chi^\pm} := V_\chi + V_{\chi^*}$ for the sum. If V is equipped with a symmetric, G-invariant $\mathbb{F}_2$-bilinear form, then the decomposition into the spaces $V_{\chi^\pm}$ is orthogonal (Lemma 3.2.7), giving a canonical decomposition as $\mathbb{F}_2[G]$-modules.

Now let K be a Galois number field with abelian Galois group G_K of odd order; then the class group $\mathrm{Cl}(K)$ and narrow class group $\mathrm{Cl}^+(K)$ are $\mathbb{Z}[G_K]$-modules. For an $\overline{\mathbb{F}}_2$-character χ, we define:

$$\begin{aligned} \rho_\chi(K) &:= \mathrm{rk}_\chi \mathrm{Cl}(K); \\ \rho_\chi^+(K) &:= \mathrm{rk}_\chi \mathrm{Cl}^+(K); \\ k_\chi^+(K) &:= \mathrm{rk}_\chi \mathrm{Cl}^+(K) - \mathrm{rk}_\chi \mathrm{Cl}(K) \\ &= \rho_\chi^+(K) - \rho_\chi(K). \end{aligned} \tag{1.2.1}$$

We refer to $k_\chi^+(K)$ as the χ-isotropy rank. When K is clear from context, we drop it from the notation. Our main theorem, governing the above structures and quantities, is as follows.

Theorem 1.2.2 (Theorem 5.4.2)**.** *Let K be a Galois number field with abelian Galois group G_K of odd order. Then for each $\overline{\mathbb{F}}_2$-character χ, there are exactly 6 possibilities for $S(K)_{\chi^\pm} \leq V_\infty(K) \boxplus V_2(K)$ up to G_K-equivariant isometry.*

Theorem 1.2.2 follows from an investigation of the $\mathbb{F}_2[G_K]$-module structure of the 2-Selmer signature map together with a classification of invariant, maximal isotropic subspaces in a bilinear space with group action. The five possibilities are given in Table 1.2.3, where in the last column we write $q := \#\mathbb{F}_2(\chi) = \#\mathbb{F}_2(\chi^*)$ for the mass, inversely proportional to $\#\,\mathrm{Isom}_G(S_{\chi^\pm})$, the number of G-equivariant isometries of $S_{\chi^\pm}$. All cases occur (see Example 6.4.1), so the statement is optimal in this sense. In fact, the same relations in Table 1.2.3

hold with $V_\infty(K)$ replaced by $V_2(K)$ and $\mathrm{Cl}^+(K)$ is replaced by $\mathrm{Cl}_4(K)$, the ray class group of K of conductor 4; we restrict attention to narrow class groups in this introduction.

		$\mathbb{F}_2[G_K]$-module structure			Comparison and Isotropy Rank			
Case	$\chi = \chi^*$	$S_{\chi^\pm}$	$S_{\chi^\pm} \cap V_\infty$	Mass	ρ_χ and ρ_{χ^*}	ρ_χ^+ and $\rho_{\chi^*}^+$	k_χ^+	$k_{\chi^*}^+$
A	Yes	$\mathbb{F}_2(\chi)$	$\mathbb{F}_2(\chi)$	$\sqrt{q}+1$	$\rho_\chi = \rho_{\chi^*}$	$\rho_\chi^+ = \rho_{\chi^*}^+$	1	1
B	No	$\mathbb{F}_2(\chi)^2$	$\mathbb{F}_2(\chi)$	1	$\rho_\chi = \rho_{\chi^*} + 1$	$\rho_\chi^+ = \rho_{\chi^*}^+$	0	1
B′	No	$\mathbb{F}_2(\chi^*)^2$	$\mathbb{F}_2(\chi^*)$	1	$\rho_\chi = \rho_{\chi^*} - 1$	$\rho_\chi^+ = \rho_{\chi^*}^+$	1	0
C	No	$\mathbb{F}_2(\chi) \oplus \mathbb{F}_2(\chi^*)$	$\mathbb{F}_2(\chi)$	1	$\rho_\chi = \rho_{\chi^*}$	$\rho_\chi^+ = \rho_{\chi^*}^+ - 1$	0	1
C′	No	$\mathbb{F}_2(\chi) \oplus \mathbb{F}_2(\chi^*)$	$\mathbb{F}_2(\chi^*)$	1	$\rho_\chi = \rho_{\chi^*}$	$\rho_\chi^+ = \rho_{\chi^*}^+ + 1$	1	0
D	No	$\mathbb{F}_2(\chi) \oplus \mathbb{F}_2(\chi^*)$	$\{0\}$	$q-1$	$\rho_\chi = \rho_{\chi^*}$	$\rho_\chi^+ = \rho_{\chi^*}^+$	0	0

Table 1.2.3: Possibilities for the Galois bilinear structure of the 2-Selmer group

The following corollary is then immediate.

Corollary 1.2.4. *Under the hypotheses of Theorem 1.2.2, we have*

$$|\mathrm{rk}_\chi \mathrm{Cl}(K) - \mathrm{rk}_{\chi^*} \mathrm{Cl}(K)| \leq 1,$$

$$|\mathrm{rk}_\chi \mathrm{Cl}^+(K) - \mathrm{rk}_{\chi^*} \mathrm{Cl}^+(K)| \leq 1,$$

and $0 \leq k_\chi^+ + k_{\chi^*}^+ \leq 1$.

Corollary 1.2.4 can be seen as a Spiegelungssatz or *reflection theorem* as in Leopoldt [28] for $p = 2$, and therefore Theorem 1.2.2 can be seen as a precise refinement of it. A precursor to Corollary 1.2.4 is the theorem of Armitage–Fröhlich [1], generalized by Taylor [39] and Oriat [34, 35]. Gras then proved a very general T-S-reflection principle [23, Théorème 5.18] (see also the presentation in his book [24, Chapter II, Theorem 5.4.5]); however, certain corollaries for $p = 2$ [24, Chapter II, Corollary 5.4.6(ii)] (details [24, Chapter II, (5.4.9)] added in the second printing) are incorrect: case D of Table 1.2.3 does not appear.

However, recalling our motivation, we show that rank inequalities like Corollary 1.2.4 for a Galois number field K of odd degree follow from Kummer duality and the G_K-module structure of the 2-Selmer group (and its intersection with coordinate subspaces in the 2-Selmer signature space). In particular, the relevant reflection principles are *already encoded*. In particular, we cover easily several classical results from the literature (see section 4.2); these results could also instead be seen to fit into a much more general context (Poitou–Tate duality of Selmer groups). However, in view of the subtleties indicated in the previous paragraph, one advantage of our approach is it provides a self-contained, uniform, and transparent proof of these corollaries. At the same time, the concrete description in Theorem 1.2.2 states the precise structure (in particular, the image of the 2-Selmer group under the signature map is a G_K-invariant, maximal totally isotropic subspace) which must be respected in a random model and thereby serves as the foundation for our heuristics, which we present in sections 1.4–1.5.

1.3. **Structure: units.** The structural result in Theorem 1.2.2 has the following consequence for units. Let $\mathcal{O}_K$ be the ring of integers of K. The archimedean signature map $\operatorname{sgn}_\infty \colon K^\times \to \prod_{v|\infty}\{\pm 1\} \simeq \mathbb{F}_2^n$ is the surjective group homomorphism recording the signs of elements of $K^\times$ under each real embedding; its kernel $K^\times_{>0} := \ker(\operatorname{sgn}_\infty)$ is the group of totally positive elements of K. Let $\mathcal{O}^\times_{K,>0} := \mathcal{O}^\times_K \cap K^\times_{>0}$ denote the group of totally positive units. Define

$$\operatorname{sgnrk}_\chi(\mathcal{O}^\times_K) := \operatorname{rk}_\chi \operatorname{sgn}_\infty(\mathcal{O}^\times_K), \tag{1.3.1}$$

and the unit signature rank of K

$$\operatorname{sgnrk}(\mathcal{O}^\times_K) := \dim_{\mathbb{F}_2} \operatorname{sgn}_\infty(\mathcal{O}^\times_K) = \textstyle\sum_\chi \operatorname{sgnrk}_\chi(\mathcal{O}^\times_K) \cdot [\mathbb{F}_2(\chi) : \mathbb{F}_2], \tag{1.3.2}$$

where the sum indexes over isomorphism classes of $\overline{\mathbb{F}}_2$-characters χ. The structure on unit signature ranks imposed by the Galois module structure is summarized in the following result, keeping the notation (1.2.1).

Theorem 1.3.3 (Theorem 5.5.2)**.** *Let K be an abelian number field of odd degree with Galois group G_K, and let χ be a $\overline{\mathbb{F}}_2$-character of G_K. Then the following statements hold.*

(a) *If $k^+_\chi(K) = 1$, then $\operatorname{sgnrk}_\chi(\mathcal{O}^\times_K) = 0$.*
(b) *If $k^+_\chi(K) = 0$, then $1 - \operatorname{rk}_\chi \operatorname{Cl}(K) \leq \operatorname{sgnrk}_\chi(\mathcal{O}^\times_K) \leq 1$.*

When the degree of K is prime, summing over χ gives the following corollary.

Corollary 1.3.4 (Corollary 5.5.4)**.** *Let K be a cyclic number field of odd prime degree ℓ, and let f be the order of 2 modulo ℓ. Then*

$$\operatorname{sgnrk}(\mathcal{O}^\times_K) \equiv 1 \pmod{f},$$

and the following statements hold.

(a) *If f is odd, then $\frac{\ell+1}{2} - \operatorname{rk}_2 \operatorname{Cl}(K) \leq \operatorname{sgnrk}(\mathcal{O}^\times_K) \leq \ell$;*
(b) *If f is even, then $\ell - \operatorname{rk}_2 \operatorname{Cl}(K) \leq \operatorname{sgnrk}(\mathcal{O}^\times_K) \leq \ell$.*

For example, if 2 is a primitive root modulo ℓ and the class number of K is odd, then $\operatorname{sgnrk}(\mathcal{O}^\times_K) = \ell$; this result for $\ell = 3$ was observed by Armitage–Fröhlich [1, Theorem V].

1.4. **Heuristics: narrow class groups.** We begin by applying the results in the previous section to make predictions for narrow class groups and signatures of units for odd-degree abelian number fields. We keep the notation of (1.2.1).

Let G be a finite abelian group of odd order. A G-number field is a Galois number field K, inside a fixed algebraic closure of $\mathbb{Q}$, equipped with an isomorphism $G_K \simeq G$, where $G_K := \operatorname{Gal}(K \,|\, \mathbb{Q})$. Such a field K is totally real, so ± 1 are the only roots of unity in K.

Returning to Theorem 1.2.2 and Table 1.2.3, we see that the quantities $k^+_\chi, k^+_{\chi^*}$ are uniquely determined by $S_{\chi^\pm}$ in the cases where χ is self-dual or cases (i)–(i′) when χ is not self-dual. However, when χ is not self-dual and $\rho_\chi = \rho_{\chi^*}$, there is a question about the distribution of cases (ii)–(ii′) and (iii). Modeling the image of 2-Selmer signature map as a random totally isotropic G-invariant subspace in the 2-Selmer signature space (see heuristic assumption (H1)), we are led to the following conjecture.

Conjecture 1.4.1 (Conjecture 6.1.1)**.** *Let G be an odd abelian group, and let χ be an $\overline{\mathbb{F}}_2$-character of G that is* not *self-dual with $q := \#\mathbb{F}_2(\chi)$. Then as K varies over G-number fields satisfying $\rho_\chi(K) = \rho_{\chi^*}(K)$,*

$$\begin{aligned} \operatorname{Prob}\big(k_\chi^+(K) + k_{\chi^*}^+(K) = 0\big) &= \frac{q-1}{q+1}; \\ \operatorname{Prob}\big(k_\chi^+(K) + k_{\chi^*}^+(K) = 1\big) &= \frac{2}{q+1}. \end{aligned} \tag{1.4.2}$$

As an example, if 2 has order $\frac{\ell-1}{2}$ modulo a prime $\ell \equiv 7 \pmod 8$, then as K varies over cyclic number fields of degree ℓ such that $\mathrm{Cl}(K)[2]$ is self-dual, Conjecture 1.4.1 predicts that

$$\operatorname{Prob}\big(\mathrm{Cl}^+(K)[2] \simeq \mathrm{Cl}(K)[2]\big) = \frac{2^{\frac{\ell-1}{2}} - 1}{2^{\frac{\ell-1}{2}} + 1}. \tag{1.4.3}$$

We further expect that the probability in Conjecture 1.4.1 remains the same in certain natural subfamilies, such as when we fix the value $\operatorname{rk}_\chi \mathrm{Cl}(K) = \operatorname{rk}_{\chi^*} \mathrm{Cl}(K) = r$. As a special case, we arrive at Conjecture 1.1.3.

1.5. **Heuristics: units.** Next, we make predictions for signatures of units. Our model can be applied under many scenarios; in this introduction, we consider two simple, illustrative cases. We first examine the situation when the degree is prime and the class number is odd. Modeling $\mathcal{O}_K^\times/(\mathcal{O}_K^\times)^2$ as a random G_K-invariant subspace of the 2-Selmer group of K containing -1, and under an independence hypothesis (H2′), we are led to the following conjecture.

Conjecture 1.5.1 (Conjecture 6.2.4)**.** *Let ℓ be an odd prime such that the order f of 2 in $(\mathbb{Z}/\ell\mathbb{Z})^\times$ is odd. Let $q := 2^f$, and define $m := \frac{\ell-1}{2f} \in \mathbb{Z}_{>0}$. Then as K varies over cyclic number fields of degree ℓ with* odd *class number,*

$$\operatorname{Prob}\big(\operatorname{sgnrk}(\mathcal{O}_K^\times) = fs + \tfrac{\ell-1}{2}\big) = \binom{m}{s}\left(\frac{q-1}{q+1}\right)^s\left(\frac{2}{q+1}\right)^{m-s}$$

for $0 \le s \le m$.

Second, we consider the situation when $\ell = 3$ or 5 with no additional assumption on the class number. In this case, Corollary 5.5.4(b) implies that $\operatorname{sgnrk}(\mathcal{O}_K^\times) = 1$ or ℓ. Although complete heuristics for the 2-part of the class group over abelian fields are not known, Malle [32] provides results in the case that $\ell = 3$ or 5. We use the following notation: for $m \in \mathbb{Z}_{\ge 0} \cup \{\infty\}$ and $q \in \mathbb{R}_{>1}$, write $(q)_0 := 1$ and otherwise $(q)_m := \prod_{i=1}^m (1-q^{-i})$. Combining these results with a uniform random hypothesis (H2), we make the following prediction.

Conjecture 1.5.2 (Conjecture 6.3.3)**.** *Let $\ell = 3$ or 5 and $q = 2^{\ell-1}$. As K varies over cyclic number fields of degree ℓ, then*

$$\operatorname{Prob}\big(\operatorname{sgnrk}(\mathcal{O}_K^\times) = 1\big) = \left(1 + \frac{1}{\sqrt{q}}\right)\frac{(\sqrt{q})_\infty (q^2)_\infty}{(q)_\infty^2} \cdot \sum_{r=0}^{\infty} \frac{(\ell-1)^r}{q^{(r^2+3r)/2} \cdot (q)_r} \cdot \frac{q^r - 1}{q^{r+1} - 1}. \tag{1.5.3}$$

Estimating the quantity in (1.5.3), we predict that approximately 3% of cyclic cubic fields have $\mathrm{sgnrk}(\mathcal{O}_K^\times) = 1$ which yields Conjecture 1.1.1. For cyclic quintic fields we predict that this proportion drops to below 0.1%. The predictions in the two conjectures above agree with the computational evidence we compiled: see section 7.

Remark 1.5.4. To extend the above conjectures to all odd primes (or more generally, to all odd abelian groups G), we would need to refine the heuristics of Malle [32, 33] to predict the distribution of $\mathrm{rk}_\chi \mathrm{Cl}(K)$. This distribution will depend on the representation theory of $\mathbb{Z}/\ell\mathbb{Z}$ (or more generally, of G); in particular, the constraints in Theorem 1.2.2 must be respected. In contrast, when 2 is a primitive root modulo ℓ, there is only one nontrivial (necessarily self-dual) $\mathbb{F}_2[\mathbb{Z}/\ell\mathbb{Z}]$-module, so these representation-theoretic complexities are immaterial; in this case, we expect that the generalization of the above conjectures to such ℓ to be more straightforward.

We expect that as $\ell \to \infty$ varies over odd primes, we have $\mathrm{Prob}\big(\mathrm{sgnrk}(\mathcal{O}_K^\times) = 1\big) \to 0\%$, and we plan to give evidence to support this limiting behavior in the future (see also Remark 7.2.3).

Remark 1.5.5. The statements we prove and conjecture above on unit signature ranks in odd degree extensions are quite different than the situation for real quadratic fields, related to solutions to the negative Pell equation. By genus theory, 100% of real quadratic fields have a totally positive unit [21], and the conjectural asymptotic due to Stevenhagen [38] arises from an apparently different heuristic involving Rédei matrices.

Remark 1.5.6. We are not aware of a function field analogue which would bear on the conjectures presented in this section. These conjectures are based on structural properties of the 2-Selmer signature map, which rely in an essential way on the fact that $2 \in \mathcal{O}_K$ is neither a unit nor zero.

1.6. **Outline.** In section 2, we set up basic notation and background. In section 3, we study these objects in general as Galois modules over $\mathbb{F}_2$. We then restrict to the case of odd Galois extensions in section 4 and show how reflection principles follow from the Galois action and Kummer duality—these are for completeness (and to indicate that they are not missing from our model). We then further restrict to abelian extensions and in section 5 prove our main structural result, and we see classical reflection principles as a corollary. In section 6 we introduce our heuristic assumptions and present our conjectures, including details on the low-degree cases. In section 7, we carry out computations that provide some experimental evidence for our conjectures. Finally, in appendix A we prove Theorem 1.1.2.

1.7. **Acknowledgements.** The authors would like to thank Edgar Costa, David Dummit, Noam Elkies, Georges Gras, Brendan Hassett, Hershy Kisilevsky, Evan O'Dorney, Arul Shankar, Jared Weinstein, and Melanie Matchett Wood for comments, and Tommy Hofmann for sharing his list of cyclic septic fields. Special thanks go to the anonymous referee for their detailed feedback and suggestions. Varma was partially supported by an NSF MSPRF Grant (DMS-1502834) and an NSF Grant (DMS-1844206). Voight was supported by an NSF

CAREER Award (DMS-1151047) and a Simons Collaboration Grant (550029). Elkies was partially supported by an NSF grant (DMS-1502161) and a Simons Collaboration Grant.

2. Properties of the 2-Selmer group and its signature spaces

We begin by setting up some notation and recalling basic definitions and previous results.

2.1. **Basic notation.** If A is a (multiplicatively written) abelian group and $m \in \mathbb{Z}_{>0}$, we write

$$A[m] := \{a \in A : a^m = 1\}$$

for the m-torsion subgroup of A. For a prime p, we write

$$\mathrm{rk}_p(A) := \dim_{\mathbb{F}_p}(A/A^p)$$

for the p-rank of A; we then have $\#A[p] = p^{\mathrm{rk}_p(A)}$.

We quickly prove a standard lemma (for lack of a reference). Let $\mathbb{Z}_{(p)} := \{a/b \in \mathbb{Q} : p \nmid b\}$ be the localization away from a prime p.

Lemma 2.1.1. *Let G be a finite group, let $p \nmid \#G$ be prime, and let M be a finitely generated, torsion $\mathbb{Z}_{(p)}[G]$-module. Then there is a (noncanonical) isomorphism $M/pM \xrightarrow{\sim} M[p]$.*

Proof. Recall (by Maschke's theorem) that every finitely generated $\mathbb{F}_p[G]$-module is semisimple, since $p \nmid \#G$. We show that for every irreducible $\mathbb{F}_p[G]$-module N, we have

$$\mathrm{mult}_N(M/pM) = \mathrm{mult}_N(M[p])$$

where mult_N is the multiplicity of N (in a decomposition into irreducibles).

Let $m = p^r$ be the exponent of M (as an abelian group), with $r \geq 0$. We argue by induction on r. If $r \leq 1$, then $pM = \{0\}$ so indeed $M/pM = M = M[p]$.

