

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
2. Properties of the 2-Selmer group and its signature spaces	6
3. Galois module structure for invariants of odd Galois number fields	9
4. Structural results	15
5. Conjectures	21
6. Computations	26
Appendix A. Cyclic cubic fields with signature rank 1 (with Noam Elkies)	30
References	35

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 [34, 19, 7], predictions for the distribution of possible signs of units under real embeddings in families of higher degree fields have only recently been developed [15, 13, 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 a special case of our predictions.

Conjecture A (Conjecture 5.3.3). *As K varies over cyclic cubic number fields, the probability that K has a totally positive system of fundamental units is approximately 3%.*

We are led to Conjecture A 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 Table 6.1.1), and the following theorem provides additional theoretical support.

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

Date: October 30, 2019.

The proof of Theorem B 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 [36, §1, p. 371], the case complementary to Theorem B.

1.2. Structural results: class groups. We now present the main structural results of this paper. Let K be an abelian number field with *odd* degree $n := [K : \mathbb{Q}]$ and Galois group $G_K := \text{Gal}(K | \mathbb{Q})$. Then K is totally real, and the class group $\text{Cl}(K)$, the narrow class group $\text{Cl}^+(K)$, and the ray class group $\text{Cl}_4(K)$ of conductor 4 are $\mathbb{Z}[G_K]$ -modules.

Every irreducible $\mathbb{F}_2[G_K]$ -module is isomorphic to $\mathbb{F}_2(\chi)$, the value field of a $\overline{\mathbb{F}}_2$ -character $\chi: G_K \rightarrow \overline{\mathbb{F}}_2^\times$ taking values in a (fixed) algebraic closure $\overline{\mathbb{F}}_2$ of \mathbb{F}_2 . For a finitely generated $\mathbb{Z}[G_K]$ -module M , write $\text{rk}_\chi M$ for the multiplicity of the irreducible module $\mathbb{F}_2(\chi)$ in the $\mathbb{F}_2[G_K]$ -module M/M^2 , and let $\text{rk}_2 M := \dim_{\mathbb{F}_2} M/M^2$. In addition, we define:

$$\begin{aligned} k_\chi^+(K) &:= \text{rk}_\chi \text{Cl}^+(K) - \text{rk}_\chi \text{Cl}(K); \\ k_{4,\chi}(K) &:= \text{rk}_\chi \text{Cl}_4(K) - \text{rk}_\chi \text{Cl}(K); \\ \rho_\chi(K) &:= \text{rk}_\chi \text{Cl}(K); \end{aligned} \tag{1.2.1}$$

When K is clear from context, we suppress it from the notation. For any $\overline{\mathbb{F}}_2$ -character χ of G_K , there is a noncanonical isomorphism $\text{Hom}_{\mathbb{F}_2[G_K]}(\mathbb{F}_2(\chi), \mathbb{F}_2) \simeq \mathbb{F}_2(\chi^{-1})$ (see Lemma 3.3.3 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 $\mathbb{F}_2[G_K]$ -modules.

By an investigation of the $\mathbb{F}_2[G_K]$ -module structure of class groups, Selmer groups, and signature spaces associated to K , we prove a refined Spiegelungssatz or *reflection theorem* as in Leopoldt [24] for $p = 2$, as follows.

Theorem C (Corollary 4.1.7, Theorem 4.2.1). *Let K be an abelian number field of odd degree with Galois group G_K , and let χ be an $\overline{\mathbb{F}}_2$ -character of G_K . Then we have*

$$|\text{rk}_\chi \text{Cl}(K) - \text{rk}_{\chi^*} \text{Cl}(K)| \leq 1. \tag{1.2.2}$$

Moreover, with notation as in (1.2.1), the following statements hold.

- (a) If χ is self-dual, then $k_\chi^+ (= k_{\chi^*}^+) = 0$, i.e., $\text{rk}_\chi \text{Cl}^+(K) = \text{rk}_\chi \text{Cl}(K)$.
- (b) If χ is not self-dual, then exactly one of the following possibilities occurs:
 - (i) $\rho_\chi = \rho_{\chi^*} + 1$, in which case $(k_\chi^+, k_{\chi^*}^+) = (0, 1)$;
 - (i') $\rho_\chi = \rho_{\chi^*} - 1$, in which case $(k_\chi^+, k_{\chi^*}^+) = (1, 0)$; or
 - (ii) $\rho_\chi = \rho_{\chi^*}$, in which case $|k_\chi^+ + k_{\chi^*}^+| \leq 1$.