Suppose the result holds whenever M has exponent dividing p^r; we prove it for M of exponent p^{r+1}. Multiplication by p gives an exact sequence

$$0 \to M[p] \to M \to pM \to 0$$

of $\mathbb{Z}_{(p)}[G]$-modules. We can repeat this with pM, giving the following diagram, with exact rows and columns:

$$\begin{array}{ccccccccc}
 & & 0 & & 0 & & 0 & & \\
 & & \downarrow & & \downarrow & & \downarrow & & \\
0 & \longrightarrow & (pM)[p] & \longrightarrow & pM & \longrightarrow & p^2M & \longrightarrow & 0 \\
 & & \downarrow & & \downarrow & & \downarrow & & \\
0 & \longrightarrow & M[p] & \longrightarrow & M & \longrightarrow & pM & \longrightarrow & 0 \\
 & & \downarrow & & \downarrow & & \downarrow & & \\
0 & \longrightarrow & M_1 & \longrightarrow & M/pM & \longrightarrow & pM/p^2M & \longrightarrow & 0 \\
 & & \downarrow & & \downarrow & & \downarrow & & \\
 & & 0 & & 0 & & 0 & &
\end{array} \tag{2.1.2}$$

Here, $M_1 := \operatorname{coker}((pM)[p] \to M[p]) \simeq M[p]/(pM)[p]$. By semisimplicity, using the left vertical and bottom horizontal maps, we conclude that

$$\begin{aligned} \operatorname{mult}_N(M/pM) &= \operatorname{mult}_N(pM/p^2M) + \operatorname{mult}_N(M_1) \\ \operatorname{mult}_N(M[p]) &= \operatorname{mult}_N((pM)[p]) + \operatorname{mult}_N(M_1) \end{aligned} \tag{2.1.3}$$

which together give

$$\operatorname{mult}_N(M/pM) - \operatorname{mult}_N(M[p]) = \operatorname{mult}_N(pM/p^2M) - \operatorname{mult}_N((pM)[p]); \tag{2.1.4}$$

since pM has exponent p^r, the right-hand side of (2.1.4) is zero, completing the proof. □

Let K be a number field of degree $n = [K : \mathbb{Q}]$ with r_1 real and r_2 complex places, with algebraic closure $\overline{K}$ and with ring of integers $\mathcal{O}_K$. For a prime p, we denote the localization of $\mathcal{O}_K$ away from (p) by

$$\mathcal{O}_{K,(p)} := \{\alpha \in K^\times : \operatorname{ord}_{\mathfrak{p}}(\alpha) \geq 0 \text{ for all primes } \mathfrak{p} \mid (p)\}$$

and the completion of $\mathcal{O}_K$ at p by $\mathcal{O}_{K,p} := \mathcal{O}_K \otimes \mathbb{Z}_p$, so that $\mathcal{O}_{K,(p)} \hookrightarrow \mathcal{O}_{K,p}$. For a place v of K, we let K_v denote the completion of K at v and $\mathcal{O}_{K,v}$ its valuation ring, and we let

$$(\_, \_)_v \colon K_v^\times \times K_v^\times \to \{\pm 1\}$$

denote the Hilbert symbol at v: recall that for α_v and $\beta_v \in K_v^\times$, we have $(\alpha_v, \beta_v)_v = 1$ if and only if β_v is in the image of the norm map from $K_v[x]/(x^2 - \alpha_v)$ to K_v.

2.2. **The 2-Selmer group and its signature spaces.** The main object of study is the 2-Selmer group of a number field K, defined as

$$\operatorname{Sel}_2(K) := \{\alpha \in K^\times : (\alpha) = \mathfrak{a}^2 \text{ for a fractional ideal } \mathfrak{a} \text{ of } K\}/(K^\times)^2.$$

Following Dummit-Voight [16, Section 3], we recall two signature spaces that keep track of behavior at ∞ and at 2, as follows.

Definition 2.2.1. The archimedean signature space $V_\infty(K)$ is defined as

$$V_\infty(K) := \prod_{v \text{ real}} \{\pm 1\} \simeq \prod_{v \mid \infty} K_v^\times / K_v^{\times 2}$$

where the second product runs over all real places of K. The archimedean signature map is

$$\begin{aligned} \operatorname{sgn}_\infty \colon K^\times &\to V_\infty(K) \\ \alpha &\mapsto (\operatorname{sgn} v(\alpha))_v \end{aligned}$$

where $\operatorname{sgn} x = x/|x|$ for $x \in \mathbb{R}^\times$.

By definition, $\ker \operatorname{sgn}_\infty = K_{>0}^\times$, the totally positive elements of K, which contains $(K^\times)^2$, and so the map $\operatorname{sgn}_\infty$ induces a well-defined map $\varphi_{K,\infty} : \operatorname{Sel}_2(K) \to V_\infty(K)$. The product of Hilbert symbols defines a map

$$b_\infty \colon V_\infty(K) \times V_\infty(K) \to \{\pm 1\}$$

which is a (well-defined) symmetric, non-degenerate $\mathbb{F}_2$-bilinear form.

Definition 2.2.2. The 2-adic signature space $V_2(K)$ is defined as

$$V_2(K) := \mathcal{O}_{K,(2)}^\times/(1+4\mathcal{O}_{K,(2)})(\mathcal{O}_{K,(2)}^\times)^2.$$

The 2-adic signature map is the map

$$\operatorname{sgn}_2\colon \mathcal{O}_{K,(2)}^\times \to V_2(K)$$

obtained from the projection $\mathcal{O}_{K,(2)}^\times \to V_2(K)$.

For the following statements we refer to Dummit–Voight [16, §4]. We have $\dim_{\mathbb{F}_2} V_2(K) = n$ and there is an isomorphism of abelian groups

$$V_2(K) \simeq \prod_{v|(2)} \mathcal{O}_{K,v}^\times/(1+4\mathcal{O}_{K,v})(\mathcal{O}_{K,v}^\times)^2.$$

Under this identification, the product of Hilbert symbols defines a map

$$\begin{aligned} b_2\colon V_2(K)\times V_2(K) &\to \{\pm 1\} \\ \big((\alpha_v)_v, (\beta_v)_v\big) &\mapsto \prod_{v|(2)} (\alpha_v,\beta_v)_v, \end{aligned}$$

which is a nondegenerate, symmetric $\mathbb{F}_2$-bilinear form on $V_2(K)$. Every class in $\operatorname{Sel}_2(K)$ has a representative α such that $\alpha \in \mathcal{O}_{K,(2)}^\times$, unique up to multiplication by an element of $(\mathcal{O}_{K,(2)}^\times)^2$; therefore, the map sgn_2 induces a well-defined map $\varphi_{K,2}\colon \operatorname{Sel}_2(K) \to V_2(K)$.

Putting these together, we define the 2-Selmer signature space as the orthogonal direct sum

$$V(K) := V_\infty(K) \boxplus V_2(K)$$

and write $b := b_\infty \perp b_2$ for the bilinear form on $V(K)$. The isometry group of $(V(K), b)$ is the product of the isometry groups (or equivalently, the subgroup of the total isometry group preserving each factor). Equipped with b, the 2-Selmer signature space $V(K)$ is a nondegenerate symmetric bilinear space over $\mathbb{F}_2$ of dimension $r_1 + n$. Similarly, we define the 2-Selmer signature map

$$\varphi_K := \varphi_{K,\infty} \perp \varphi_{K,2}\colon \operatorname{Sel}_2(K) \to V(K). \tag{2.2.3}$$

Theorem 2.2.4 (Dummit–Voight [16, Theorem 6.1])**.** *For a number field K, the image of the 2-Selmer signature map φ_K is a maximal totally isotropic subspace.*

Recall from the introduction that the class group of K is denoted by $\operatorname{Cl}(K)$, its narrow class group is denoted by $\operatorname{Cl}^+(K)$, and its ray class group of conductor 4 by $\operatorname{Cl}_4(K)$.

Definition 2.2.5. The archimedean isotropy rank of a number field K is

$$k^+(K) := \operatorname{rk}_2 \operatorname{Cl}^+(K) - \operatorname{rk}_2 \operatorname{Cl}(K),$$

and the 2-adic isotropy rank of K is

$$k_4(K) := \operatorname{rk}_2 \operatorname{Cl}_4(K) - \operatorname{rk}_2 \operatorname{Cl}(K).$$

By Dummit–Voight [16, Theorem 6.1], we have

$$k^+(K) = \dim_{\mathbb{F}_2} \operatorname{img}(\varphi_K) \cap V_\infty = \dim_{\mathbb{F}_2} \ker(\varphi_{K,2}) - \dim_{\mathbb{F}_2} \ker(\varphi_K)$$
$$k_4(K) = \dim_{\mathbb{F}_2} \operatorname{img}(\varphi_K) \cap V_2 = \dim_{\mathbb{F}_2} \ker(\varphi_{K,\infty}) - \dim_{\mathbb{F}_2} \ker(\varphi_K)$$

hence the nomenclature given in Definition 2.2.5. Moreover, there is a classical equality

$$k_4(K) = k^+(K) + r_2 \tag{2.2.6}$$

(see for example, Theorem 2.2 of Lemmermeyer [29]).

2.3. **Connections to $\mathrm{Sel}_2(K)$ via class field theory.** There is a natural, well-defined map $\mathrm{Sel}_2(K) \to \mathrm{Cl}(K)[2]$ sending $[\alpha] \mapsto [\mathfrak{a}]$ where $\mathfrak{a}^2 = (\alpha)$; this map is surjective and fits into the exact sequence

$$1 \to \mathcal{O}_K^\times/(\mathcal{O}_K^\times)^2 \to \mathrm{Sel}_2(K) \to \mathrm{Cl}(K)[2] \to 1. \tag{2.3.1}$$

In addition, the 2-Selmer signature map arises naturally in class field theory as follows. Let $H \supseteq K$ be the Hilbert class field of K. Class field theory provides an isomorphism $\mathrm{Gal}(H \,|\, K) \simeq \mathrm{Cl}(K)$; let $H^{(2)}$ denote the fixed field of the subgroup $\mathrm{Cl}(K)^2$. The Kummer pairing

$$\begin{aligned} \mathrm{Gal}(H^{(2)} \,|\, K) \times \ker(\varphi_K) &\to \{\pm 1\} \\ (\tau, [\alpha]) &\mapsto \frac{\tau(\sqrt{\alpha})}{\sqrt{\alpha}} \end{aligned}$$

is (well-defined and) perfect [16, (3.11)]. The Artin reciprocity map provides a canonical isomorphism $\mathrm{Gal}(H^{(2)} \,|\, K) \simeq \mathrm{Cl}(K)/\mathrm{Cl}(K)^2$ and so we can rewrite the above map instead as

$$\mathrm{Cl}(K)/\mathrm{Cl}(K)^2 \times \ker(\varphi_K) \to \{\pm 1\}. \tag{2.3.2}$$

The pairing (2.3.2) is the first of four perfect pairings [16, Lemma 3.10] (see also Lemmermeyer [29, Theorem 6.3]); the other three perfect pairings are

$$\begin{aligned} \mathrm{Cl}_4(K)/\mathrm{Cl}_4(K)^2 \times \ker(\varphi_{K,\infty}) &\to \{\pm 1\}, \\ \mathrm{Cl}^+(K)/\mathrm{Cl}^+(K)^2 \times \ker(\varphi_{K,2}) &\to \{\pm 1\}, \text{ and} \\ \mathrm{Cl}_4^+(K)/\mathrm{Cl}_4^+(K)^2 \times \mathrm{Sel}_2(K) &\to \{\pm 1\}, \end{aligned} \tag{2.3.3}$$

where $\mathrm{Cl}_4^+(K)$ denotes the ray class group of K of conductor $4 \cdot \infty$.

3. Galois module structures

We next study the Galois module structure on the arithmetic objects introduced in the previous section; we will continue in the next section with more precise results in the odd degree case. Our results overlap substantially with those of Taylor [39].

From now on, suppose that K is Galois over $\mathbb{Q}$, with Galois group $G_K := \mathrm{Gal}(K \,|\, \mathbb{Q})$. We work throughout with left $\mathbb{F}_2[G_K]$-modules. (We could consider more generally structures implied by the action of a nontrivial automorphism group $\mathrm{Aut}(K)$, and many of the results below could be generalized to this setting; we focus here on the extreme case, where $\mathrm{Aut}(K)$ is as large as possible.)

3.1. **Basic invariants.** We first prove Galois invariance of the signature spaces in generality. Recall that a $\mathbb{F}_2$-bilinear form $b\colon V \times V \to \mathbb{F}_2$ on an $\mathbb{F}_2[G]$-module V is G-invariant if $b(\alpha,\beta) = b(\sigma(\alpha),\sigma(\beta))$ for all $\sigma \in G$.

Proposition 3.1.1. *The following statements hold.*

(a) *If K is totally real, then $V_\infty(K) \simeq \mathbb{F}_2[G_K]$ as $\mathbb{F}_2[G_K]$-modules; otherwise, $V_\infty(K)$ is trivial. In either case, the bilinear forms b_∞ is G_K-invariant.*

(b) *We have $V_2(K) \simeq \mathbb{F}_2[G_K]$ as $\mathbb{F}_2[G_K]$-modules, and b_2 is G_K-invariant.*

Proof. We begin with (a), and suppose that K is totally real. The Galois group G_K acts on $V_\infty(K)$ (on the left) via its permutation action on the (index) set of real places of K (as $v \mapsto v \circ \sigma^{-1}$), so $V_\infty(K) \simeq \mathbb{F}_2[G_K]$ as $\mathbb{F}_2[G_K]$-modules. Since b_∞ is defined as the product over real places v, it is G_K-invariant.

For (b), we follow the proof in Dummit–Voight [16, Proposition 4.4]. The map $a \mapsto 1+2a$ induces an isomorphism

$$\mathcal{O}_{K,(2)}/2\mathcal{O}_{K,(2)} \xrightarrow{\sim} \left(\mathcal{O}_{K,(2)}^\times/(1+4\mathcal{O}_{K,(2)})\right)[2]$$

which is visibly G_K-equivariant. By Lemma 2.1.1, the right hand side is isomorphic to $V_2(K)$ as $\mathbb{F}_2[G_K]$-modules, since $(1+4\mathcal{O}_{K,(2)})^2 \le 1+8\mathcal{O}_{K,(2)} \le \mathcal{O}_{K,(2)}^{\times 2}$.

Finally, we show b_2 is G_K-invariant. Let $\alpha,\beta \in \mathcal{O}_{K,(2)}^\times$ and let $v \mid 2$ be a prime of K. Since G_K acts transitively (on the left) on the set of places $\{v : v \mid (2)\}$ with stabilizers $D_v := \mathrm{Aut}(K_v)$ the decomposition group, choosing a place v we have

$$b_2(\alpha,\beta) = \prod_{\tau D_v \in G_K/D_v} (\alpha,\beta)_{\tau(v)}$$

well defined. The Hilbert symbol $(\_,\_)_v$ is G_K-equivariant and D_v-invariant, so for $\sigma \in G_K$,

$$b_2(\sigma(\alpha),\sigma(\beta)) = \prod_{\tau D_v \in G_K/D_v} (\sigma(\alpha),\sigma(\beta))_{\tau(v)} = \prod_\tau (\alpha,\beta)_{(\sigma^{-1}\tau)(v)} = \prod_\tau (\alpha,\beta)_{\tau(v)} = b_2(\alpha,\beta)$$

since σ permutes the cosets of D_v in G_K. □

Lemma 3.1.2. *The 2-Selmer signature map φ_K is G_K-equivariant.*

Proof. For sgn_∞, we may suppose that K is totally real, and then

$$\mathrm{sgn}_\infty(\sigma(\alpha)) = (\mathrm{sgn}(v(\sigma(\alpha))))_v = (\mathrm{sgn}((\sigma^{-1}v)(\alpha)))_v = \sigma(\mathrm{sgn}_\infty(\alpha))$$

so sgn_∞ is G_K-equivariant.

To show that sgn_2 is G_K-equivariant, we observe that sgn_2 is simply the composition of a natural embedding and projection, so it suffices to note that any $\sigma \in G_K$ stabilizes $(\mathcal{O}_{K,(2)}^\times)^2(1+4\mathcal{O}_{K,(2)})$. □

Corollary 3.1.3. *For a Galois number field K, the image of the 2-Selmer signature map φ_K is a G_K-invariant maximal totally isotropic subspace.*

Proof. Combine Theorem 2.2.4 with Proposition 3.1.1 and Lemma 3.1.2. □

3.2. **Duals and pairings.** We now treat some issues of duality, with an application to the Kummer pairing. Let G be a finite group and let V be a finitely generated (left) $\mathbb{F}_2[G]$-module.

Definition 3.2.1. The dual of V is the $\mathbb{F}_2$-vector space

$$V^\vee := \mathrm{Hom}_{\mathbb{F}_2}(V, \mathbb{F}_2)$$

equipped with the (left) $\mathbb{F}_2[G]$-action, arising from extending $\mathbb{F}_2$-linearly the natural G-action: if $\sigma \in G$, $f \in V^\vee$, and $x \in V$, then $(\sigma f)(x) := f(\sigma^{-1}x)$. We say V is self-dual if $V \simeq V^\vee$ as $\mathbb{F}_2[G]$-modules.

The canonical evaluation pairing

$$\begin{aligned} e\colon V^\vee \times V &\to \mathbb{F}_2 \\ e(f,x) &= f(x) \end{aligned} \tag{3.2.2}$$

is nondegenerate and G-invariant, so gives a canonical isomorphism $V \xrightarrow{\sim} (V^\vee)^\vee$ as $\mathbb{F}_2[G]$-modules.

Lemma 3.2.3. *For K a Galois number field, the Kummer pairings (2.3.2)–(2.3.3) induce canonical isomorphisms of $\mathbb{F}_2[G_K]$-modules:*

$$\begin{aligned} \mathrm{Cl}(K)/\mathrm{Cl}(K)^2 &\simeq \ker(\varphi_K)^\vee \\ \mathrm{Cl}_4(K)/\mathrm{Cl}_4(K)^2 &\simeq \ker(\varphi_{K,\infty})^\vee \\ \mathrm{Cl}^+(K)/\mathrm{Cl}^+(K)^2 &\simeq \ker(\varphi_{K,2})^\vee \\ \mathrm{Cl}_4^+(K)/\mathrm{Cl}_4^+(K)^2 &\simeq \mathrm{Sel}_2(K)^\vee \end{aligned} \tag{3.2.4}$$

Proof. We work with the first line, the others follow by the same argument. The Kummer isomorphism

$$K^\times/K^{\times 2} \xrightarrow{\sim} \mathrm{Hom}(\mathrm{Gal}(\overline{K}\,|\,K), \{\pm 1\}) \tag{3.2.5}$$

is G_K-equivariant and defines a canonical isomorphism $\ker(\varphi_K) \xrightarrow{\sim} \mathrm{Hom}(\mathrm{Gal}(Q\,|\,F), \{\pm 1\})$, where Q is the maximal subfield of exponent dividing 2 in the Hilbert class field of K. The Artin map defines a canonically G_K-equivariant isomorphism $\mathrm{Gal}(Q\,|\,F) \xrightarrow{\sim} \mathrm{Cl}(K)/\mathrm{Cl}(K)^2$. Combining these with the evaluation map then gives a canonical pairing

$$\mathrm{Cl}(K)/\mathrm{Cl}(K)^2 \times \ker(\varphi_K) \to \{\pm 1\} \tag{3.2.6}$$

as claimed. This pairing may be explicitly described as

$$([\mathfrak{a}], [\alpha]) \mapsto \left(\frac{\alpha}{\mathfrak{a}}\right)$$

where $\mathfrak{a} \subseteq \mathcal{O}_K$ is an ideal of odd norm, $\alpha \in \mathcal{O}_K$ is coprime to $\mathfrak{a}$, and $\left(\frac{\alpha}{\mathfrak{a}}\right)$ is the Jacobi symbol. □

Applying Lemma 2.1.1 to the groups on the left-hand side of (3.2.4) gives (now noncanonical) isomorphisms $\mathrm{Cl}(K)[2] \simeq \ker(\varphi_K)^\vee$, etc.