Finally, the same conclusions hold with k_χ^+ replaced by $k_{4,\chi}$ and $k_{\chi^*}^+$ replaced by k_{4,χ^*} throughout.

A precursor to Theorem C is the theorem of Armitage–Fröhlich [1], generalized by Taylor [35] and Oriat [30, 31]. Gras then proved a very general reflection principle [21, Théorème 5.18] explained in his book [22, Theorem 5.4.5]; however, certain corollaries for $p = 2$ [22, Corollaries 5.4.6(ii), 5.4.9] are incorrect: case (b)(ii) of Theorem C, the only situation in which $k_\chi^+(K)$ and $k_{\chi^*}^+(K)$ are not uniquely determined, does not appear. Our statement is optimal in the sense that all possibilities occur (see Example 5.4.1), and our proof is

self-contained and transparent: the cases arise from the possible intersections of a totally isotropic subspace with the coordinate subspaces in the 2-Selmer signature space.

In light of (1.2.2), one may wonder if a similar bound holds for narrow class groups of abelian number fields of odd degree. This is answered in the affirmative by the following result.

Theorem D (Theorem 4.2.6). *Let K be an abelian number field of odd degree with Galois group G_K . If χ is a $\overline{\mathbb{F}}_2$ -character, then we have*

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

as well as $|\mathrm{rk}_\chi \mathrm{Cl}_4(K) - \mathrm{rk}_{\chi^*} \mathrm{Cl}_4(K)| \leq 1$.

Our structural results on class groups recover several classical results from the literature, which we now recall. Let m be the exponent of the Galois group G_K . If $-1 \in \langle 2 \rangle \leq (\mathbb{Z}/m\mathbb{Z})^\times$ then every $\mathbb{F}_2[G_K]$ -module is self-dual; therefore Theorem C(a) implies that

$$\mathrm{Cl}^+(K)[2] \simeq \mathrm{Cl}(K)[2] \simeq \mathrm{Cl}_4(K)[2] \tag{1.2.3}$$

as $\mathbb{F}_2[G_K]$ -modules. The first isomorphism in (1.2.3) can be derived from work of Taylor [35]; it was proven by Oriat [31, Corollaire 2c], reproven by Edgar–Mollin–Peterson [16, Theorem 2.5], appears in a survey by Lemmermeyer [25, Theorem 7.2], and it is generalized by the reflection principle of Gras [21, Théorème 5.18] (see also Theorem 3.2.4). Most notably, this applies when K is a cyclic number field of prime degree ℓ where 2 is a primitive root modulo ℓ . The next simplest case is treated by the following corollary.

Corollary E (Corollary 4.2.4). *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 5.1.2 (see also (1.4.2)).

1.3. Structural results: units. We retain the same notation: K is an abelian number field of odd degree n with Galois group G_K . Let \mathcal{O}_K be the ring of integers of K . Define the archimedean signature map $\mathrm{sgn}_\infty: K^\times \rightarrow \prod_{v|\infty} \{\pm 1\} \simeq \mathbb{F}_2^n$ as the surjective group homomorphism recording the signs of elements of K^\times under each real embedding; its kernel $K_{>0}^\times := \ker(\mathrm{sgn}_\infty)$ is the group of totally positive elements of K . Let $\mathcal{O}_{K,>0}^\times := \mathcal{O}_K^\times \cap K_{>0}^\times$ denote the group of totally positive units. Define

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

and the unit signature rank of K

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

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.

Theorem F (Theorem 4.3.2). *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 . With the notation (1.2.1), the following statements hold.*

- (a) *If $k_\chi^+(K) = 1$, then $\text{sgnrk}_\chi(\mathcal{O}_K^\times) = 0$.*
- (b) *If $k_\chi^+(K) = 0$, then $1 - \rho_\chi(K) \leq \text{sgnrk}_\chi(\mathcal{O}_K^\times) \leq 1$.*

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

Corollary G (Corollary 4.3.4). *Let K be a cyclic number field of odd prime degree ℓ , and let f be the order of 2 modulo ℓ . Then*

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

and the following statements hold.

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

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

1.4. Heuristics. Having established many cases where the structure is fixed, we turn to the remaining cases: we propose a model for the 2-part of the narrow class group and for unit signature ranks for abelian number fields of odd degree. Our approach follows Dummit–Voight [15], but we take care of the Galois module structure. The compatibility of Leopoldt’s Spiegelungssatz and the Cohen–Lenstra heuristics for p -ranks of class groups have been analyzed for $p > 2$ by Lee [23]; here, we consider the more delicate behavior at $p = 2$, taking into consideration that the second roots of unity are contained in every number field (but no odd-degree number field contains the 4th roots of unity).

Let G be a finite abelian group of odd order and let χ be an $\overline{\mathbb{F}}_2$ -character of G . A *G -number field* is a number field K , inside a fixed algebraic closure of \mathbb{Q} , that is normal over \mathbb{Q} and that is equipped with an isomorphism $\text{Gal}(K|\mathbb{Q}) \simeq G$. For the conjectures in this section, we sidestep the issue of ordering fields: we expect that any *fair* counting function in the terminology of Wood [37] should be allowed, for example ordering by conductor or by the norm of the product of ramified primes.

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 H (Conjecture 5.1.1). *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 in the notation of (1.2.1), as K varies over G -number fields satisfying $\text{rk}_\chi \text{Cl}(K) = \text{rk}_{\chi^*} \text{Cl}(K)$,*

$$\text{Prob}(k_\chi^+(K) + k_{\chi^*}^+(K) = 0) = \frac{q-1}{q+1}. \tag{1.4.1}$$

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 $\text{Cl}(K)[2]$ is self-dual, we predict in Conjecture 5.1.2

that

$$\text{Prob}(\text{Cl}^+(K)[2] \simeq \text{Cl}(K)[2]) = \frac{2^{\frac{\ell-1}{2}} - 1}{2^{\frac{\ell-1}{2}} + 1}. \quad (1.4.2)$$

We further expect that the probability in Conjecture [H](#) remains the same in certain natural subfamilies, such as when we fix the value $\rho_\chi(K) = \rho_{\chi^*}(K) = r$. In particular, among cyclic septic number fields of odd class number, we conjecture that $\text{Cl}(K)[2] \simeq \text{Cl}^+(K)[2]$ with probability $\frac{7}{9}$.

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 I (Conjecture [5.2.4](#)). *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,*

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

for $0 \leq s \leq m$.

Second, we consider the situation when $\ell = 3$ or 5 with no additional assumption on the class number. In this case, Corollary [4.3.4](#)(b) implies that $\text{sgnrk}(\mathcal{O}_K^\times) = 1$ or ℓ . Although complete heuristics for the 2-part of the class group over abelian fields are not known, Malle [[28](#)] provides results in the case that $\ell = 3$ or 5 . We use the following notation: for $m \in \mathbb{Z}_{\geq 0} \cup \{\infty\}$ 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 J (Conjecture [5.3.3](#)). *Let $\ell = 3$ or 5 and $q = 2^{\ell-1}$. As K varies over cyclic number fields of degree ℓ , then*

$$\text{Prob}(\text{sgnrk}(\mathcal{O}_K^\times) = 1) = \left(1 + \frac{1}{\sqrt{q}}\right) \frac{(\sqrt{q})_\infty (q^2)_\infty}{(q)_\infty^2} \cdot \sum_{r=0}^{\infty} \frac{(\ell-1)^r}{q^{(r^2+3r)/2} \cdot (q)_r} \cdot \frac{q^r - 1}{q^{r+1} - 1}. \quad (1.4.3)$$

Estimating the quantity in [\(1.4.3\)](#), we predict that approximately 3% of cyclic cubic fields have $\text{sgnrk}(\mathcal{O}_K^\times) = 1$ which yields Conjecture [A](#). For cyclic quintic fields we predict that this proportion drops to below 0.1%. We expect that as $\ell \rightarrow \infty$ varies over odd primes, the probability $\text{Prob}(\text{sgnrk}(\mathcal{O}_K^\times) = 1) \rightarrow 0\%$, and we plan to give evidence to support this limiting behavior in the future (see also Remark [6.2.3](#)).

Remark 1.4.4. 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 [[28](#), [29](#)] to predict the distribution of ρ_χ . This distribution will depend on the representation theory of $\mathbb{Z}/\ell\mathbb{Z}$ (or more generally, of G); in particular, the constraint in Theorem [C](#) 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.