Lemma 3.2.7. *Let $b\colon V \times V \to \mathbb{F}_2$ be a G-invariant $\mathbb{F}_2$-bilinear form, and let $W, W' \subseteq V$ be irreducible $\mathbb{F}_2[G]$-modules. If $W^\vee \not\simeq W'$ as $\mathbb{F}_2[G]$-modules, then $b(W, W') = \{0\}$.*

Proof. Restricting b, we obtain an $\mathbb{F}_2[G]$-module map $W' \to W^\vee$ by $w' \mapsto b(\_, w')$; by Schur's lemma, this map is either zero or an isomorphism, and the result follows. □

Lemma 3.2.7, although easy to prove, is fundamental in what follows: it shows that when a decomposition of V into irreducibles is possible, it is already *almost* an orthogonal decomposition. We refine this into a canonical orthogonal decomposition in the next section.

To conclude this section, suppose G has *odd* order, so the category of $\mathbb{F}_2[G]$-modules is semisimple. Let W be an irreducible $\mathbb{F}_2[G]$-module. We write V_W for the W-isotypic component of V in a decomposition of V into irreducibles. Suppose that V is equipped with a symmetric, G-invariant, $\mathbb{F}_2$-bilinear form. Then by Lemma 3.2.7, the decomposition into the spaces $V_{\chi^\pm}$ is orthogonal, so we have a canonical decomposition as $\mathbb{F}_2[G]$-modules

$$V \simeq \bigboxplus_W (V_W + V_{W^\vee}), \tag{3.2.8}$$

where the orthogonal direct sum is indexed by irreducibles W up to isomorphism and duals. We call the decomposition given in (3.2.8) the canonical orthogonal decomposition of V.

4. Galois module structures for odd degree extensions

In this section, we suppose throughout that K has *odd* degree (but remains Galois). Then K is totally real and the only roots of unity in K are ± 1. Moreover, since $\#G_K$ is odd, the category of left $\mathbb{F}_2[G_K]$-modules is semisimple.

4.1. Basic invariants.

We quickly prove two standard lemmas, for completeness.

Lemma 4.1.1. *We have $\mathcal{O}_K^\times/(\mathcal{O}_K^\times)^2 \simeq \mathbb{F}_2[G_K]$ as $\mathbb{F}_2[G_K]$-modules.*

Proof. We consider $\mathcal{O}_K^\times$ as a $\mathbb{Z}[G_K]$-module multiplicatively. By Dirichlet's unit theorem,

$$(\mathcal{O}_K^\times/\{\pm 1\} \otimes_{\mathbb{Z}} \mathbb{R}) \oplus \mathbb{R} \simeq \mathbb{R}[G_K]$$

as $\mathbb{R}[G_K]$-modules where $\mathbb{R}$ has trivial G_K action (corresponding to the trace zero hyperplane in the Minkowski embedding). Counting idempotents, we conclude that

$$(\mathcal{O}_K^\times/\{\pm 1\} \otimes_{\mathbb{Z}} \mathbb{Z}_{(2)}) \oplus \mathbb{Z}_{(2)} \simeq \mathbb{Z}_{(2)}[G_K] \tag{4.1.2}$$

as $\mathbb{Z}_{(2)}$-modules; tensoring (4.1.2) with $\mathbb{Z}/2\mathbb{Z}$ and using that $\{\pm 1\}$ has trivial action gives

$$\mathcal{O}_K^\times/(\mathcal{O}_K^\times)^2 \simeq \mathcal{O}_K^\times/\{\pm 1\}(\mathcal{O}_K^\times)^2 \times \{\pm 1\} \simeq \mathbb{F}_2[G_K].$$ □

Corollary 4.1.3. *We have $\mathrm{Sel}_2(K) \simeq \mathbb{F}_2[G_K] \oplus \mathrm{Cl}(K)[2]$ as $\mathbb{F}_2[G_K]$-modules.*

Proof. Since $\mathbb{F}_2[G_K]$ is semisimple, the short exact sequence (2.3.1) splits as $\mathbb{F}_2[G_K]$-modules; the result then follows from Lemma 4.1.1. □

Lemma 4.1.4. *For any odd Galois number field K, the G_K-invariant subspace of each of the $\mathbb{F}_2[G_K]$-modules $\mathrm{Cl}(K)[2]$, $\mathrm{Cl}^+(K)[2]$ and $\mathrm{Cl}_4(K)[2]$ is trivial, whereas the G_K-invariant subspace of $\mathrm{Cl}(K)_4^+(K)$ is isomorphic to $\mathbb{F}_2$.*

Proof. Let $C(K)$ denote one of the groups under consideration, and let $C(\mathbb{Q})$ denote the ray class group of the same modulus but over $\mathbb{Q}$. The norm map induces a group homomorphism $C(K)[2] \to C(\mathbb{Q})[2]$, and on G_K-invariants it is an isomorphism: if $[\mathfrak{a}] \in C(K)[2]$ is G_K-invariant, then $[\mathrm{Nm}(\mathfrak{a})] = [\mathfrak{a}]^n = [\mathfrak{a}]$, since n is odd. Since the groups $\mathrm{Cl}(\mathbb{Q}), \mathrm{Cl}^+(\mathbb{Q}), \mathrm{Cl}_4(\mathbb{Q})$ are trivial and $\mathrm{Cl}_4^+(\mathbb{Q}) \simeq \mathbb{Z}/2\mathbb{Z}$, the result follows. □

4.2. **First reflection principle.** In this section, we show that the Galois module structure of the 2-Selmer group and Kummer duality imply rank inequalities on the class group, classically known as a *reflection theorem*. Let W be an irreducible (left) $\mathbb{F}_2[G_K]$-module, and for a finitely generated $\mathbb{Z}[G_K]$-module M, let $\mathrm{rk}_W(M) \in \mathbb{Z}_{\geq 0}$ be the multiplicity of W in a decomposition of $M/2M$ into irreducible $\mathbb{F}_2[G_K]$-modules. We recall Lemma 2.1.1, which gives an isomorphism $M/2M \simeq M[2]$ for a torsion, finitely generated $\mathbb{Z}_{(2)}$-module M, in particular giving $\mathrm{rk}_W(M) = \mathrm{rk}_W(M[2])$.

As mentioned in the introduction, our reflection theorems (Proposition 4.2.2, Proposition 4.3.3, and Theorem 4.4.1) are special cases of the very general T-S-reflection theorem of Gras [23, Théorème 5.18]. Our goal in the next few sections is to give a direct proof of these results: it shows that they can be read off from the 2-Selmer group. In particular, they do not enter into our model (rather, the below shows that our model refines them).

We use the notation

$$\begin{aligned} \rho_W(K) &:= \mathrm{rk}_W \mathrm{Cl}(K) \\ \rho_W^+(K) &:= \mathrm{rk}_W \mathrm{Cl}^+(K) \\ \rho_{4,W}(K) &:= \mathrm{rk}_W \mathrm{Cl}_4(K). \end{aligned} \tag{4.2.1}$$

Proposition 4.2.2. *Let K be a Galois number field of odd degree, and let W be an irreducible $\mathbb{F}_2[G_K]$-module. Then*

$$|\rho_W(K) - \rho_{W^\vee}(K)| \leq \mathrm{rk}_W \mathbb{F}_2[G_K]. \tag{4.2.3}$$

Proof. Since the short exact sequence in (2.3.1) splits as a sequence of $\mathbb{F}_2[G_K]$-modules, decomposing $\mathrm{Sel}_2(K)$ under φ_K gives

$$\mathcal{O}_K^\times/(\mathcal{O}_K^\times)^2 \oplus \mathrm{Cl}(K)[2] \simeq \mathrm{Sel}_2(K) \simeq S(K) \oplus \ker(\varphi_K) \tag{4.2.4}$$

as $\mathbb{F}_2[G_K]$-modules. By Lemma 4.1.1, we have $\mathcal{O}_K^\times/(\mathcal{O}_K^\times)^2 \simeq \mathbb{F}_2[G_K]$. By Lemma 3.2.3, we have $\mathrm{Cl}(K)[2] \simeq \ker(\varphi_K)^\vee$, so $\rho_W(K) = \mathrm{rk}_{W^\vee} \ker(\varphi_K)$. Write $m(W) := \mathrm{rk}_W \mathbb{Z}_{(2)}[G_K]$; then $m(W) = m(W^\vee)$. Plugging these in and taking $\mathrm{rk}_{W^\vee}$ in (4.2.4) yields

$$m(W) + \rho_{W^\vee}(K) = \mathrm{rk}_{W^\vee} S(K) + \rho_W(K) \tag{4.2.5}$$

so

$$\rho_W(K) - \rho_{W^\vee}(K) = m(W) - \mathrm{rk}_{W^\vee} S(K) \leq m(W). \tag{4.2.6}$$

Repeating the argument with $W^\vee$ and negating then gives (4.2.3). □

In particular, we see from the proof of Proposition 4.2.2 that the inequality is refined by the equality 4.2.6, with the discrepancy in the inequality being measured by the group $S(K)$. This is the simplest instance of the motivation of our paper: we seek to understand structural properties of the 2-Selmer signature map, from which reflection principles are corollaries.

4.3. **Isotropy ranks.** Similar inequalities govern the narrow class group and its relationship to the class group, encoded in the 2-Selmer group. To measure these contributions, we make the following definitions. Throughout, let W be an irreducible $\mathbb{F}_2[G_K]$-module.

Definition 4.3.1. The archimedean W-isotropy rank of K is

$$k_W^+(K) := \operatorname{rk}_W \operatorname{Cl}^+(K) - \operatorname{rk}_W \operatorname{Cl}(K)$$

and the 2-adic W-isotropy rank of K is

$$k_{4,W}(K) := \operatorname{rk}_W \operatorname{Cl}_4(K) - \operatorname{rk}_W \operatorname{Cl}(K).$$

We have $k_W^+(K), k_{4,W}(K) \in \mathbb{Z}_{\geq 0}$, since $\operatorname{Cl}^+(K), \operatorname{Cl}_4(K)$ surject onto $\operatorname{Cl}(K)$.

Lemma 4.3.2. *We have*

$$\begin{aligned} k_W^+(K) &= \operatorname{rk}_{W^\vee}(S(K) \cap V_\infty(K)), \text{ and} \\ k_{4,W}(K) &= \operatorname{rk}_{W^\vee}(S(K) \cap V_2(K)). \end{aligned}$$

Proof. We have that $S(K) \cap V_\infty(K) \simeq \ker(\varphi_{K,2})/\ker(\varphi_K)$; since $\ker(\varphi_{K,2})$ and $\ker(\varphi_K)$ are *Kummer dual* to $\operatorname{Cl}^+(K)[2]$ and $\operatorname{Cl}(K)[2]$ by Lemma 3.2.3, we have

$$\operatorname{rk}_{W^\vee}(S(K) \cap V_\infty(K)) = \operatorname{rk}_W \operatorname{Cl}^+(K) - \operatorname{rk}_W \operatorname{Cl}(K).$$

The second equality follows similarly. □

With this notation, we immediately turn to our next reflection principle: again, all we use is $\mathbb{F}_2[G_K]$-module structure and Kummer duality.

Proposition 4.3.3. *Let W be an irreducible $\mathbb{F}_2[G_K]$-module. Then*

$$\begin{aligned} |\rho_W^+(K) - \rho_{W^\vee}^+(K)| &\leq \operatorname{rk}_W \mathbb{F}_2[G_K], \text{ and} \\ |\rho_{4,W}(K) - \rho_{4,W^\vee}(K)| &\leq \operatorname{rk}_W \mathbb{F}_2[G_K]. \end{aligned} \tag{4.3.4}$$

Proof. As K is fixed, we drop it from the notation. We may decompose

$$S \simeq (S \cap V_\infty) \oplus (S \cap V_2) \oplus S'$$

as $\mathbb{F}_2[G_K]$-modules (for some choice $S' \subseteq S$). By Lemma 4.3.2, we obtain

$$\operatorname{rk}_{W^\vee} S = k_W^+ + k_{4,W} + \operatorname{rk}_{W^\vee} S'. \tag{4.3.5}$$

From (4.2.5) we get

$$\operatorname{rk}_{W^\vee} S = m(W) + \rho_{W^\vee} - \rho_W$$

with $m(W) = \operatorname{rk}_W \mathbb{Z}_{(2)}[G_K]$, so plugging and rearranging gives

$$\begin{aligned} \rho_W^+ = k_W^+ + \rho_W &= m(W) + \rho_{W^\vee} - k_{4,W} - \operatorname{rk}_{W^\vee} S' \\ \rho_W^+ - \rho_{W^\vee}^+ &= m(W) - k_{W^\vee}^+ - k_{4,W} - \operatorname{rk}_{W^\vee} S' \leq m(W). \end{aligned} \tag{4.3.6}$$

Repeating with W replaced by $W^\vee$ gives the first inequality in (4.3.4); a similar argument gives the other. □

4.4. **Further duality.** A further duality is reflect in the totally positive elements in the 2-Selmer group, as follows.

Theorem 4.4.1. *Let K be a Galois number field of odd degree. Then*

$$\mathrm{Cl}^+(K)[2] \simeq \mathrm{Cl}_4(K)[2]^\vee$$

as $\mathbb{F}_2[G_K]$-modules.

Proof. Let $\mathrm{Sel}_2^+(K) := \ker(\varphi_{K,\infty})$ be the classes in the 2-Selmer group represented by a totally positive element; then $\mathrm{Sel}_2^+(K) \simeq \mathrm{Cl}_4(K)[2]^\vee$ by Lemma 3.2.3; we show $\mathrm{Sel}_2^+(K) \simeq \mathrm{Cl}^+(K)[2]$ as $\mathbb{F}_2[G_K]$-modules.

Our proof considers the analogue for $\mathrm{Sel}_2^+(K)$ of the exact sequence (2.3.1). Let P_K be the group of principal fractional ideals of K, and let $P_{K,>0}$ be the subgroup of P_K consisting of principal fractional ideals generated by a totally positive element. The map $K^\times \to P_K$ sending $\alpha \mapsto (\alpha)$ is surjective and G_K-equivariant with kernel $\mathcal{O}_K^\times$; it induces the exact sequence

$$1 \to \mathcal{O}_K^\times/\mathcal{O}_{K,>0}^\times \to K^\times/K_{>0}^\times \to P_K/P_{K,>0} \to 1.$$

By weak approximation, the natural map $K^\times/K_{>0}^\times \to V_\infty(K)$ is a G_K-equivariant isomorphism, and so $K^\times/K_{>0}^\times \simeq \mathbb{F}_2[G_K]$ by Proposition 3.1.1(a). Therefore we obtain a canonical isomorphism of $\mathbb{F}_2[G_K]$-modules

$$\mathbb{F}_2[G_K] \simeq (\mathcal{O}_K^\times/\mathcal{O}_{K,>0}^\times) \oplus (P_K/P_{K,>0}). \tag{4.4.2}$$

The natural G_K-equivariant map $P_K \to \mathrm{Cl}^+(K)$ defined by $(\alpha) \mapsto [(\alpha)]$ has kernel $P_{K,>0}$ and so we have a canonical injection $P_K/P_{K,>0} \hookrightarrow \mathrm{Cl}^+(K)$. Since P_K^2 is a subgroup of $P_{K,>0}$ the image of the injection is contained in $\mathrm{Cl}^+(K)[2]$. Therefore, the map

$$\mathrm{Sel}_2^+(K) \to \mathrm{Cl}^+(K)[2]/(P_K/P_{K,>0})$$

mapping the class of $\alpha \in K^\times$ to the class of the fractional ideal $\mathfrak{a}$ such that $\mathfrak{a}^2 = (\alpha)$ is well-defined; it is also visibly surjective, and so fits into the short exact sequence

$$1 \to \mathcal{O}_{K,>0}^\times/\mathcal{O}_K^{\times 2} \to \mathrm{Sel}_2^+(K) \to \mathrm{Cl}^+(K)[2]/(P_K/P_{K,>0}) \to 1$$

of $\mathbb{F}_2[G_K]$-modules, giving the isomorphism

$$P_K/P_{K,>0} \oplus \mathrm{Sel}_2^+(K) \simeq \mathcal{O}_{K,>0}^\times/\mathcal{O}_K^{\times 2} \oplus \mathrm{Cl}^+(K)[2]. \tag{4.4.3}$$

Adding $\mathcal{O}_K^\times/\mathcal{O}_{K,>0}^\times$ to both sides of (4.4.3), and using (4.4.2) and Lemma 4.1.1 we conclude

$$\mathbb{F}_2[G_K] \oplus \mathrm{Sel}_2^+(K) \simeq \mathbb{F}_2[G_K] \oplus \mathrm{Cl}^+(K)[2]$$

and cancelling gives the result. □

Proposition 4.4.4. *We have*

$$0 \le k_W^+ + k_{W^\vee}^+ = k_{4,W} + k_{4,W^\vee} \le m(W). \tag{4.4.5}$$

Proof. For the middle equality, by Theorem 4.4.1, we have

$$\rho_W^+ + \rho_{W^\vee}^+ = \rho_{4,W} + \rho_{4,W^\vee};$$

subtracting $\rho_W + \rho_{W^\vee}$ from both sides gives the result. For the right-most inequality, from (4.3.6) we have

$$k_W^+ + k_{4,W} + \rho_W - \rho_{W^\vee} = m(W) - \mathrm{rk}_{W^\vee} S'$$

But $k_{4,W} + \rho_W = \rho_{4,W} = \rho_{W^\vee}^+$ by Theorem 4.4.1, so

$$k_W^+ + k_{W^\vee}^+ = m(W) - \mathrm{rk}_{W^\vee} S' \leq m(W). \tag{4.4.6}$$

To restore symmetry, we repeat the same argument with $W^\vee$ and conclude that $\mathrm{rk}_W S' = \mathrm{rk}_{W^\vee} S'$, so in fact S' is self-dual. □

Just as in Proposition 4.2.2, we see from the proof of Proposition (4.4.4) that the real content lies in the equality (4.4.6), i.e., the discrepancy in the upper bound (4.4.5) is measured by the (noncanonically defined) "diagonal subspace" $S'(K) \subseteq S(K)$.

We deduce corollaries of these statements in the abelian case in section 5.4.

5. Galois module structures for odd abelian extensions

In this section, we specialize further and suppose that the odd-order group G is *abelian* and prove the main structural results of the paper, first for class groups and then for unit signatures.

5.1. **Duality in the abelian case.** We begin by revising notation and duality in the abelian setting. Let $\overline{\mathbb{F}}_2$ be a (fixed) algebraic closure of $\mathbb{F}_2$. A $\overline{\mathbb{F}}_2$-character of G is a group homomorphism $\chi\colon G \to \overline{\mathbb{F}}_2^\times$. For an $\overline{\mathbb{F}}_2$-character χ, let $\mathbb{F}_2(\chi) \subseteq \overline{\mathbb{F}}_2$ be the subfield generated by the values of χ. Then $\mathbb{F}_2(\chi)$ is a finite extension of $\mathbb{F}_2$: more precisely, if χ has (odd) order d and 2 has order f in $(\mathbb{Z}/d\mathbb{Z})^\times$, then $\mathbb{F}_2(\chi) \simeq \mathbb{F}_{2^f}$ as $\mathbb{F}_2$-vector spaces. The group G acts naturally on $\mathbb{F}_2(\chi)$ via multiplication by $\chi(\sigma)$; thus $\mathbb{F}_2(\chi)$ is a cyclic, irreducible $\mathbb{F}_2[G]$-module, generated by 1. Conversely, choosing a cyclic generator, every irreducible $\mathbb{F}_2[G]$-module is of the form $\mathbb{F}_2(\chi)$ for some $\overline{\mathbb{F}}_2$-character χ.

By character theory, two such modules $\mathbb{F}_2(\chi)$ and $\mathbb{F}_2(\chi')$ are isomorphic if and only if there exists $\psi \in \mathrm{Gal}(\overline{\mathbb{F}}_2 \,|\, \mathbb{F}_2)$ such that $\chi' = \psi \circ \chi$. In particular, since ψ is a power of the Frobenius automorphism, $\mathbb{F}_2(\chi) \simeq \mathbb{F}_2(\chi')$ if and only if $\chi' = \chi^{2^k}$ for some $k \in \mathbb{Z}$. Moreover, $\mathrm{Aut}_{\mathbb{F}_2[G]}(\mathbb{F}_2(\chi)) \simeq \mathbb{F}_2(\chi)^\times$.

There is also a simple way to understand duality when G is abelian. Let V be a finitely generated $\mathbb{F}_2[G]$-module. The map $\sigma \mapsto \sigma^{-1}$ for $\sigma \in G$ extends by $\mathbb{F}_2$-linearity to an involution $^*\colon \mathbb{F}_2[G] \to \mathbb{F}_2[G]$. We define V^* to be the $\mathbb{F}_2[G]$-module with the same underlying $\mathbb{F}_2$-vector space V but with the action of $\mathbb{F}_2[G]$ under pullback from the involution map. Explicitly, if $\gamma \in \mathbb{F}_2[G]$ and $x^* \in V^*$ denotes the same element $x \in V$ then $\gamma(x^*) := \gamma^*(x)^*$; in particular, for $\sigma \in G$, then $\sigma(x^*) = \sigma^*(x)^* = \sigma^{-1}(x)^*$. We conclude that

$$\mathbb{F}_2(\chi)^* \simeq \mathbb{F}_2(\chi^{-1}),$$

which explains the notation $\chi^* = \chi^{-1}$ from the introduction.

Remark 5.1.1. Without the hypothesis that G is abelian, starting with a left $\mathbb{F}_2[G]$-module V, we would obtain a *right* $\mathbb{F}_2[G]$-module V^*.

Lemma 5.1.2. *There is a (non-canonical) $\mathbb{F}_2[G]$-module isomorphism $V^* \xrightarrow{\sim} V^\vee$.*

Proof. Decomposing into irreducibles up to isomorphism, we may suppose without loss of generality that $V = \mathbb{F}_2(\chi)$. Consider the map

$$\begin{aligned} V^* &\to V^\vee \\ x^* &\mapsto (\mathrm{Tr}(x \cdot \_) : V \to \mathbb{F}_2) \end{aligned}$$

where $\mathrm{Tr}\colon \mathbb{F}_2(\chi) \to \mathbb{F}_2$ is the trace map. This map is nonzero and $\mathbb{F}_2$-linear, and it is also G-equivariant because for any $y \in V$,

$$\mathrm{Tr}(\sigma^*(x) \cdot y) = \mathrm{Tr}(\sigma^{-1}(x) \cdot y) = (\sigma \,\mathrm{Tr})(x \cdot y)$$

for $\sigma \in G$ and $x, y \in V$; hence, it is an isomorphism by Schur's lemma. □

Lemma 5.1.3. *Let $m \in \mathbb{Z}_{\geq 1}$ denote the (odd) exponent of the abelian group G. Every irreducible $\mathbb{F}_2[G]$-module is self-dual if and only if there exists $t \in \mathbb{Z}$ such that $2^t \equiv -1 \pmod{m}$, where m is the exponent of G.*

Proof. Let $\mathbb{F}_2(\chi)$ be an irreducible $\mathbb{F}_2[G]$-module, and let d be the order of χ. We have $\mathbb{F}_2(\chi) \simeq \mathbb{F}_2(\chi)^* = \mathbb{F}_2(\chi^*)$ if and only if $\chi^* = \chi^{2^k}$ for some $k \in \mathbb{Z}$, i.e., $2^k \equiv -1 \pmod{d}$. Choosing a character with order $d = m$ then gives the result. □

Example 5.1.4. The smallest (odd) values of $m \in \mathbb{Z}_{>0}$ where $-1 \notin \langle 2 \rangle \leq (\mathbb{Z}/m\mathbb{Z})^\times$ are $m = 7$, 15, 21, and 23.

Example 5.1.5. Suppose $\#G = \ell$ is prime and let f be the order of 2 in $(\mathbb{Z}/\ell\mathbb{Z})^\times$. Then there are $\frac{\ell-1}{f}$ distinct, nontrivial $\mathbb{F}_2[G]$-modules, up to isomorphism. They are all isomorphic as $\mathbb{F}_2$-vector spaces to $\mathbb{F}_{2^f}$, a generator of G acts by a primitive ℓth root of unity $\zeta \in \mathbb{F}_{2^f}$, and two such are isomorphic if and only if $\zeta' = \zeta^{2^k}$ for some $k \in \mathbb{Z}$. Finally, all such modules are self-dual if and only if f is even.

The Galois module structure has concrete implications for ranks.

Example 5.1.6. If K be a cyclic number field of odd prime degree ℓ, and let f denote the order of 2 modulo ℓ. Then taking $G = G_K$, applying the decomposition into irreducibles given in Example 5.1.5 and Lemma 4.1.4, we conclude that f divides each of $\mathrm{rk}_2 \mathrm{Cl}(K)$, $\mathrm{rk}_2 \mathrm{Cl}^+(K)$, and $\mathrm{rk}_2 \mathrm{Cl}_4(K)$.

5.2. **Bilinear forms.** For an $\overline{\mathbb{F}}_2$-character χ of G, we write V_χ for the $\mathbb{F}_2(\chi)$-isotypic component of V and $V_{\chi^\pm} := V_\chi + V_{\chi^{-1}} = V_\chi + V_{\chi^*}$ for the sum of the $\mathbb{F}_2(\chi)$- and $\mathbb{F}_2(\chi^*)$-isotypic components of V. (If χ is not self-dual, then this sum is direct; if χ is self-dual, then $V_{\chi^\pm} = V_\chi$.)

Example 5.2.1. Since G is abelian, each isomorphism class of irreducible $\mathbb{F}_2[G]$-modules occurs in $\mathbb{F}_2[G]$ with multiplicity 1. Therefore

$$\mathbb{F}_2[G]_{\chi^\pm} \simeq \begin{cases} \mathbb{F}_2(\chi), & \text{if } \chi \text{ is self-dual;} \\ \mathbb{F}_2(\chi) \oplus \mathbb{F}_2(\chi^*), & \text{otherwise.} \end{cases}$$

If V is equipped with a symmetric, G-invariant, $\mathbb{F}_2$-bilinear form, then V has a canonical orthogonal decomposition (3.2.8)

$$V \simeq \boxplus_{\chi} V_{\chi^{\pm}}, \tag{5.2.2}$$

where the orthogonal direct sum is indexed by characters χ taken up to isomorphism and inverses. Consequently, it is enough to understand bilinear forms on the components $V_{\chi^{\pm}}$. We use this technique to prove the following fundamental classification result.

Theorem 5.2.3. *Let G be an abelian group of odd order. Then there is a unique G-invariant, symmetric, nondegenerate, $\mathbb{F}_2$-bilinear form on $\mathbb{F}_2[G]$ up to G-equivariant isometry, given by*

$$\begin{aligned} b\colon \mathbb{F}_2[G] \times \mathbb{F}_2[G] &\to \mathbb{F}_2 \\ (x, y) &\mapsto \mathrm{Tr}(x^* y). \end{aligned} \tag{5.2.4}$$

Proof. Recalling that $\mathbb{F}_2[G]$ is commutative, we see that the trace pairing is symmetric because

$$b(y, x) = \mathrm{Tr}(y^* x) = \mathrm{Tr}((x^* y)^*) = \mathrm{Tr}(x^* y) = b(x, y),$$

nondegenerate because $\mathbb{F}_2[G]$ is (absolutely) semisimple, and G-invariant because

$$b(\sigma x, \sigma y) = \mathrm{Tr}((\sigma x)^* \sigma y) = \mathrm{Tr}(\sigma^{-1}(x^*)\sigma y) = \mathrm{Tr}(x^* y) = b(x, y)$$

for all $\sigma \in G$. Note * is the adjoint with respect to b, since

$$b(\nu x, y) = \mathrm{Tr}((\nu x)^* y) = \mathrm{Tr}(\nu^* x^* y) = \mathrm{Tr}(x^*(\nu^* y)) = b(x, \nu^* y). \tag{5.2.5}$$

To show every such form arises as claimed, by the orthogonal decomposition (3.2.8) we reduce to showing uniqueness on each $\mathbb{F}_2[G]_{\chi^{\pm}}$. We have two cases. First, suppose χ is self-dual; two such pairings differ by an $\mathbb{F}_2[G]$-module automorphism of $\mathbb{F}_2(\chi)$, given by multiplication by an element $\nu \in \mathbb{F}_2(\chi)^\times$, so any other such form b' is given by $b'(x, y) := b(\nu x, y)$. We showed b is symmetric above, and b' is symmetric by hypothesis; thus, using (5.2.5),

$$b(x, \nu y) = b(\nu y, x) = b'(y, x) = b'(x, y) = b(\nu x, y) = b(x, \nu^* y)$$

for all $x, y \in \mathbb{F}_2[G]$; by nondegeneracy, we have $\nu = \nu^*$. The fixed field of the involution * is a subfield of index 2 and the norm map from $\mathbb{F}_2(\chi)$ surjects onto this field, so there exists $\eta \in \mathbb{F}_2(\chi)$ such that $\nu = \eta^* \eta$. Therefore

$$b'(x, y) = b(\nu x, y) = b(\eta^* \eta x, y) = b(\eta x, (\eta^*)^* y) = b(x, y).$$

To conclude, suppose instead that χ is not self-dual. Still, by Schur's lemma, two such pairings differ by a pair of $\mathbb{F}_2[G]$-module automorphisms, one for $\mathbb{F}_2(\chi)$ and one for $\mathbb{F}_2(\chi^*)$ and in each case given by multiplication by a nonzero element. Using the fact that $\mathbb{F}_2[G]$ surjects onto $\mathbb{F}_2(\chi) \oplus \mathbb{F}_2(\chi^*)$, we may repeat the argument in the previous paragraph and reach the same conclusion. □

Remark 5.2.6. Taking the standard basis $g \in G$ for $\mathbb{F}_2[G]$, we compute on this basis that the form in Theorem 5.2.3 is the standard 'dot product', so is again clearly seen to have the properties listed.

Example 5.2.7. As this will be central to our investigation, we write down explicitly the pairing in Theorem 5.2.3 restricted to orthogonal components as in (3.2.8).

If χ is self-dual, then $\mathbb{F}_2[G]_{\chi^\pm} \simeq \mathbb{F}_2(\chi) \simeq \mathbb{F}_{2^f}$ and the bilinear form is alternating when χ is trivial and non-alternating when χ is non-trivial. When χ is trivial then $\mathbb{F}_2(\chi) = \mathbb{F}_2$ and $b(1,1) = \mathrm{Tr}(1) = 1$ so the form is non-alternating. Now suppose that χ has order $d > 1$ and let $\zeta \in \mathbb{F}_2(\chi)$ be a primitive dth root of unity. Then an $\mathbb{F}_2$-basis for $\mathbb{F}_2(\chi)$ is given by $\zeta, \zeta^2, \cdots, \zeta^{2^{f-1}}$ where f is the order of 2 in $(\mathbb{Z}/d\mathbb{Z})^\times$. Since $\mathrm{Tr}(1) = 0$ (as f is even), we have $b(\zeta^{2^k}, \zeta^{2^k}) = \mathrm{Tr}(1) = 0$ for all k, so by linearity we conclude that b is alternating. (We also observe $\mathrm{Tr}(\zeta) = \mathrm{Tr}(\zeta^{2^k}) = 1$ so $b(1, \zeta^{2^k}) = 1$ for all k.)

If χ is not self-dual, then $\mathbb{F}_2[G]_{\chi^\pm} \simeq \mathbb{F}_2(\chi) \oplus \mathbb{F}_2(\chi^*) \simeq (\mathbb{F}_{2^f})^2$ and the bilinear form is a sum of hyperbolic planes, pairing dual basis elements nontrivially. Put another way, the canonical pairing (3.2.2) induces a natural pairing on $\mathbb{F}_2(\chi)^\vee \oplus \mathbb{F}_2(\chi)$, which can be described explicitly as

$$b((f,x),(g,y)) = f(y) + g(x).$$

5.3. **Maximal totally isotropic subspaces.** In this section, we will classify the maximal isotropic subspaces of $\mathbb{F}_2[G] \boxplus \mathbb{F}_2[G]$ and study their isometry groups.

We continue our hypothesis that G is a finite abelian group of odd order. Let V be a finitely generated $\mathbb{F}_2[G]$-module equipped with a G-invariant, symmetric, $\mathbb{F}_2$-bilinear form. We let $\mathrm{Isom}_G(V) \leq \mathrm{Aut}_G(V)$ be the group of G-equivariant isometries of V, i.e., the set of $\mathbb{F}_2[G]$-module automorphisms of V which preserve the bilinear form.

Lemma 5.3.1. *Equip $\mathbb{F}_2[G]$ with the trace bilinear form b (5.2.4), and let χ be an $\overline{\mathbb{F}}_2$-character of G. Then*

$$\#\,\mathrm{Isom}_G(\mathbb{F}_2[G]_{\chi^\pm}) = \begin{cases} \sqrt{q}+1, & \text{if } \chi \text{ is self-dual;} \\ q-1, & \text{otherwise.} \end{cases}$$

Proof. First, suppose χ is self-dual, so $\mathbb{F}_2[G]_{\chi^\pm} \simeq \mathbb{F}_2(\chi)$. As in the proof of Theorem 5.2.3, the group $\mathrm{Aut}_G(V)$ of $\mathbb{F}_2[G]$-module automorphisms of $\mathbb{F}_2(\chi)$ are given by multiplication by an element $\nu \in \mathbb{F}_2(\chi)^\times$. The subgroup $\mathrm{Isom}_G(V) \leq \mathrm{Aut}_G(V)$ of isometries are those for which

$$b(x,y) = b(\nu x, \nu y) = b(x, \nu\nu^* y) \tag{5.3.2}$$

for all $x, y \in \mathbb{F}_2(\chi)$; since b is nondegenerate, this is equivalent to $\nu\nu^* = 1$. The map $\nu \mapsto \nu\nu^*$ is the norm to the unique subfield of $\mathbb{F}_2(\chi)$ of index 2; since the norm is surjective, we conclude that $\mathrm{Isom}_G(\mathbb{F}_2(\chi))$ is a cyclic group of cardinality $(q-1)/(\sqrt{q}-1) = \sqrt{q}+1$.

Second, suppose χ is not self-dual, and write $V := \mathbb{F}_2[G]_{\chi^\pm} = \mathbb{F}_2(\chi) \oplus \mathbb{F}_2(\chi^*)$. Then * acts on V by $(x,y)^* = (y^*, x^*)$. The group $\mathrm{Aut}_G(V)$ is given by coordinate-wise multiplication by $(\mu,\nu) \in \mathbb{F}_2(\chi)^\times \times \mathbb{F}_2(\chi^*)^\times$. Such an automorphism is an isometry if and only if

$$\begin{aligned} b((x_1,x_2),(y_1,y_2)) &= b((\nu x_1, \mu x_2),(\nu y_1, \mu y_2)) = b((x_1,x_2),(\nu\mu^* y_1, \mu\nu^* y_2)) \\ &= b((x_1,x_2),(\nu\mu^* y_1, (\nu\mu^*)^* y_2)) \end{aligned} \tag{5.3.3}$$

for all $(x_1,x_2),(y_1,y_2) \in \mathbb{F}_2(\chi) \times \mathbb{F}_2(\chi^*)$. The same nondegeneracy argument in the previous paragraph shows this is equivalent to $\nu\mu^* = 1 \in \mathbb{F}_2(\chi)^\times$ (equivalently, $\mu\nu^* = 1 \in \mathbb{F}_2(\chi^*)^\times$).

We conclude that $\mathrm{Isom}_G(V) \leq \mathrm{Aut}_G(V)$ consists of the elements $(\nu, (\nu^{-1})^*)$ with $\nu \in \mathbb{F}_2(\chi)^\times$, a cyclic group of cardinality $q-1$. □

A maximal totally isotropic subspace $S \subseteq V \boxplus V$ is said to be projection-free if each coordinate projection is $\{0\}$.

Lemma 5.3.4. *Suppose the bilinear form on V is nondegenerate. Then all G-invariant maximal totally isotropic projection-free subspaces are in the same G-equivariant isometry class, and there are exactly $\#\,\mathrm{Isom}_G(V)$ of them.*

Proof. See Dummit–Voight [16, Lemma A.9] for a proof in the case of $\mathbb{F}_2$-vector spaces; the method of proof gives the same result for $\mathbb{F}_2[G]$-modules. □

In our main classification in section 4.3, we will need to classify Galois invariant maximal totally subspaces in the setting of the following theorem.

Theorem 5.3.5. *Let G be an abelian group of odd order, and let χ be an $\overline{\mathbb{F}}_2$-character of G with $q := \#\mathbb{F}_q(\chi)$. Let $V := V_1 \boxplus V_2$ with each $V_i := \mathbb{F}_2[G]_{\chi^\pm}$ equipped with the restriction of the bilinear form (5.2.4) for $i = 1, 2$.*

Then the possible G-invariant, maximal totally isotropic subspaces $S \subseteq V$ are described in Table 5.3.6, each row representing a different G-equivariant isometry class.

		$\mathbb{F}_2[G_K]$-module structure		
Case	$\chi = \chi^*$?	$S_{\chi^\pm}$	$S_{\chi^\pm} \cap V_\infty$	Mass
A	Yes	$\mathbb{F}_2(\chi)$	$\mathbb{F}_2(\chi)$	$\sqrt{q}+1$
B	No	$\mathbb{F}_2(\chi)^2$	$\mathbb{F}_2(\chi)$	1
B′	No	$\mathbb{F}_2(\chi^*)^2$	$\mathbb{F}_2(\chi^*)$	1
C	No	$\mathbb{F}_2(\chi) \oplus \mathbb{F}_2(\chi^*)$	$\mathbb{F}_2(\chi)$	1
C′	No	$\mathbb{F}_2(\chi) \oplus \mathbb{F}_2(\chi^*)$	$\mathbb{F}_2(\chi^*)$	1
D	No	$\mathbb{F}_2(\chi) \oplus \mathbb{F}_2(\chi^*)$	$\{0\}$	$q-1$

Table 5.3.6: Possibilities for maximal totally isotropic subspaces

Proof. First, suppose χ is self-dual. Then up to G-equivariant isometry, we have $V_i \simeq \mathbb{F}_2(\chi)$ for $i = 1, 2$ with the (restriction of the) trace bilinear form (5.2.4) (see also Example 5.2.7). A subspace is G-invariant if and only if it is an $\mathbb{F}_2(\chi)$-subspace; so by dimensions, a maximal isotropic subspace S is generated by the $\mathbb{F}_2(\chi)$-span of a single vector. We cannot have $S = V_{1,\chi}$ or $S = V_{2,\chi}$, since each $b_{i,\chi}$ is nondegenerate. We finish with Lemma 5.3.1 and Lemma 5.3.4. Alternatively, each subspace is spanned by a unique vector $(1, \nu)$ with $\nu \in \mathbb{F}_2(\chi)^\times$, and one can verify directly that the $\mathbb{F}_2(\chi)$-span is totally isotropic if and only if $\nu\nu^* = 1$, consistent with the calculation in (5.3.2). This covers case A.

So now suppose χ is not self-dual. Now $V_i \simeq \mathbb{F}_2(\chi) \oplus \mathbb{F}_2(\chi^*)$ for $i = 1, 2$, still with the trace bilinear form b. Let $S \subseteq V_{\chi^\pm}$ be a G-invariant, maximal totally isotropic subspace. Since S has half of the $\mathbb{F}_2$-dimension of the bilinear space, as an $\mathbb{F}_2[G]$-module the possibilities for S are $\mathbb{F}_2(\chi)^2$, $\mathbb{F}_2(\chi^*)^2$, or $\mathbb{F}_2(\chi) \oplus \mathbb{F}_2(\chi^*)$. If $S \simeq \mathbb{F}_2(\chi)^2$, then $S = V_{1,\chi} \boxplus V_{2,\chi}$ which is totally

isotropic since the restriction b_χ of b to V_χ is identically zero by Lemma 3.2.7. Similarly for $S \simeq \mathbb{F}_2(\chi^*)^2$; this handles cases B and B'.