1.5. Outline. In section 2, we set up basic notation and background. In section 3, we study these objects as Galois modules over \mathbb{F}_2 , and in section 4, we determine the fixed structure of class groups and narrow class groups in order to prove Theorems C and F. In section 5 we introduce our heuristic assumptions and present our conjectures, including details on the low-degree cases. In section 6, we carry out computations that provide some experimental evidence for our conjectures. Finally, in appendix A we prove Theorem B.

1.6. Acknowledgements. The authors would like to thank Edgar Costa, David Dummit, Noam Elkies, Georges Gras, Brendan Hassett, Hershy Kisilevsky, Arul Shankar, Jared Weinstein, and Melanie Matchett Wood for comments, and Tommy Hofmann for sharing his list of cyclic septic fields. 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 an 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 $\#A[p] = p^{\mathrm{rk}_p(A)}$.

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

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

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 we let

$$(-, -)_v : K_v^\times \times K_v^\times \rightarrow \{\pm 1\}$$

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

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

Following Dummit-Voight [15, 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

$$V_\infty(K) := \bigoplus_{v \text{ real}} \{\pm 1\}$$

where the direct sum runs over all real places of K , and the archimedean signature map is

$$\begin{aligned} \text{sgn}_\infty: K^\times &\rightarrow V_\infty(K) \\ \alpha &\mapsto \bigoplus_{v \text{ real}} \frac{v(\alpha)}{|v(\alpha)|}. \end{aligned}$$

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

$$b_\infty: V_\infty(K) \times V_\infty(K) \rightarrow \{\pm 1\}$$

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

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

The 2-adic signature map is the map

$$\text{sgn}_2: \mathcal{O}_{K,(2)}^\times \rightarrow V_2(K)$$

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

For the following statements we refer to Dummit–Voight [15, §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

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

which is a nondegenerate, symmetric \mathbb{F}_2 -bilinear form on $V_2(K)$. Every class in $\text{Sel}_2(K)$ 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 $\varphi_{K,2}: \text{Sel}_2(K) \rightarrow V_2(K)$.

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

$$\varphi_K := \varphi_{K,\infty} \perp \varphi_{K,2}: \text{Sel}_2(K) \rightarrow V(K).$$

Theorem 2.2.3 (Dummit–Voight [15, 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 $\text{Cl}(K)$, its narrow class group is denoted by $\text{Cl}^+(K)$, and its ray class group of conductor 4 by $\text{Cl}_4(K)$.

Definition 2.2.4. The archimedean isotropy rank of a number field K is

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

and the 2-adic isotropy rank of K is

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

By Dummit–Voight [15, Theorem 6.1], we have

$$k^+(K) = \dim_{\mathbb{F}_2} \text{img}(\varphi_{K,\infty})$$

$$k_4(K) = \dim_{\mathbb{F}_2} \text{img}(\varphi_{K,2})$$

hence the nomenclature given in Definition 2.2.4. Moreover, there is a classical equality

$$k_4(K) = k^+(K) + r_2 \tag{2.2.5}$$

(see for example, Theorem 2.2 of Lemmermeyer [25]). If K is totally real, then not only do we have that $k_4(K) = k^+(K)$, but in fact, $\text{img}(\varphi_{K,\infty})$ is isometric to $\text{img}(\varphi_{K,2})$ by Dummit–Foote–Voight [15, Theorem A.13].

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

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

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 $\text{Gal}(H|K) \simeq \text{Cl}(K)$; let $H^{(2)}$ denote the fixed field of the subgroup $\text{Cl}(K)^2$. The Kummer pairing

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

is (well-defined and) perfect [15, (3.11)]. The Artin reciprocity map provides a canonical isomorphism $\text{Gal}(H^{(2)}|K) \simeq \text{Cl}(K)/\text{Cl}(K)^2$ and so we can rewrite the above map instead as

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

The pairing (2.3.2) is the first of four perfect pairings [15, Lemma 3.10] (see also Lemmermeyer [25, Theorem 6.3]); the other three perfect pairings are

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

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

3. GALOIS MODULE STRUCTURE FOR INVARIANTS OF ODD GALOIS NUMBER FIELDS

We next study the Galois module structure on the arithmetic objects introduced in the previous section. Our results overlap substantially with those of Taylor [35].

From now on, suppose that K is Galois over \mathbb{Q} of *odd* degree n , with Galois group $G_K := \text{Gal}(K | \mathbb{Q})$. Hence, K is totally real, and the only roots of unity in K are ± 1 .