We now consider the possibilities for $S \simeq \mathbb{F}_2(\chi) \oplus \mathbb{F}_2(\chi^*)$. We have $S = S_\chi \oplus S_{\chi^*}$ where

$$\begin{aligned} S_\chi &:= \mathbb{F}_2(\chi)(x_1, x_2) \subseteq V_\chi, \\ S_{\chi^*} &:= \mathbb{F}_2(\chi^*)(y_1, y_2) \subseteq V_{\chi^*}, \end{aligned} \tag{5.3.7}$$

and $(x_1, x_2), (y_1, y_2)$ are both nonzero. Suppose that $x_1 = 0$. Then

$$b((0, x_2), (y_1, y_2)) = b_1(0, y_1) + b_2(x_2, y_2) = b_2(x_2, y_2); \tag{5.3.8}$$

the nondegeneracy of $b_{2,\chi}$ on $V_{2,\chi^\pm}$ then implies that $y_2 = 0$, and $S = V_{1,\chi^*} \boxplus V_{2,\chi}$. Indeed, S is isotropic since the restriction $b_{i,\chi}$ of b_i to $V_{i,\chi}$ for $i = 1, 2$ is identically zero by Lemma 3.2.7. Similar conclusions hold when $x_2 = 0$, giving cases C and C'. Finally, if x_1, x_2, y_1, y_2 are all nonzero, then $S \cap V_1 = S \cap V_2 = \{0\}$; by Lemma 5.3.1 and Lemma 5.3.4, the number of subspaces of this form is $q-1$ and each subspace is in the same G-equivariant isometry class. Alternatively, a calculation like (5.3.3) shows that S is uniquely determined by the spans of $(x_1, x_2) = (1, \nu)$ and $(y_1, y_2) = (1, \mu)$ with $\nu\mu^* = 1$, giving indeed $q - 1$ possibilities. □

5.4. **Main result, and consequences.** It is now a straightforward matter to conclude our main structural result, restated here for convenience. We recall (2.2.3) the 2-Selmer signature map $\varphi_K \colon \mathrm{Sel}_2(K) \to V(K) = V_\infty(K) \boxplus V_2(K)$; by Proposition 3.1.1, we have $V_\infty(K) \simeq V_2(K) \simeq \mathbb{F}_2[G_K]$ as $\mathbb{F}_2[G_K]$-modules, equipped with the orthogonal direct sum of the bilinear forms (5.2.4). The image

$$S(K) := \mathrm{img}(\varphi_K) \simeq \mathrm{Sel}_2(K)/\ker(\varphi_K)$$

of the 2-Selmer group under the signature map is a G_K-invariant maximal totally isotropic subspace of $V(K)$ by Corollary 3.1.3. By the canonical orthogonal decomposition (3.2.8),

$$S(K) = \bigboxplus_\chi S(K)_{\chi^\pm}, \tag{5.4.1}$$

thus we conclude that $S(K)_{\chi^\pm}$ are maximal totally isotropic G_K-invariant subspaces of $V(K)_{\chi^\pm}$.

Theorem 5.4.2. *Let K be a Galois number field with abelian Galois group G_K of odd order. Then for each $\overline{\mathbb{F}}_2$-character χ, there are exactly 6 possibilities for $S(K)_{\chi^\pm} \leq V_\infty(K) \boxplus V_2(K)$ up to G_K-equivariant isometry.*

Proof. In view of the first paragraph, Theorem 5.3.5 applies to classify the possibilities. □

Using the notation (1.2.1), which matches (4.2.1) but with characters, we fill in Table 1.2.3 starting with a copy of Table 5.3.6 with the remaining columns filled in using Kummer duality (2.3.3) and Lemma 4.3.2.

We now see some immediate corollaries. First, the cornerstone result of Taylor [39].

Corollary 5.4.3 (Taylor [39, (*)]). *For an abelian Galois number field K of odd degree, let $\mathbb{F}_2(\chi)$ be an irreducible $\mathbb{F}_2[G_K]$-module. Then we have*

$$\begin{aligned} 0 \leq \ & k_\chi^+(K) + k_{\chi^*}^+(K) \ \leq 1, \\ 0 \leq \ & k_{4,\chi}(K) + k_{4,\chi^*}(K) \leq 1. \end{aligned}$$

Moreover, if $\mathbb{F}_2(\chi)$ is self-dual, then $k_\chi^+(K) = k_{\chi^*}^+(K) = 0 = k_{4,\chi}(K) = k_{4,\chi^*}(K)$.

Proof. Immediate from either Proposition 4.4.4, using that $\mathrm{rk}_\chi \mathbb{F}_2[G] = 1$ for all χ, or from Table 1.2.3. □

The next simplest case not treated by Corollary 5.4.3 is treated by the following corollary.

Corollary 5.4.4 (Corollary 5.4.10). *Let K be a cyclic field of prime degree $\ell \equiv 7 \pmod 8$ such that 2 has order $\frac{\ell-1}{2}$. If $\mathrm{Cl}(K)[2]$ is* not *self-dual, then $\mathrm{Cl}^+(K)[2]$ is self-dual and*

$$\mathrm{Cl}^+(K)[2] \simeq \mathbb{F}_2(\chi) \oplus \mathrm{Cl}(K)[2],$$

where χ is a nontrivial $\overline{\mathbb{F}}_2$-character of G_K.

In the case that $\mathrm{Cl}(K)[2]$ is self-dual, there are no restrictions on $\mathrm{Cl}^+(K)[2]$, and we model this situation in Conjecture 6.1.2.

Another corollary we obtain is the following result, proven by Oriat [35] (and a special case of the T-S-reflection principle of Gras [23, Théorème 5.18]): see also the survey by by Lemmermeyer [29, Theorem 7.2].

Corollary 5.4.5 (Oriat [35, Corollaire 2c]). *Let $m \in \mathbb{Z}_{\geq 1}$ denote the exponent of the Galois group G_K for the abelian number field K of odd degree. If there exists $t \in \mathbb{Z}$ such that $2^t \equiv -1 \pmod m$, then $\mathrm{Cl}^+(K)[2] \simeq \mathrm{Cl}_4(K)[2] \simeq \mathrm{Cl}(K)[2]$ as $\mathbb{F}_2[G_K]$-modules.*

Proof. By Lemma 5.1.3, every $\mathbb{F}_2[G]$-module is self-dual so the conclusion of Corollary 5.4.3 implies that $k_\chi^+(K) = k_{4,\chi}(K) = 0$ for all χ in the notation of Definition 4.3.1; the result follows. Alternatively, for the first isomorphism, apply Theorem 4.4.1, given that all modules are self-dual. □

Example 5.4.6. If ℓ is an odd prime such that 2 is a primitive root modulo ℓ, then any cyclic number field K of degree ℓ satisfies $\mathrm{rk}_2 \mathrm{Cl}(K) = \mathrm{rk}_2 \mathrm{Cl}^+(K)$ by Corollary 5.4.5.

Example 5.4.7. More generally, if 2 has even order modulo ℓ, then Corollary 5.4.5 applies to cyclic number fields of degree ℓ. The first prime for which 2 has even order modulo ℓ but 2 is not a primitive root in $(\mathbb{Z}/\ell\mathbb{Z})^\times$ is $\ell = 17$.

Example 5.4.8. Corollary 5.4.5 also applies to abelian groups that are not cyclic. For instance, if K is a number field with Galois group $G_K \simeq \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}$, then Corollary 5.4.5 implies that $\mathrm{rk}_2 \mathrm{Cl}(K) = \mathrm{rk}_2 \mathrm{Cl}^+(K)$.

Remark 5.4.9. Edgar–Mollin–Peterson [18, Theorem 2.5] reprove Corollary 5.4.5, and they additionally make the claim that the corollary holds for all *Galois* extensions (even though they only give a proof for the abelian case). Lemmermeyer [29, p. 13] observes that this

claim is erroneous. We give an explicit counterexample (of smallest degree). Let K be the degree-27 normal closure over $\mathbb{Q}$ of the field K_0 of discriminant $3^{16} \cdot 37^4$ defined by

$$x^9 - 3x^8 - 21x^7 + 63x^6 + 141x^5 - 435x^4 - 273x^3 + 996x^2 - 192x - 64,$$

which has LMFDB label 9.9.80676485676081.1. This nonabelian extension K has Galois group isomorphic to the Heisenberg group $C_3^2 : C_3$ (with label 9T7), which has exponent $m = 3$. The class group $\mathrm{Cl}(K)$ is trivial and $\mathrm{Cl}^+(K) \simeq (\mathbb{Z}/2\mathbb{Z})^6$.

Corollary 5.4.10. *Suppose K is a cyclic number field of prime degree $\ell \equiv 7 \pmod 8$ such that 2 has order $\frac{\ell-1}{2}$ in $(\mathbb{Z}/\ell\mathbb{Z})^\times$. Then there exist exactly 2 nontrivial irreducible $\mathbb{F}_2[G_K]$-modules $\mathbb{F}_2(\chi) \not\simeq \mathbb{F}_2(\chi^*)$.*

Moreover, if $\mathrm{Cl}(K)[2]$ is not self-dual, then either $\mathrm{Cl}^+(K)[2] \simeq \mathbb{F}_2(\chi) \oplus \mathrm{Cl}(K)[2]$ or $\mathrm{Cl}^+(K)[2] \simeq \mathbb{F}_2(\chi^*) \oplus \mathrm{Cl}(K)[2]$; and the same conclusion holds with $\mathrm{Cl}^+(K)[2]$ replaced by $\mathrm{Cl}_4(K)[2]$.

Proof. By Lemma 5.1.3, the hypotheses on ℓ imply that there is an irreducible $\mathbb{F}_2[G_K]$-module that is not self-dual. The first statement then follows from Example 5.1.5. In addition, $\mathrm{Cl}(K)[2]$ is not self-dual if and only if $\rho_\chi(K) \neq \rho_{\chi^*}(K)$, and so the second statement follows from cases B and B′. □

5.5. **Unit signature ranks.** We now deduce some consequences for unit signature ranks. Recall that the unit signature rank of K is $\mathrm{sgnrk}(\mathcal{O}_K^\times) = \dim_{\mathbb{F}_2} \mathrm{sgn}_\infty(\mathcal{O}_K^\times)$, where sgn_∞ was defined in Definition 2.2.1. There is a natural exact sequence

$$1 \to \{\pm 1\}^n / \mathrm{sgn}_\infty(\mathcal{O}_K^\times) \to \mathrm{Cl}^+(K) \to \mathrm{Cl}(K) \to 1$$

tying together the unit signature rank and the isotropy rank. For example, we have

$$n - \mathrm{sgnrk}(\mathcal{O}_K^\times) \leq \mathrm{rk}_2 \mathrm{Cl}^+(K).$$

In addition, recall from (1.3.1) that $\mathrm{sgnrk}_\chi(\mathcal{O}_K^\times)$ is equal to the multiplicity of $\mathbb{F}_2(\chi)$ in $\mathrm{sgn}_\infty(\mathcal{O}_K^\times)$. Since $\mathcal{O}_K^\times/(\mathcal{O}_K^\times)^2 \simeq \mathbb{F}_2[G_K]$, and G_K is abelian, every irreducible $\mathbb{F}_2[G_K]$-module occurs with multiplicity 1 inside the unit group and hence

$$0 \leq \mathrm{sgnrk}_\chi(\mathcal{O}_K^\times) \leq 1. \tag{5.5.1}$$

We improve upon the above inequality in the following main result.

Theorem 5.5.2. *Let K be an abelian number field of odd degree with Galois group G_K. Let χ be an $\overline{\mathbb{F}}_2$-character of G_K. Then the following statements hold.*

(a) *If $k_\chi^+(K) = 1$, then*

$$\mathrm{sgnrk}_\chi(\mathcal{O}_K^\times) = 0.$$

(b) *If $k_\chi^+(K) = 0$, then*

$$\max\big(0, 1 - \rho_\chi(K)\big) \leq \mathrm{sgnrk}_\chi(\mathcal{O}_K^\times) \leq 1.$$

Proof. The statement $\operatorname{sgnrk}_\chi(\mathcal{O}_K^\times) = 0$ is equivalent to $\left(\mathcal{O}_K^\times/(\mathcal{O}_K^\times)^2\right)_\chi \subseteq \ker(\varphi_{K,\infty})_\chi$. We can determine $\ker(\varphi_{K,\infty})_\chi$ by combining Theorem 4.4.1 with Lemma 3.2.3 to get

$$\ker(\varphi_{K,\infty}) \simeq \operatorname{Cl}_4(K)[2]^\vee \simeq \operatorname{Cl}^+(K)[2].$$

Hence, the $\mathbb{F}_2(\chi)$-multiplicities of $\ker(\varphi_{K,\infty})_\chi \subseteq \operatorname{Sel}_2(K)_\chi$ are given as follows:

$$\operatorname{rk}_\chi \operatorname{Sel}_2(K) = \rho_\chi(K) + 1$$
$$\operatorname{rk}_\chi \ker(\varphi_{K,\infty}) = \rho_\chi(K) + k_\chi^+(K) = \rho_\chi^+(K).$$

When $k_\chi^+(K) = 1$, then $(\mathcal{O}_K^\times/\mathcal{O}_K^{\times 2})_\chi \subseteq \operatorname{Sel}_2(K)_\chi = \ker(\varphi_{K,\infty})_\chi$ and so $\operatorname{sgnrk}_\chi(\mathcal{O}_K^\times) = 0$. This establishes (a). For (b), observe that in order for $(\mathcal{O}_K^\times/\mathcal{O}_K^{\times 2})_\chi \subseteq \ker(\varphi_{K,\infty})_\chi$, we would need to have $\operatorname{rk}_\chi \ker(\varphi_{K,\infty})_\chi \neq 0$ which does not occur if $k_\chi^+(K) = \rho_\chi(K) = 0$. □

Example 5.5.3. Let χ be the trivial character so that $\mathbb{F}_2(\chi) \simeq \mathbb{F}_2$ is the trivial $\mathbb{F}_2[G_K]$-module. Then $\operatorname{sgnrk}_\chi(\mathcal{O}_K^\times) = 1$: indeed, -1 generates the unique subspace of $\mathcal{O}_K^\times/(\mathcal{O}_K^\times)^2$ with trivial action. To see that this accords with Theorem 5.5.2, note that from Lemma 4.1.4 we have $\rho_\chi(K) = 0$ and hence $\operatorname{sgnrk}_\chi(\mathcal{O}_K^\times) = 1$.

Summing the contributions of each irreducible gives the following corollary.

Corollary 5.5.4. *Let K be a cyclic number field of odd prime degree ℓ, and let f be the order of 2 modulo ℓ. Then*

$$\operatorname{sgnrk}(\mathcal{O}_K^\times) \equiv 1 \pmod{f}$$

and the following statements hold:

(a) *If f is odd, then*

$$\max\left(1, \tfrac{\ell+1}{2} - \operatorname{rk}_2 \operatorname{Cl}(K)\right) \leq \operatorname{sgnrk}(\mathcal{O}_K^\times) \leq \ell.$$

(b) *If f is even, then*

$$\max\left(1, \ell - \operatorname{rk}_2 \operatorname{Cl}(K)\right) \leq \operatorname{sgnrk}(\mathcal{O}_K^\times) \leq \ell.$$

Proof. By Example 5.1.5, all nontrivial irreducible $\mathbb{F}_2[G_K]$-modules have cardinality 2^f, and so together with the trivial component generated by -1 gives the first congruence.

To prove (b), note that all $\mathbb{F}_2[G_K]$-modules are self-dual by Lemma 5.1.3, hence Corollary 5.4.3 implies that $k_\chi^+(K) = 0$. By adding up Theorem 5.5.2(b) for all $1 + \frac{\ell-1}{f}$ irreducible $\mathbb{F}_2[G_K]$-modules as in Example 5.1.5, we conclude the result.

For statement (a), every nontrivial $\mathbb{F}_2[G]$-module is not self-dual by Lemma 5.1.3. If $k_\chi^+(K) = 1$, then $k_{\chi^*}^+(K) = 0$ by Corollary 5.4.3, and $\operatorname{sgnrk}_\chi(\mathcal{O}_K^\times) = 0$ so

$$1 - \rho_\chi(K) - \rho_{\chi^*}(K) \leq 1 - \rho_{\chi^*}(K) \leq \operatorname{sgnrk}_\chi(\mathcal{O}_K^\times) + \operatorname{sgnrk}_{\chi^*}(\mathcal{O}_K^\times);$$

to obtain an upper bound, note that if $k_\chi^+(K) = k_{\chi^*}^+(K) = 0$, then

$$\operatorname{sgnrk}_\chi(\mathcal{O}_K^\times) + \operatorname{sgnrk}_{\chi^*}(\mathcal{O}_K^\times) \leq 2.$$

Summing over the $(\ell-1)/(2f)$ pairs of irreducible nontrivial $\mathbb{F}_2[G_K]$-modules as well as the trivial $\mathbb{F}_2[G_K]$-module, then gives

$$\frac{\ell+1}{2} - \operatorname{rk}_2 \operatorname{Cl}(K) \leq \operatorname{sgnrk}(\mathcal{O}_K^\times) \leq \ell.$$ □

We record the following result (observed for $\ell = 3$ by Armitage–Fröhlich [1, Theorem V]).

Corollary 5.5.5. *If K is a cyclic number field of prime degree ℓ where 2 is a primitive root modulo ℓ, then* $\operatorname{sgnrk}(\mathcal{O}_K^\times) = 1$ *or ℓ. If the class number of K is odd, then* $\operatorname{sgnrk}(\mathcal{O}_K^\times) = \ell$.

Proof. A special case of Corollary 5.5.4. □

The above setup allows us to recover many other related statements. We illustrate with the following.

Theorem 5.5.6 (Ichimura [25, Theorem 2])**.** *Let K be an abelian number field of odd degree with Galois group G_K. Let χ be an $\overline{\mathbb{F}}_2$-character of G_K. Then the following statements are equivalent:*

(i) $\big(\mathcal{O}_K^\times/(\mathcal{O}_K^\times)^2\big)_{\chi^\pm} \cap \ker(\operatorname{sgn}_\infty) \neq \{0\}$.
(ii) $\big(\mathcal{O}_K^\times/(\mathcal{O}_K^\times)^2\big)_{\chi^\pm} \cap \ker(\operatorname{sgn}_2) \neq \{0\}$.

Proof. This statement is trivially true whenever $\big(\mathcal{O}_K^\times/(\mathcal{O}_K^\times)^2\big)_{\chi^\pm} \cap \ker(\varphi_K) \neq \{0\}$. Otherwise, we have $S(K)_{\chi^\pm} = \varphi_K\big(\big(\mathcal{O}_K^\times/(\mathcal{O}_K^\times)^2\big)_{\chi^\pm}\big)$ and then it is equivalent to Proposition 4.4.4. □

6. Conjectures

Even with many aspects determined in a rigid way by the results of the previous section, there still remain scenarios where randomness remains. In this section, we propose a model in the spirit of the Cohen–Lenstra heuristics for this remaining behavior.

6.1. **Isotropy ranks.** We begin by developing a model for isotropy ranks when K runs over a collection of G-number fields (i.e., Galois number fields K equipped with an isomorphism such that $\operatorname{Gal}(K \mid \mathbb{Q}) \simeq G$), where G is a fixed finite abelian group of odd order. In light of Theorem 5.4.2 (and Table 1.2.3) a heuristic is only necessary to distinguish cases C,C' from D, i.e., when χ is a non-self-dual $\overline{\mathbb{F}}_2$-character of G and the collection is restricted to those K such that $\rho_\chi(K) = \rho_{\chi^*}(K)$. For all other cases, the isotropy ranks are determined.

We make the following heuristic assumption:

(H1) For the collection of G-number fields K such that $\rho_\chi(K) = \rho_{\chi^*}(K)$, the image component $S(K)_{\chi^\pm}$ as defined in (5.4.1) is distributed as a uniformly random G-invariant maximal totally isotropic subspace of $\mathbb{F}_2[G]^2_{\chi^\pm}$ (see Example 5.2.1).

The assumption (H1), combined with the restrictions and masses in Table 1.2.3 lead us to one of our main conjectures.

Conjecture 6.1.1. *Let G be an odd finite abelian group, and let χ be a non-self-dual $\overline{\mathbb{F}}_2$-character of G with underlying module of cardinality $\#\mathbb{F}_2(\chi) = q$. Then as K varies over G-number fields such that $\rho_\chi(K) = \rho_{\chi^*}(K)$, we have:*

$$\operatorname{Prob}\big(k_\chi^+(K) + k_{\chi^*}^+(K) = 0\big) = \frac{q-1}{q+1};$$
$$\operatorname{Prob}\big(k_\chi^+(K) + k_{\chi^*}^+(K) = 1\big) = \frac{2}{q+1}.$$

The same heuristic implies the same conjecture for the 2-adic isotropy ranks; indeed by Proposition 4.4.4, we have $k_\chi^+(K)+k_{\chi^*}^+(K) = k_{4,\chi}(K)+k_{4,\chi^*}(K)$. A particularly simple case of Conjecture 6.1.1 is complementary to Corollary 5.4.10.

Conjecture 6.1.2. *Let $G = \mathbb{Z}/\ell\mathbb{Z}$ where $\ell \equiv 7 \pmod 8$ is prime and suppose 2 has order $\frac{\ell-1}{2}$ in $(\mathbb{Z}/\ell\mathbb{Z})^\times$, and let $q := 2^{\frac{\ell-1}{2}}$. As K varies over G-number fields such that $\mathrm{Cl}(K)[2]$ is a self-dual $\mathbb{F}_2[G_K]$-module, we have*

$$\mathrm{Cl}^+(K)[2] \simeq \begin{cases} \mathrm{Cl}(K)[2] & \text{with probability } \frac{q-1}{q+1}; \\ \mathbb{F}_2(\chi) \oplus \mathrm{Cl}(K)[2] & \text{with probability } \frac{1}{q+1}; \\ \mathbb{F}_2(\chi^*) \oplus \mathrm{Cl}(K)[2] & \text{with probability } \frac{1}{q+1}. \end{cases}$$

where χ is a nontrivial $\overline{\mathbb{F}}_2$-character of G_K.

We predict the same probabilities as in Conjectures 6.1.1 and 6.1.2 in other natural subfamilies, such as when we fix the value $\rho_\chi(K) = \rho_{\chi^*}(K) = r$; in particular, this includes the family of G-number fields with odd class number (i.e., those with $\mathrm{rk}_2\,\mathrm{Cl}(K) = 0$).

6.2. **Unit signature ranks.** We now extend these heuristics to the unit signature rank. Recall that the 2-Selmer group $\mathrm{Sel}_2(K)$ is an $\mathbb{F}_2[G_K]$-module containing $\mathcal{O}_K^\times/(\mathcal{O}_K^\times)^2$ and the subspace $\ker(\varphi_{K,\infty}) \subseteq \mathrm{Sel}_2(K)$ of totally positive elements. To study the distribution of the units, for each finite odd abelian group G, we make the following heuristic assumption:

(H2) For the collection of G-number fields K, the subspace of $\mathrm{Sel}_2(K)$ generated by $\mathcal{O}_K^\times/(\mathcal{O}_K^\times)^2$ is distributed as a uniformly random $\mathbb{F}_2[G]$-submodule isomorphic to $\mathbb{F}_2[G]$ containing -1.

Decomposing into irreducibles, since $\mathcal{O}_K^\times/(\mathcal{O}_K^\times)^2 \simeq \mathbb{F}_2[G]$ we have $\mathrm{rk}_\chi\,\mathcal{O}_K^\times = 1$ for each irreducible $\mathbb{F}_2(\chi)$, and so we might also make the heuristic assumption:

(H2′) For the collection of G-number fields K and for each *nontrivial* $\overline{\mathbb{F}}_2$-character of G, the subspace of $\mathrm{Sel}_2(K)_\chi$ generated by $(\mathcal{O}_K^\times/(\mathcal{O}_K^\times)^2)_\chi$ is distributed as a uniformly random, 1-dimensional $\mathbb{F}_2(\chi)$-subspace.

Note that (H2) is equivalent to (H2′) and an *independence assumption* for each $\mathbb{F}_2(\chi)$, i.e., we expect no extra structure relating different isotypic components of the units inside $\mathrm{Sel}_2(K)$.

Remark 6.2.1. To make assumption (H2), we consider $\mathcal{O}_K^\times/(\mathcal{O}_K^\times)^2 \subseteq \mathrm{Sel}_2(K)$ and we do *not* look at the 2-Selmer map $\varphi_{K,\infty}$. The pairing and duality relations that put restrictions on the $k_\chi(K)$'s as in Corollary 5.4.3 will have an effect on the subspace $\ker(\varphi_{K,\infty}) \subseteq \mathrm{Sel}_2(K)$; in particular, it will impose constraints on the isotypic components of $\ker(\varphi_{K,\infty})$. However, as the subspace $\ker(\varphi_{K,\infty})$ is completely independent from $\mathcal{O}_K^\times/(\mathcal{O}_K^\times)^2$; hence, there are no restrictions on $(\mathcal{O}_K^\times/(\mathcal{O}_K^\times)^2)_\chi$ inside $\mathrm{Sel}_2(K)_\chi$.

We now state a conjecture for collections of G-number fields that are not completely determined by Theorem 5.5.2. We recall from (5.5.1) that $\mathrm{sgnrk}_\chi(\mathcal{O}_K^\times) = 0$ or 1 for any $\overline{\mathbb{F}}_2$-character χ of G_K.

Conjecture 6.2.2. *Let G be an abelian group of odd order and let χ be an $\overline{\mathbb{F}}_2$-character of G with $q := \#\mathbb{F}_2(\chi)$. As K varies over G-number fields such that $\operatorname{rk}_\chi \operatorname{Cl}^+(K) = \operatorname{rk}_\chi \operatorname{Cl}(K) = r$, we have*

$$\operatorname{Prob}\big(\operatorname{sgnrk}_\chi(\mathcal{O}_K^\times) = 0\big) = \frac{q^r - 1}{q^{r+1} - 1};$$
$$\operatorname{Prob}\big(\operatorname{sgnrk}_\chi(\mathcal{O}_K^\times) = 1\big) = \frac{q^{r+1} - q^r}{q^{r+1} - 1}.$$

Proof assuming (H2′). The dimensions of the isotypic components are given as follows:

- $\operatorname{rk}_\chi \mathcal{O}_K^\times/(\mathcal{O}_K^\times)^2 = 1$;
- $\operatorname{rk}_\chi \ker(\varphi_{K,\infty}) = r$; and
- $\operatorname{rk}_\chi \operatorname{Sel}_2(K) = r + 1$.

Therefore, under (H2′) we would have

$$\begin{aligned}\operatorname{Prob}\big((\mathcal{O}_K^\times/(\mathcal{O}_K^\times)^2)_\chi \subseteq \ker(\varphi_{K,\infty})_\chi\big) &= \frac{\#\{\text{1-dimensional subspaces of } \ker(\varphi_{K,\infty})_\chi\}}{\#\{\text{1-dimensional subspaces of } \operatorname{Sel}_2(K)_\chi\}} \\ &= \frac{(q^r - 1)/(q-1)}{(q^{r+1} - 1)/(q-1)} = \frac{q^r - 1}{q^{r+1} - 1}\end{aligned}$$

as claimed. □

We now turn to the simplest case, where G is cyclic of prime order ℓ and 2 is a primitive root mod ℓ. By Corollary 5.5.5, we conclude that $\operatorname{sgnrk}(\mathcal{O}_K^\times) = 1$ or ℓ.

Conjecture 6.2.3. *Let ℓ be an odd prime such that 2 is a primitive root modulo ℓ, and let $q := 2^{\ell-1}$. If $r \in \mathbb{Z}_{\geq 0}$, then as K ranges over cyclic number fields of degree ℓ with $\operatorname{rk}_2 \operatorname{Cl}(K) = (\ell-1)r$, we have*

$$\operatorname{Prob}\big(\operatorname{sgnrk}(\mathcal{O}_K^\times) = 1\big) = \frac{q^r - 1}{q^{r+1} - 1}; \qquad \operatorname{Prob}\big(\operatorname{sgnrk}(\mathcal{O}_K^\times) = \ell\big) = \frac{q^{r+1} - q^r}{q^{r+1} - 1}.$$

Proof assuming (H2′). There is a unique nontrivial $\overline{\mathbb{F}}_2$-character χ of $\mathbb{Z}/\ell\mathbb{Z}$, and so $\operatorname{rk}_2 \operatorname{Cl}(K) = (\ell-1)r$ if and only if $\operatorname{rk}_\chi \operatorname{Cl}(K) = r$. The result follows then from the hypothesis (H2′). □

Conjecture 6.2.3 is a theorem for the case $r = 0$ (odd class number) by Corollary 5.5.5.

In a different direction, we can consider the class of fields where not all modules are self-dual. The most common case is expected to be among fields with odd class number which by Theorem 5.5.2(b) has $\operatorname{sgnrk}_\chi(\mathcal{O}_K^\times) = 1 - k_\chi^+(K)$. Using Conjecture 6.1.1 and summing over the contributions we end up with the following binomial distribution.

Conjecture 6.2.4. *Let ℓ be an odd prime, let f be the order of 2 modulo ℓ, and suppose that f is odd. Let $q := 2^f$ and $m := \frac{\ell-1}{2f} \in \mathbb{Z}_{>0}$. Then as K varies over cyclic number fields of degree ℓ with* odd *class number, we have*

$$\operatorname{Prob}\Big(\operatorname{sgnrk}(\mathcal{O}_K^\times) = fs + \frac{\ell+1}{2}\Big) = \binom{m}{s}\left(\frac{q-1}{q+1}\right)^s\left(\frac{2}{q+1}\right)^{m-s}$$

for $0 \leq s \leq m$.

6.3. **Applications of class group heuristics for cyclic cubic and quintic fields.** The conjectures in the previous section give predictions conditioned on the 2-rank of the class group. We next combine our conjectures with predictions for the latter by applying the conjectures of [32] correcting the Cohen–Lenstra heuristics for cubic cyclic and quintic fields.

For $m \in \mathbb{Z}_{\geq 0} \cup \{\infty\}$ and $q \in \mathbb{R}_{>1}$, define $(q)_0 := 1$ and for nonzero m, let

$$(q)_m := \prod_{i=1}^{m} (1 - q^{-i}).$$

For cyclic fields of odd prime degree ℓ, Cohen–Lenstra [9] made a prediction for the 2-part of their class groups; in particular, they imply (in the first moment) that the average size of $\mathrm{Cl}(K)[2]$ is equal to $\left(1 + 2^{-f}\right)^{\frac{\ell-1}{f}}$, where f is the order of 2 in $(\mathbb{Z}/\ell\mathbb{Z})^\times$. However, computations by Malle [32] suggest that this prediction needs a correction for the fact that the second roots of unity (but not the fourth roots of unity) are contained in any such field. Malle [32, (1),(2)] goes on to make predictions for the distribution of $\mathrm{rk}_2\,\mathrm{Cl}(K)$ as K ranges over cyclic fields of degrees 3 and 5.

Conjecture 6.3.1 (Malle)**.** *Let $\ell = 3$ or 5, and let $q = 2^{\ell-1}$. Then as K ranges over cyclic number fields of degree ℓ, we have*

$$\mathrm{Prob}\big(\mathrm{rk}_2\,\mathrm{Cl}(K) = (\ell-1)r\big) = \left(1 + \frac{1}{\sqrt{q}}\right) \frac{(\sqrt{q})_\infty (q^2)_\infty}{(q)_\infty^2} \cdot \frac{1}{\sqrt{q}^{r(r+2)} \cdot (q)_r} \tag{6.3.2}$$

for all $r \in \mathbb{Z}_{\geq 0}$.

Note that under the hypotheses of Conjecture 6.3.1, we have $\mathrm{rk}_2\,\mathrm{Cl}(K) = \mathrm{rk}_2\,\mathrm{Cl}^+(K)$ by Corollary 5.4.5, hence the left-hand side of (6.3.2) is equal to $\mathrm{Prob}\big(\mathrm{rk}_2\,\mathrm{Cl}^+(K) = (\ell-1)r\big)$. (For a discussion about class group heuristics for cyclic fields of prime degree $\ell \geq 7$, see Remark 7.2.3.)

Combining Conjecture 6.3.1 with Conjecture 6.2.3 and summing gives the following:

Conjecture 6.3.3. *As K varies over cyclic number fields of degree $\ell = 3$ or 5, we predict*

$$\mathrm{Prob}\big(\mathrm{sgnrk}(\mathcal{O}_K^\times) = 1\big) = \left(1 + \frac{1}{\sqrt{q}}\right) \cdot \frac{(\sqrt{q})_\infty (q^2)_\infty}{(q)_\infty^2} \cdot \sum_{r=0}^{\infty} \frac{1}{\sqrt{q}^{r(r+2)} \cdot (q)_r} \cdot \frac{q^r - 1}{q^{r+1} - 1},$$

where $q = 2^{\ell-1}$.

The values of these probabilities are given in the following table:

	$\ell = 3$	$\ell = 5$
$\mathrm{sgnrk}(\mathcal{O}_K^\times) = 1$	0.029573	0.000965
$\mathrm{sgnrk}(\mathcal{O}_K^\times) = \ell$	0.970427	0.999035

6.4. **Summary of results in small degree.** We now summarize the results and conjectures for the case $\ell = 3$, 5, and 7.

Cyclic cubic fields. We begin with the case $G = \mathbb{Z}/3\mathbb{Z}$ and $\ell = 3$. Here, 2 is a primitive root, and so there is a unique nontrivial irreducible $\mathbb{F}_2[G]$-module with $\mathbb{F}_2$-dimension $\ell - 1 = 2$ implying that $\operatorname{rk}_2 \operatorname{Cl}(K)$ is always even. Malle [32, (1)] (as in Conjecture 6.3.1) predicts

$$\operatorname{Prob}\big(\operatorname{rk}_2 \operatorname{Cl}(K) = 0, 2, 4\big) \approx 85.30\%, 14.21\%, 0.47\%;$$

the remaining cyclic cubic fields (having $\operatorname{rk}_2 \operatorname{Cl}(K) \geq 6$) conjecturally comprise less than 0.004% of all cyclic cubic fields. By Corollary 5.4.5, we have $\operatorname{Cl}(K)[2] \simeq \operatorname{Cl}^+(K)[2]$.

In this case, Conjecture 6.2.3 predicts $\operatorname{Prob}\big(\operatorname{sgnrk}(\mathcal{O}_K^\times) = s \mid \operatorname{rk}_2 \operatorname{Cl}(K) = r\big)$ according to the following table:

	$r = 0$	$r = 2$	$r = 4$
$s = 1$	0	$\frac{1}{5}$	$\frac{5}{21}$
$s = 3$	1	$\frac{4}{5}$	$\frac{16}{21}$

For example, amongst cyclic cubic fields with $\operatorname{rk}_2 \operatorname{Cl}(K) = 4$, we predict $\frac{16}{21}$ will have units of mixed signature. Combining these first three values for the 2-ranks with the associated conditional probabilities for $\operatorname{sgnrk}(\mathcal{O}_K^\times)$ yields

$$\operatorname{Prob}\big(\operatorname{sgnrk}(\mathcal{O}_K^\times) = 3\big) \approx 1 \cdot 85.30\% + \frac{4}{5} \cdot 14.21\% + \frac{16}{21} \cdot 0.47\% \approx 97.03\%.$$

Conjecture 6.3.3 then implies: as K varies over cyclic cubic fields, the unit signature rank is equal to 1 approximately 3% of the time, and the unit signature rank is equal to 3 approximately 97% of the time.

Cyclic quintic fields. When $G = \mathbb{Z}/5\mathbb{Z}$, we again have that 2 is a primitive root modulo 5, so there is a unique irreducible nontrivial irreducible $\mathbb{F}_2[G_K]$-module of dimension 4. Malle [32, (2)] predicts

$$\begin{aligned} \operatorname{Prob}\big(\operatorname{rk}_2 \operatorname{Cl}(K) = 0\big) &\approx 98.35\%, \\ \operatorname{Prob}\big(\operatorname{rk}_2 \operatorname{Cl}(K) = 4\big) &\approx 1.63\%, \end{aligned}$$

and $\operatorname{Prob}\big(\operatorname{rk}_2 \operatorname{Cl}(K) \geq 8\big) \leq 0.02\%$. Again, by Corollary 5.4.5 we have $\operatorname{Cl}(K)[2] \simeq \operatorname{Cl}^+(K)[2]$. Here, Conjecture 6.2.3 predicts $\operatorname{Prob}\big(\operatorname{sgnrk}(\mathcal{O}_K^\times) = s \mid \operatorname{rk}_2 \operatorname{Cl}(K) = r\big)$ as:

	$r = 0$	$r = 4$	$r = 8$
$s = 1$	0	$\frac{1}{17}$	$\frac{17}{273}$
$s = 5$	1	$\frac{16}{17}$	$\frac{256}{273}$

Summing as above yields

$$\operatorname{Prob}\big(\operatorname{sgnrk}(\mathcal{O}_K^\times) = 5\big) \approx 1 \cdot 98.35\% + \frac{16}{17} \cdot 1.63\% + \frac{256}{273} \cdot 0.001\% \approx 99.90\%,$$

and so Conjecture 6.3.3 predicts that 99.9% of cyclic quintic fields have units of all possible signatures. The smallest conductor of a cyclic quintic field with $\operatorname{sgnrk}(\mathcal{O}_K^\times) = 1$ is 39821. This field is $K = \mathbb{Q}(\alpha)$ where α is a root of the polynomial

$$x^5 + x^4 - 15928x^3 - 218219x^2 + 20800579x + 363483463.$$

Cyclic septic fields. We now consider the case $G = \mathbb{Z}/7\mathbb{Z}$. Since 2 has order 3 modulo 7 and $-1 \notin \langle 2\rangle \leq (\mathbb{Z}/7\mathbb{Z})^\times$, there are two nontrivial irreducibles $\mathbb{F}_2(\chi) \not\simeq \mathbb{F}_2(\chi^*)$ with $\#\mathbb{F}_2(\chi) = \#\mathbb{F}_2(\chi^*) = 2^3 = 8$. In this case, we may or may not have $\mathrm{Cl}^+(K)[2] \simeq \mathrm{Cl}(K)[2]$. We refer to Theorem 5.4.2 and recall Definition 2.2.5.

- If $\mathrm{Cl}(K)[2]$ is not self-dual, then $k^+(K) = 3$.
- If $\mathrm{Cl}(K)[2]$ is self-dual, then $k^+(K) = 0$ or 3, and Conjecture 6.1.1 predicts that
$$\mathrm{Prob}\big(k^+(K) = 3\big) = \tfrac{2}{9}.$$

Example 6.4.1. We now provide examples of the above three cases for cyclic septic number fields. For each case let $K = \mathbb{Q}(\alpha)$ where α is a root of the polynomial $f(x)$.

- For the field with LMFDB label 7.7.14011639427134441.1 of discriminant 491^6 defined by $f(x) = x^7 - x^6 - 210x^5 - 1423x^4 - 1410x^3 + 8538x^2 + 9203x - 19427$, we have that $\mathrm{Cl}(K)[2]$ not self-dual and $k^+(K) = 3$.
- For 7.7.6321363049.1 of discriminant 43^6 defined by $f(x) = x^7 - x^6 - 18x^5 + 35x^4 + 38x^3 - 104x^2 + 7x + 49$, we have that $\mathrm{Cl}(K)[2]$ is self-dual and $k^+(K) = 0$.
- For 7.7.6321363049.1 again of discriminant 43^6 defined by $f(x) = x^7 - x^6 - 12x^5 + 7x^4 + 28x^3 - 14x^2 - 9x - 1$, we have that $\mathrm{Cl}(K)[2]$ is self-dual and $k^+(K) = 3$.

For unit signature ranks, using the formulas in Conjectures 6.2.2 and 6.2.4 we make the following predictions for class groups of cyclic septic fields with low 2-rank.

- Suppose $\mathrm{rk}_2\,\mathrm{Cl}(K) = 0$. Conjecture 6.2.4 then implies:
$$\begin{aligned}\mathrm{Prob}\big(\mathrm{sgnrk}(\mathcal{O}_K^\times) = 4 \,|\, \mathrm{rk}_2\,\mathrm{Cl}(K) = 0\big) &= \tfrac{2}{9};\\ \mathrm{Prob}\big(\mathrm{sgnrk}(\mathcal{O}_K^\times) = 7 \,|\, \mathrm{rk}_2\,\mathrm{Cl}(K) = 0\big) &= \tfrac{7}{9}.\end{aligned}$$
- Suppose $\mathrm{rk}_2\,\mathrm{Cl}(K) = 3$. Without loss of generality, assume $\rho_\chi(K) = 1$ and $\rho_{\chi^*}(K) = 0$. By Theorems 5.4.2(b)(i) and 5.5.2(a), we have $\mathrm{sgnrk}_{\chi^*}(\mathcal{O}_K^\times) = 0$. Using Conjecture 6.2.2 with $\rho_\chi(K) = 1$, we predict that $\mathrm{sgnrk}_\chi(\mathcal{O}_K^\times) = 0$ occurs with probability $\frac{7}{63}$, so
$$\begin{aligned}\mathrm{Prob}\big(\mathrm{sgnrk}(\mathcal{O}_K^\times) = 1 \,|\, \mathrm{rk}_2\,\mathrm{Cl}(K) = 3\big) &= \tfrac{1}{9};\\ \mathrm{Prob}\big(\mathrm{sgnrk}(\mathcal{O}_K^\times) = 4 \,|\, \mathrm{rk}_2\,\mathrm{Cl}(K) = 3\big) &= \tfrac{8}{9}.\end{aligned}$$

7. Computations

In this section, we present computations that provide evidence to support our conjectures. To avoid redundancy, instead of working with families of G-number fields (which weights each isomorphism class of a field K by $\#\,\mathrm{Aut}(G_K)$), we weight each isomorphism class of number fields by 1. (Either weighting evidently gives the same probabilities and moments.)

We begin by describing a method for computing a random cyclic number field of odd prime degree ℓ of conductor $\leq X$. Recall (by the Kronecker–Weber theorem) that $f \in \mathbb{Z}_{\geq 0}$ arises as a conductor for such a field if and only if $f = f'$ or $\ell^2 f'$ where f' is a squarefree product of primes $p \equiv 1 \pmod{\ell}$. Moreover, the number of such fields is equal to $(\ell-1)^{\omega(f)-2}$ if $\omega(f) \geq 2$ and $\ell \mid f$, otherwise the number is $(\ell-1)^{\omega(f)-1}$. Our algorithm generates a random factored integer $f \leq X$ of this form and a uniform random character with given conductor; then, it constructs the corresponding field by computing an associated Gaussian period.

7.1. **Cubic fields.** We sampled cyclic cubic fields in this manner, performing our computations in Magma [31]; the total computing time was a few CPU days. The class group and narrow class group computations are conjectural on the Generalized Riemann Hypothesis (GRH). Our code generating this data is available online [5].

Let $\mathcal{N}_3(X)$ denote the set of sampled cyclic cubic fields K (having $\mathrm{Cond}(K) \leq X$), and let $\mathcal{N}_3(X, \rho = r) \subseteq \mathcal{N}_3(X)$ denote the subset of fields K with $\mathrm{rk}_2\,\mathrm{Cl}(K) = r$. For each of $X = 10^5$, 10^6, and 10^7, we sampled $\#\mathcal{N}_3(X) = 10^4$ fields. Note that the asymptotic number of cyclic cubic fields with conductor bounded by X is $c_3 \cdot X$ where $c_3 \approx 0.159$ [12] (see also [8, Corollary 4.7]). We remark that in the below tables, N = sample size, $\pm 1/\sqrt{N}$ indicates the confidence interval, and when the prediction is a theorem, we indicate it in bold.

Family	Property	Proportion of Family satisfying Property			Prediction
		$X = 10^5$	$X = 10^6$	$X = 10^7$	
$\mathcal{N}_3(X)$	$\mathrm{rk}_2\,\mathrm{Cl}(K) = 0$	0.873	0.871	0.867	0.853
	$\mathrm{rk}_2\,\mathrm{Cl}(K) = 2$	0.127	0.129	0.133	0.142
$1/\sqrt{N} = .01$	$\mathrm{rk}_2\,\mathrm{Cl}(K) \geq 4$	0.001	0.001	0.001	0.005
$\mathcal{N}_3(X)$	$\mathrm{sgnrk}(\mathcal{O}_K^\times) = 1$	0.023	0.024	0.026	0.030
$1/\sqrt{N} = .01$	$\mathrm{sgnrk}(\mathcal{O}_K^\times) = 3$	0.977	0.976	0.974	0.970
$\mathcal{N}_3(X, \rho = 0)$	$\mathrm{sgnrk}(\mathcal{O}_K^\times) = 1$	0.000	0.000	0.000	**0**
$1/\sqrt{N} \approx .11$	$\mathrm{sgnrk}(\mathcal{O}_K^\times) = 3$	1.000	1.000	1.000	**1**
$\mathcal{N}_3(X, \rho = 2)$	$\mathrm{sgnrk}(\mathcal{O}_K^\times) = 1$	0.177	0.185	0.189	$0.200 = \frac{1}{5}$
$1/\sqrt{N} \approx .27\text{-}.28$	$\mathrm{sgnrk}(\mathcal{O}_K^\times) = 3$	0.823	0.814	0.811	$0.800 = \frac{4}{5}$

Table 7.1.1: Data for class group and signature ranks of sampled cyclic cubic fields

Family	Moment	Average			Prediction
		$X = 10^5$	$X = 10^6$	$X = 10^7$	
$\mathcal{N}_3(X)$	$\#\,\mathrm{Cl}(K)[2]$	1.404	1.434	1.467	$1.500 = \frac{3}{2}$
	$(\#\,\mathrm{Cl}(K)[2])^2$	3.268	3.702	4.079	$4.500 = \frac{9}{2}$
$1/\sqrt{N} = .01$	$(\#\,\mathrm{Cl}(K)[2])^3$	14.76	21.44	26.67	$40.50 = \frac{81}{2}$

Table 7.1.2: Data for moments of (narrow) class groups of sampled cyclic cubic fields

7.2. **Septic fields.** We now turn to computations for cyclic extensions of degree seven. The complexity of the fields grew so quickly that it was infeasible to sample fields. Instead we computed the first 8000 cyclic degree seven fields ordered by conductor. This list is available online [5], and we confirmed our results against independent computations of Hofmann [6].

Let $\mathcal{N}_7(X)$ denote the set of septic cyclic fields with $\mathrm{Cond}(K) < X$, and let $\mathcal{N}_7(X, \rho = r) \subseteq \mathcal{N}_7(X)$ denote the subset of fields K satisfying $\mathrm{rk}_2\,\mathrm{Cl}(K) = r$. Asymptotically, we have $\mathcal{N}_7(X) \sim c_7 \cdot X$ where $c_7 \approx 0.033$ by [8, Corollary 4.7]. The first 8000 cyclic septic fields

corresponds to the set $\mathcal{N}_7(X_0)$ where $X_0 = 244861$. In addition, we have $\#\mathcal{N}_7(X_0, \rho = 0) = 7739$, $\#\mathcal{N}_7(X_0, \rho = 3) = 241$, and $\#\mathcal{N}_7(X_0, \rho = 6) = 20$. For all other $r \in \mathbb{Z}_{\geq 0}$, we have $\#\mathcal{N}_7(X_0, \rho = r) = 0$. Because the sample size was so small, in Table 7.2.1 below we do not compute statistics for the subset $\mathcal{N}_7(X_0, \rho = 6)$. The first few fields in $\mathcal{N}_7(X_0, \rho = 6)$ are generated by the roots of the polynomials:

$x^7 - 1491x^5 + 29323x^4 - 118783x^3 - 662004x^2 + 1844864x - 899641,$

$x^7 + x^6 - 3360x^5 + 54087x^4 + 1523280x^3 - 24904626x^2 - 194909041x + 2439485891,$

$x^7 - x^6 - 8274x^5 - 249021x^4 + 3000578x^3 + 60235500x^2 + 152710207x + 67428091,$

$x^7 - x^6 - 14340x^5 + 328464x^4 + 46377824x^3 - 1467892080x^2 - 11615446400x + 118681888000,$

$x^7 - 18543x^5 + 154525x^4 + 67057669x^3 - 1368522848x^2 - 26253624432x + 269027889901.$

These computations took approximately 1 CPU day. Further computations quickly run into the difficulty of computing class groups of fields with large discriminants. When the prediction is a theorem, we indicate it in bold. In addition, the class group and narrow class group computations remain conjectural on GRH. Our code is available online [5].

Family	Property	Proportion of Family satisfying Property	Prediction
		$X \approx 244861$	
$\mathcal{N}_7(X)$ $\#$ = 8000	$\mathrm{rk}_2\,\mathrm{Cl}(K) = 0$	0.967	?
	$\mathrm{rk}_2\,\mathrm{Cl}(K) = 3$	0.030	?
	$\mathrm{rk}_2\,\mathrm{Cl}(K) \geq 6$	0.003	?
$\mathcal{N}_7(X, \rho = 0)$ $\#$ = 7739	$\mathrm{rk}_2\,\mathrm{Cl}^+(K) = 0$	0.772	$0.778 = \frac{7}{9}$
	$\mathrm{rk}_2\,\mathrm{Cl}^+(K) = 3$	0.228	$0.222 = \frac{2}{9}$
$\mathcal{N}_7(X, \rho = 0)$ $\#$ = 7739	$\mathrm{sgnrk}(\mathcal{O}_K^\times) = 4$	0.228	$0.222 = \frac{2}{9}$
	$\mathrm{sgnrk}(\mathcal{O}_K^\times) = 7$	0.772	$0.778 = \frac{7}{9}$
$\mathcal{N}_7(X, \rho = 3)$ $\#$ = 241	$\mathrm{rk}_2\,\mathrm{Cl}^+(K) = 3$	0.00	**0**
	$\mathrm{rk}_2\,\mathrm{Cl}^+(K) = 6$	1.00	**1**
$\mathcal{N}_7(X, \rho = 3)$ $\#$ = 241	$\mathrm{sgnrk}(\mathcal{O}_K^\times) = 1$	0.083	$0.111 = \frac{1}{9}$
	$\mathrm{sgnrk}(\mathcal{O}_K^\times) = 4$	0.917	$0.889 = \frac{8}{9}$
	$\mathrm{sgnrk}(\mathcal{O}_K^\times) = 7$	0.000	**0**

Table 7.2.1: Data for class group and signature ranks of the first 8000 cyclic septic fields

There are two non-trivial characters χ and χ^* for the Galois group when $G_K \simeq \mathbb{Z}/7\mathbb{Z}$. In light of Corollary 1.2.4, one may wonder how often the inequalities $|\,\mathrm{rk}_\chi\,\mathrm{Cl}(K) - \mathrm{rk}_{\chi^*}\,\mathrm{Cl}(K)| \leq 1$ and $|\,\mathrm{rk}_\chi\,\mathrm{Cl}^+(K) - \mathrm{rk}_{\chi^*}\,\mathrm{Cl}^+(K)| \leq 1$ are equalities, i.e., how often the class group or the narrow class group is *not* self-dual. The 2-torsion subgroup of the class group is self-dual

when the exponent n satisfying $\mathrm{rk}_2\,\mathrm{Cl}(K) = 3^n$ is *even*. In particular, for the first 8000 cyclic septic fields we found that a proportion of 0.970 have $\mathrm{Cl}(K)[2]$ self-dual.

Family	Moment	Average	Prediction
	$X \approx 244861$		
$\mathcal{N}_7(X)$ $1/\sqrt{N} = 0.11$	$\#\,\mathrm{Cl}(K)[2]$	1.368	$1.375 = \frac{11}{8}$?
	$(\#\,\mathrm{Cl}(K)[2])^2$	13.13	?
	$(\#\,\mathrm{Cl}(K)[2])^3$	671.7	?
$\mathcal{N}_7(X)$ $1/\sqrt{N} = 0.11$	$\#\,\mathrm{Cl}^+(K)[2]$	4.823	?
	$\left(\#\,\mathrm{Cl}^+(K)[2]\right)^2$	277.5	?
	$\left(\#\,\mathrm{Cl}^+(K)[2]\right)^3$	75643.8	?

Table 7.2.2: Data for moments of class groups of the first 8000 cyclic septic fields

For the 2-torsion subgroup of the narrow class group, there are two possibilities: if $\mathrm{Cl}(K)[2]$ is not self-dual, then $\mathrm{Cl}^+(K)[2]$ is self-dual; and if $\mathrm{Cl}(K)[2]$ is self-dual we conjecture that $\mathrm{Cl}^+(K)[2]$ is also self-dual with probability $7/9 = 0.778$. Our conjecture implies that the proportion of cyclic septic fields with $\mathrm{Cl}^+(K)[2]$ self-dual is at least 0.778. This data suggests that it may be much more likely for class groups and narrow class groups to be self-dual.

Remark 7.2.3. As of yet, no corrected predictions taking into account the existence of the 2nd (but not 4th) roots of unity in the base field have been made on the distribution of the 2-ranks of class groups of cyclic septic fields over $\mathbb{Q}$ (or more generally, of degree ℓ cyclic fields for any (fixed) prime $\ell \geq 7$ over $\mathbb{Q}$). The original distribution in Cohen–Lenstra [9] predicts the average size of $\mathrm{Cl}(K)[2]$ when K varies over cyclic septic fields to be $\frac{81}{64} \approx 1.266$. However, our computations for $\ell = 7$ (see Table 7.2.2) suggest that the average size of $\mathrm{Cl}(K)[2]$ for cyclic septic fields is $\frac{11}{8}$.

In fact, we expect that the distribution of the moments for the 2-torsion subgroups in class groups of cyclic fields of prime degree ℓ to be quite different when the order of 2 modulo ℓ is even than when the order is odd. For example, the distribution given in Conjecture 6.3.1 implies that the average size of $\mathrm{Cl}(K)[2]$ is $1 + 2^{-f/2}$ for $\ell = 3$ or 5 and f denotes the order of 2 modulo ℓ. For $\ell = 7$, this computes to approximately 1.354, which is already exceeded for the family of cyclic septic fields of conductor bounded by X_0 where $X_0 \approx 244861$ (see Table 7.2.2).

Appendix A. Cyclic cubic fields with signature rank 1 (with Noam Elkies)

In this appendix, we use Diophantine methods to construct infinite families of cyclic cubic fields with no units of mixed sign (unit signature rank 1).

A.1. **Setup.** Start with a generic polynomial of the form

$$f_{a,b}(x) = f(x) := x^3 - ax^2 + bx - 1, \qquad (a, b) \in \mathbb{Z}^2,$$

with constant coefficient -1; a root of $f(x)$ is a unit in $\mathbb{Z}[x]/(f(x))$. By the rational root test, the polynomial $f(x)$ is reducible over $\mathbb{Q}$ if and only if $b = a$ or $b = -a - 2$. When $f(x)$ is irreducible, let $K := \mathbb{Q}[x]/(f(x))$. To ensure that K is a cyclic cubic field, we need the discriminant $D(a, b)$ of this polynomial to be a square, i.e., we need $c \in \mathbb{Z}$ such that

$$c^2 = D(a, b) = -4a^3 + a^2b^2 + 18ab - (4b^3 + 27). \tag{A.1.1}$$

The equation (A.1.1) describes a surface S in $\mathbb{A}^3_{\mathbb{Z}}$ in the variables (a, b, c). Several curves on the surface S have been studied; for example, the *simplest cubics* of Shanks [36] are defined by $(a, b, c) = (a, -(a+3), a^2+3a+9)$. See also work of Balady [3] for a study of the surface S over $\mathbb{Q}$ and other families of cubic fields arising from rational curves on S; unfortunately, the families he presents [3, §4] all have unit signature rank 3. By studying the surface S we prove the following theorem.

Theorem A.1.2. *There are cyclic cubic fields of arbitrarily large discriminant with unit signature rank* 1.

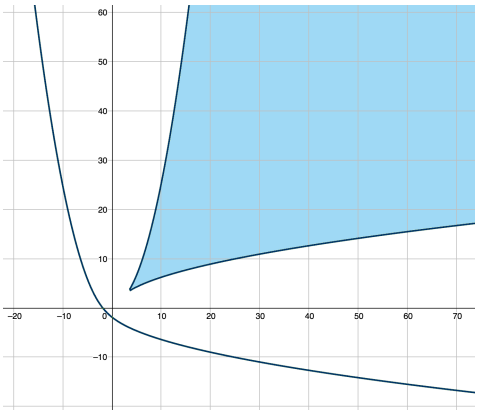
More precisely, we find families of Fermat–Pell curves on S that have infinitely many integral points $(a, b, c) \in S(\mathbb{Z})$ and such that:

$$\text{the roots of } f(x) \text{ are totally positive and not squares of smaller units.} \tag{A.1.3}$$

Studying the ramification in these extensions proves that our procedure produces cyclic cubic fields of arbitrarily large discriminant.

Theorem A.1.2 makes a result of Dummit–Dummit–Kisilevsky [14, Theorem 3] unconditional: namely, the difference between $\varphi(m)/2$ and the unit signature rank of $\mathbb{Q}(\cos(2\pi/m))$ can be arbitrarily large. This result has also been given a different (unconditional) proof by Dummit–Kisilevsky [15, Theorem 7].

A.2. **Construction of curves.** Plotting the discriminant $D(a, b) = 0$ we find two curves:



(A.2.1)

By continuity and checking values, the region in the upper right quadrant bounded by the cuspidal curve is the locus of $(a, b) \in \mathbb{R}^2$ with three positive roots: these are precisely the values of (a, b) where $a, b > 0$ and $f(x)$ has all real roots.

The curve $D(a, b) = 0$ has a visible cusp at $(a, b) = (3, 3)$, corresponding to the cubic $f_{3,3}(x) = (x-1)^3$. There are also two conjugate cusps $(a, b) = (3\zeta, 3\bar{\zeta})$ where ζ is one of the nontrivial cube roots of unity $(-1 \pm \sqrt{-3})/2$; these likewise correspond to $f_{3\zeta,3\bar{\zeta}}(x) = (x-\zeta)^3$.

The line joining these cusps is $a+b+3=0$; on this line $D(a,b)=D(a,-(a+3))$ is a quartic in a with a double root at each $a=3\zeta$, and indeed $D(a,-(a+3))=(a^2+3a+9)^2$, so we recover Shanks' "simplest cubics"; we know already that we cannot use those cubics, and indeed the line $a+b+3=0$ is disjoint from the shaded region in (A.2.1).

We obtain our Fermat–Pell curves by trying curves of the next-lowest degree passing through the conjugate cusps. We use the pencil of parabolas in the (a,b)-plane passing through those cusps and the point at infinity $(a:b:1)=(0:1:0)$; that is,

$$P_m\colon b = m(a^2+3a+9)-(a+3)$$

depending on a parameter $m\in\mathbb{Q}$. On such a parabola, $D(a,b)$ is a sextic in a divisible by $(a^2+3a+9)^2$; explicitly,

$$c^2=(a^2+3a+9)^2Q_m(a), \tag{A.2.2}$$

where Q_m is the quadratic polynomial

$$Q_m(a)=m^2(1-4m)a^2+(-12m^3+12m^2-2m)a+(-36m^3+36m^2-12m+1).$$

Dividing equation (A.2.2) by the square factor on the right side transforms the Diophantine equation $D(a,b)=c^2$ into an equivalent Fermat–Pell curve of the form $x^2=Q_m(a)$ for suitable choices of m.

To avoid issues with integrality, let $m=p/q$ (written in lowest terms) and clear the denominators of (A.2.2) by multiplying by q^3. The change of variable $y=qc/(a^2+3a+9)$ yields an equivalent integral curve

$$C_m\colon qy^2=Aa^2+Ba+C \tag{A.2.3}$$

in $\mathbb{A}^2_{\mathbb{Z}}$, where

$$\begin{aligned}A&:=-4p^3+p^2q,\\ B&:=-12p^3+12p^2q-2pq^2,\\ C&:=-36p^3+36p^2q-12pq^2+q^3.\end{aligned}$$

We shall see that there are m for which this curve yields an infinite family of cyclic cubic fields with no mixed-sign units.

For starters, in order for P_m to have integral points, the denominator of m must be odd since a^2+3a+9 is always odd. Additionally, for P_m to have infinitely many integral points in the first quadrant of the ab-plane, we must have $m>0$, else the intersection of P_m with the the half-plane $b>0$ is bounded.

Proposition A.2.4. *Let $m\in\mathbb{Q}$ be such that the following conditions hold:*

(i) *There exists $(a,y_0)\in C_m(\mathbb{Z})$ with $2Aa+B>0$;*
(ii) *$m=p/q$ with q odd;*
(iii) *$0<m<1/4$; and*
(iv) *$1-4m$ is not a square.*

Then there exist infinitely many $(a,y)\in C_m(\mathbb{Z})$ with $a>0$, and we have a map

$$\begin{aligned}\phi_m\colon C_m(\mathbb{Z})&\to S(\mathbb{Z})\\ (a,y)&\mapsto (a,b,c)=(a,m(a^2+3a+9)-(a+3),y(a^2+3a+9)/q).\end{aligned}$$

Remark A.2.5. We note that condition (i) implies condition (ii) in Proposition A.2.4. This can be shown by checking 2-adic valuations of each side of Equation (A.2.3).

Proof. Completing the square in (A.2.3), we obtain the standard form:

$$x^2 - (4Aq)y^2 = B^2 - 4AC \tag{A.2.6}$$

where $x = 2Aa + B$. By (i), there exists $(a, y_0) \in C_m(\mathbb{Z})$ which gives a point $(x_0, y_0) \in \mathbb{Z}^2$ on (A.2.6) with $x_0 = 2Aa + B > 0$ so that $a = (x_0 - B)/(2A) > 0$, and we may suppose without loss of generality that $y_0 > 0$. By (ii), we have $0 < m^2(1 - 4m) = A/q^3$ so $4Aq > 0$. By (iii), we conclude $4Aq = (1 - 4m)(2mq^2)^2$ is not a square. Therefore, by the theory of Pell equations, we have infinitely many solutions $(x, y) \in \mathbb{Z}^2$ to (A.2.6) with $x \equiv x_0 \equiv B \pmod{2A}$ and $x > 0$: explicitly, there exists a power of the fundamental unit for the real quadratic field $\mathbb{Q}(\sqrt{Aq})$ of the form $\epsilon = r + s\sqrt{4Aq}$ with $r, s \in \mathbb{Z}_{>0}$ and $r \equiv 1 \pmod{2A}$, so the solutions (x, y) obtained by multiplying $x_0 + y_0\sqrt{4Aq}$ by the powers $\epsilon^k = r_k + s_k\sqrt{4Aq}$ for $k \geq 1$ have $r_k \equiv 1 \pmod{2A}$ and $r_k, s_k > 0$, so $x = r_k s_0 + s_k y_0(4Aq) \equiv x_0 \pmod{2A}$ and $x > 0$. Letting $a = (x - B)/(2A) > 0$ and reversing the steps gives infinitely many $(a, y) \in C_m(\mathbb{Z})$.

To conclude, we claim that if $(a, y) \in C_m(\mathbb{Z})$, then

$$b = m(a^2 + 3a + 9) - (a + 3) \in \mathbb{Z}.$$

Reducing (A.2.3) modulo q gives

$$0 \equiv -4p^3a^2 - 12p^3a - 36p^3 = -4p^3(a^2 + 3a + 9) \pmod{q};$$

and since q is odd and $\gcd(p, q) = 1$ we conclude $q \mid (a^2 + 3a + 9)$, so $m(a^2 + 3a + 9) \in \mathbb{Z}$ and consequently $b \in \mathbb{Z}$. □

Remark A.2.7. The method for getting infinitely many $(a, y) \in C_m(\mathbb{Z})$ from an initial solution was already known to Euler [20]; see Dickson [13, pp. 355–356] (English translation in the Euler Archive, http://eulerarchive.maa.org/tour/tour_12.html). Dickson describes Euler's technique, which comes down to the same construction, though of course Euler did not use the arithmetic of real quadratic number fields.

To find a value of m suitable for applying Proposition A.2.4, we work backwards by first selecting an integral point $(a, b, c) \in S$ (by a brute force search or starting with a cyclic cubic field of unit signature rank 1) and then solving for the parameter m of the parabola P_m. (Since m occurs linearly in the formula for P_m, there is a unique solution; explicitly

$$m = \frac{a + b + 3}{a^2 + 3a + 9}. \tag{A.2.8}$$

As it happens the denominator is always positive so we do not even have to worry about dividing by zero at an unfortunate choice of (a, b).)

Example A.2.9. Let $(a, b) = (149, 4018)$. Solving for the corresponding parabola yields $m = 30/163$ which satisfies the conditions on m. The resulting equation is

$$C_m \colon 163y^2 = 38700a^2 - 157740a - 924893$$

and yields a sequence of solutions

$$(a,b) = (149, 4018), (395449, 28781401718),$$
$$(655993191035058918, 7920130061675324583839884151153754 9), \dots$$

Example A.2.10. Similarly for $(a,b) = (269, 10986)$, we obtain $m = 2/13$,

$$C_m \colon 13y^2 = 20a^2 - 148a - 275,$$

and

$$(a,b) = (1725, 456858), (17657181, 47965535241018),$$
$$(114572909, 2019530934725706),$$
$$(1175297035181, 212511249369405417243018), \dots$$

Remark A.2.11. Having found one m satisfying the conditions of Proposition A.2.4, such as $m = 2/13$ above, we can find infinitely many more. This is because D, and thus S, is symmetric under $(a,b) \leftrightarrow (b,a)$. Given an infinite sequence of $(a_k, b_k) \in C_m(\mathbb{Z})$, we may switch a, b in (A.2.8) to find an infinite sequence of $m_k = (a_k+b_k+3)/(b_k^2+3b_k+9)$ satisfying condition (i) of Proposition A.2.4. For $m = 2/13$, these m_k begin

$$\frac{2}{21447}, \frac{2}{910279}, \frac{2}{95931035167687}, \frac{2}{4039061640305607}, \frac{2}{425022498736460240415687}, \dots$$

corresponding to the initial solution $(a,b) = (149, 4018)$ in Example A.2.9 and the further four solutions listed there. Condition (ii), that $0 < m_k < 1/4$, is satisfied for all but finitely many k: each m_k is positive, and $m_k \to 0$ because $a_k \to \infty$ and $b_k \sim ma_k^2$. It remains to check that $1 - 4m_k$ is not a square for infinitely many k (condition (iii)). This can be done in various ways; for example, once we have checked this for one k_0, we can find some prime ℓ such that $1 - 4m_{k_0}$ is not a square mod ℓ, and apply Euler's theorem as in A.2.4 to find infinitely many k such that $m_k \equiv m_{k_0} \pmod{\ell}$, whence $1 - 4m_k$ is not a square either. For our $m = 2/13$ we may use $m_{k_0} = 2/21447$ and $\ell = 5$. This gives infinitely many curves C_{m_k} each containing infinitely many integral points of S above the shaded region in (A.2.1), thus showing that such points are Zariski-dense in S. (This is the same trick used by Elkies [19] to find a Zariski-dense set of rational points on the Fermat quartic surface $A^4 + B^4 + C^4 = D^4$ starting from a single elliptic curve on that surface with infinitely many rational points.)

A.3. **Infinitely many cyclic cubic fields.** The construction above produces infinitely many integral points (a,b) that correspond to cyclic cubic fields with totally positive units. We now show that for all but finitely many (a,b), the condition (A.1.3) holds.

For $a, b \in \mathbb{Z}^2$ such that $f_{a,b}(x) = x^3 - ax^2 + bx - 1$ is irreducible, let $K_{a,b} := \mathbb{Q}[x]/(f_{a,b}(x))$ and let $\eta_{a,b} \in K_{a,b}$ be the image of x.

Lemma A.3.1. *The following statements hold.*

(a) *If $\eta_{a,b} \in K_{a,b}^{\times 2}$, then $(a,b) = (A^2 - 2B, B^2 - 2A)$ for some $A, B \in \mathbb{Z}$.*
(b) *Let $m \in \mathbb{Q}$. Then there are only finitely many $(a,b) \in P_m(\mathbb{Z})$ such that $\eta_{a,b} \in K_{a,b}^{\times 2}$.*

Proof. For (a), let $\epsilon^2 = \eta_{a,b}$. Replacing ϵ by $-\epsilon$ if necessary, we may suppose that ϵ is a root of $x^3 - Ax^2 + Bx - 1$. Expressing a, b as symmetric polynomials in the roots, we obtain the result.

For (b), we study the squares on the parabola P_m by substituting in (a) to get

$$B^2 - 2A = m((A^2 - 2B)^2 + 3(A^2 - 2B) + 9) - (A^2 - 2B + 3).$$

which yields

$$(1 - 4m)B^2 + (4mA^2 + 6m - 2)B = mA^4 + (3m - 1)A^2 + 2A + (9m - 3). \tag{A.3.2}$$

The discriminant of (A.3.2) factors as $m(27m^2 - 9m + 1)^3$ up to a nonzero constant. So for $m \neq 0$ or $1/4$, this equation defines a genus 1 curve in the variables A, B. By Siegel's theorem [37, Corollary IX.3.2.2] it has finitely many integral points. □

Next, we prove that the construction above produces infinitely many distinct fields of the form $K_{a,b}$. Let $\alpha_{a,b} := 3\eta_{a,b} - a \in \mathcal{O}_{K_{a,b}}$; then $\alpha_{a,b}$ is an algebraic integer satisfying:

$$M_{a,b}(x) := x^3 + (a^2 + 3a + 9)(9m - 3)x + (a^2 + 3a + 9)(a(9m - 2) - 3) \in \mathbb{Z}[x].$$

Lemma A.3.3. *Let $m \in \mathbb{Q}$ satisfy conditions* (i)–(iii) *of Proposition* A.2.4. *Then as a ranges over points $(a, b, c) \in \phi_m(C_m(\mathbb{Z})) \subseteq S(\mathbb{Z})$ with $a > 0$, the set of primes ℓ such that $3 \nmid \mathrm{ord}_\ell(a^2 + 3a + 9)$ is infinite. Moreover, $\alpha_{a,b}$ generates a totally ramified extension of $\mathbb{Q}_\ell$ for all but finitely many such ℓ (depending on m).*

Proof. Let $t \in \mathbb{Z}_{>0}$ be cubefree. Then $a^2 + 3a + 9 = tz^3$ defines a genus 1 curve, so by Siegel's theorem it has finitely many integral points. Therefore there are only finitely many $(a, y) \in C_m(\mathbb{Z})$ such that $a^2 + 3a + 9 = tz^3$ for $z \in \mathbb{Z}$. But $\#C_m(\mathbb{Z}) = \infty$ by Proposition A.2.4, so the cubefree part of $a^2 + 3a + 9$ must take on infinitely many values.

For the second statement, we consider the Newton polygon of $M_{a,b}(x)$ at ℓ. Since

$$(81m^2 - 36m + 4)(a^2 + 3a + 9) + ((2 - 9m)a + 3 - 27m)((9m - 2)a - 3) = 27(27m^2 - 9m + 1)$$

it follows that, for any prime ℓ such that $\ell \nmid 27(27m^2 - 9m + 1)q^2$, we have

$$\mathrm{ord}_\ell[(a^2 + 3a + 9)(a(9m - 2) - 3)] = \mathrm{ord}_\ell(a^2 + 3a + 9).$$

For such primes, the ℓ-Newton polygon of $M_{a,b}(x)$ consists of a single segment of slope $\mathrm{ord}_\ell(a^2+3a+9)/3$, and hence the extension defined by $M_{a,b}(x)$ over $\mathbb{Q}_\ell$ is totally ramified. □

We finish with a proof of the theorem in this section.

Proof of Theorem A.1.2. Let $m \in \mathbb{Q}$ satisfy (i)–(iii) of Proposition A.2.4, so that $\phi_m(C_m)(\mathbb{Z})$ contains infinitely many points $(a, b, c) \in S(\mathbb{Z})$ with $a > 0$, and hence $b > 0$; for example, we may take $m = 30/163, 2/13$ as in Examples A.2.9 and A.2.10. The intersection of P_m with the lines $b = a$ and $b = a - 2$ removes at most 4 values of a; for the values that remain, $f_{a,b}(x) = x^3 - ax^2 + bx - 1$ is irreducible over $\mathbb{Q}$. To each of these points we associate the field $K_{a,b} = \mathbb{Q}(\eta_{a,b})$ where $\eta_{a,b}$ is a root of $f(x)$, and consider the set of fields

$$\mathcal{K}_m := \{K_{a,b} : (a, b, c) \in \phi_m(C_m)(\mathbb{Z}) \text{ and } f_{a,b}(x) \text{ is irreducible}\}.$$

Each $K_{a,b} \in \mathcal{K}_m$ is a cyclic cubic extension because its discriminant is (up to squares) equal to c^2, and since $a, b > 0$ its roots are totally positive as in (A.2.1). By Lemma A.3.3, there

are infinitely many primes ℓ dividing the discriminants of the fields in $\mathcal{K}$ and so the set contains fields with arbitrarily large discriminants. By Lemma A.3.1, in the set $\mathcal{K}$ there are only finitely many fields where $\eta_{a,b} \in K_{a,b}^{\times 2}$; let $\mathcal{K}^+$ be the infinitely many remaining fields. Since $\eta_{a,b} \notin K_{a,b}^{\times 2}$, then $\eta_{a,b}$ is a totally positive unit that is not a square. By Corollary 5.5.4, we have $\operatorname{sgnrk} \mathcal{O}_{K_{a,b}}^{\times} = 1, 3$, so we must have unit signature rank 1, i.e., there is a basis of totally positive units. □

References

[1] J.V. Armitage and A. Fröhlich, *Class numbers and unit signatures*, Mathematika **14** (1967), 94–98.

[2] M. Adam and G. Malle, *A class group heuristic based on the distribution of 1-eigenspaces in matrix groups*, J. Number Theory **149** (2015), 225-235.

[3] S. Balady, *Families of cyclic cubic fields*, J. Number Theory **167** (2016), 394–406.

[4] B. Breen, *The 2-Selmer group of number fields*, Ph.D. thesis, in preparation.

[5] B. Breen, I. Varma, and J. Voight, *Cyclic fields code*, 2019, available at https://github.com/BenKBreen/Cyclic-fields-code.

[6] C. Fieker, T. Hofmann, and C. Sircana. *On the construction of class fields*, Proceedings of the Thirteenth Algorithmic Number Theory Symposium, eds. Renate Scheidler and Jonathan Sorenson, Open Book Series 2, Mathematical Sciences Publishers, Berkeley, 2019, 239–255.

[7] S. Chan, P. Koymans, D. Milovic, and C. Pagano, *On the negative Pell equation*, arXiv preprint available at https://arxiv.org/abs/1908.01752.

[8] H. Cohen, F. Diaz y Diaz, and M. Olivier, *On the density of discriminants of cyclic extensions of prime degree*, J. reine angew. Math. **550** (2002), 169–109.

[9] H. Cohen and H.W. Lenstra, *Heuristics on class groups of number fields*, Number theory, Noordwijkerhout (1983), Lecture Notes in Math, no. 1068, Springer, Berlin (1984), 33–62.

[10] H. Cohen and J. Martinet, *Étude heuristique des groupes de classes des corps de nombres*, J. Reine Angew. Math. **404** (1990), 39–76.

[11] H. Cohen and J. Martinet, *Heuristics on class groups: some good primes are not too good*, Math. Comp. **63** (1994), no. 207, 329–334.

[12] H. Cohn, *The density of abelian cubic fields*, Proc. Amer. Math. Soc. **5** (1954), 476–477.

[13] L. E. Dickson, *History of the theory of numbers. Vol. II: Diophantine analysis*, Stechert & Co., Mineola, NY 1934.

[14] D.S. Dummit, E.P. Dummit, and H. Kisilevsky, *Signature ranks of units in cyclotomic extensions of abelian number fields*, Pacific Journal of Math. **298** (2019), no. 2, 285–298.

[15] D.S. Dummit and H. Kisilevsky, *Unit signatures in real biquadratic and multiquadratic number fields*, arXiv preprint available at https://arxiv.org/pdf/1904.04411.

[16] D.S. Dummit and J. Voight, *The 2-Selmer group of a number field and heuristics for narrow class groups and signature ranks of units*, appendix with Richard Foote, Proc. London Math. Soc. **117** (2018), 682–726.

[17] P. Dutarte, *Compatibilité avec le Spiegelungssatz de probabilités conjecturales sur le p-rang du groupe des classes*, Number theory (Besançon), 1983-?1984, Exp. no. 4, Publ. Math. Fac. Sci. Besançon, Univ. Franche-Comté, Besançon, 1984, 11 pages.

[18] H.M. Edgar, R.A. Mollin, and B.L. Peterson, *Class groups, totally positive units, and squares*, Proc. Amer. Math. Soc. **98** (1986), no. 1, 33–37.

[19] N.D. Elkies, *On* $A^4 + B^4 + C^4 = D^4$, Math. of Comp. **51** (Oct. 1988), 825–835.

[20] L. Euler, *De resolutione formularum quadricarum indeterminatarum per numeros integros* (On the resolution of formulas of squares of indeterminates by integral numbers), Novi Comm. Acad. Petrop. **9** (1764), 3–39; *Opera Omnia* (1) **2**, 576–611.

[21] É. Fouvry and J. Klüners, *On the negative Pell equation*, Ann. of Math. **172** (2010), no. 3, 2035–2104.

[22] A. Fröhlich, *Galois module structure of algebraic integers*, Springer, New York, 1983.
[23] G. Gras *Théoremes de réflexions*, J. Théor. Nombres Bordeaux **10** (1998), no. 2, 399–499.
[24] G. Gras, *Class field theory: from theory to practice*, Springer Monographs in Mathematics, Springer-Verlag, Berlin, 2010, corrected 2nd printing.
[25] H. Ichimura, *On a duality of Gras between totally positive and primary cyclotomic units*, Math. Journal of Okayama University **58** (2016), 125–132.
[26] Y. Lee, *Cohen–Lenstra heuristics and the Spiegelungssatz: number fields*, J. Number Theory **92** (2002), 37–66.
[27] Y. Lee, *Cohen–Lenstra heuristics and the Spiegelungssatz: function fields*, J. Number Theory **106** (2004), no. 2, 187–199.
[28] H.W. Leopoldt, *Zur Struktur der ℓ-Klassengruppe galoisscher Zahlkörper*, J. Reine Angew. Math. **199** (1958), 165–174.
[29] F. Lemmermeyer, *Selmer groups and quadratic reciprocity*, Abh. Math. Sem. Univ. Hamburg **76** (2006), 279–293.
[30] The LMFDB Collaboration, *The L-functions and Modular Forms Database*, http://www.lmfdb.org, 2019.
[31] W. Bosma, J. Cannon, and C. Playoust, *The Magma algebra system. I. The user language*, J. Symbolic Comput. **24** (3–4), 1997, 235–265.
[32] G. Malle, *Cohen-Lenstra heuristic and roots of unity*, J. Number Theory **128** (2008), no. 10, 2823–2835.
[33] G. Malle, *On the distribution of class groups of number fields*, Exp. Math. **19** (2010), vol. 4, 465–474.
[34] B. Oriat, *Relations entre les 2-groupes des classes d'idéaux des extensions quadratiques $k(\sqrt{d})$ et $k(\sqrt{-d})$*, Ann. Inst. Fourier (Grenoble) **27** (1977), no. 2, vii, 37–59.
[35] B. Oriat, *Relation entre les 2-groupes des classes d'idéaux au sens ordinaire et restreint de certains corps de nombres*, Bull. Soc. Math. France **104** (1976), no. 3, 301–307.
[36] D. Shanks, *The simplest cubic fields*, Math. Comp. **28** (1974), no. 128, 1137–1152.
[37] J.H. Silverman, *The arithmetic of elliptic curves*, 2nd ed., Grad. Texts in Math., vol. 106, Springer, Dordrecht, 2009.
[38] P. Stevenhagen, *The number of real quadratic fields having units of negative norm*, Experiment. Math. **2** (1993), issue 2, 121–136.
[39] M. Taylor, *Galois module structure of classgroups and units*, Mathematika **22** (1975), no. 2, 156–160.
[40] L.C. Washington, *Class numbers of the simplest cubic fields*, Math. Comp. **48** (1987), no. 177, 371–384.
[41] M.M. Wood, *On the probabilities of local behaviors in abelian field extensions*, Compos. Math. **146** (2010), no. 1, 102–128.

Email address: benjamin.k.breen.gr@dartmouth.edu

Department of Mathematics, Dartmouth College, 6188 Kemeny Hall, Hanover, NH 03755

Email address: ila@math.toronto.edu

Department of Mathematics, University of Toronto, Bahen Centre, 40 St. George Street, Toronto, ON M5S 2E4

Email address: jvoight@gmail.com

Department of Mathematics, Dartmouth College, 6188 Kemeny Hall, Hanover, NH 03755
URL: http://www.math.dartmouth.edu/~jvoight/