3.1. Basic invariants. We work throughout with left $\mathbb{F}_2[G_K]$ -modules, and since $\#G_K$ is odd, this is a semisimple category. We quickly prove two standard lemmas, for completeness.

Lemma 3.1.1. *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

$$(\mathcal{O}_K^\times / \{\pm 1\} \otimes_{\mathbb{Z}} \mathbb{Z}_{(2)}) \oplus \mathbb{Z}_{(2)} \simeq \mathbb{Z}_{(2)}[G_K] \quad (3.1.2)$$

as $\mathbb{Z}_{(2)}$ -modules; tensoring (3.1.2) with $\mathbb{Z}/2\mathbb{Z}$ and using that $\{\pm 1\}$ has trivial action gives

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

Corollary 3.1.3. *We have $\text{Sel}_2(K) \simeq \mathbb{F}_2[G_K] \oplus \text{Cl}(K)[2]$ 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 3.1.1. \square

Lemma 3.1.4. *For any odd Galois number field K , the G_K -invariant subspace of each of the $\mathbb{F}_2[G_K]$ -modules $\text{Cl}(K)[2]$, $\text{Cl}^+(K)[2]$ and $\text{Cl}_4(K)[2]$ is trivial.*

Proof. Let $\text{Cl}(\mathbb{Q}, m)$ be a ray class group of \mathbb{Q} of conductor m , and let $\text{Cl}(K, m)$ be the ray class group of K of the same conductor. The norm map induces a group homomorphism $\text{Cl}(K, m)[2] \rightarrow \text{Cl}(\mathbb{Q}, m)[2]$ which is injective on G_K -invariants, because if $[\mathfrak{a}] \in \text{Cl}(K, m)[2]$ is G_K -invariant then $[\text{Nm}(\mathfrak{a})] = [\mathfrak{a}]^n = [1]$ but also $[\mathfrak{a}]^2 = [1]$ so $[\mathfrak{a}] = [1]$. Since $\text{Cl}(\mathbb{Q}, m)$ is trivial when $m = 1, 4$, and ∞ , the result follows immediately. \square

We now turn to the signature spaces. Recall that a \mathbb{F}_2 -bilinear form $b: V \times V \rightarrow \mathbb{F}_2$ 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 3.1.5. *We have $V_\infty(K) \simeq V_2(K) \simeq \mathbb{F}_2[G_K]$ as $\mathbb{F}_2[G_K]$ -modules, and the bilinear forms b_∞ and b_2 are G_K -invariant.*

Proof. We begin with $V_\infty(K)$ and b_∞ . 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 $V_2(K)$ and b_2 , we follow the proof in Dummit–Voight [15, Proposition 4.4]. The map

$$\begin{aligned} \mathcal{O}_{K,(2)} &\rightarrow V_2(K) \\ a &\mapsto 1 + 2a \end{aligned}$$

induces an isomorphism of groups

$$\mathcal{O}_{K,(2)}/2\mathcal{O}_{K,(2)} \simeq V_2(K).$$

This map is visibly G_K -equivariant. Since $n = [K : \mathbb{Q}]$ is odd, K is at most tamely ramified at the primes above 2; therefore, $\mathcal{O}_{K,(2)} \simeq \mathbb{Z}_{(2)}[G_K]$ by Noether's theorem [20, Theorem 3], and so $\mathcal{O}_{K,2}/2\mathcal{O}_{K,2} \simeq \mathbb{F}_2[G_K]$ as $\mathbb{F}_2[G_K]$ -modules.

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 $D_v := \text{Aut}(K_v)$ 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 3.1.6. *The 2-Selmer signature map φ_K is G_K -equivariant.*

Proof. Let $\text{sgn}(x) := x/|x| \in \{\pm 1\}$ for $x \in \mathbb{R}^\times$. Then

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

Hence, 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 3.1.7. *For any odd 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 2.2.3 with Proposition 3.1.5 and Lemma 3.1.6. □

3.2. Duals and pairings. We now treat some issues of duality, including an application to the Kummer pairing and the proof of our first result.

Let G be a finite group of odd cardinality 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

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

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

$$e: V^\vee \times V \rightarrow \mathbb{F}_2$$

$$e(f, x) = f(x)$$

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

Lemma 3.2.2. *Let $b: V \times V \rightarrow \mathbb{F}_2$ be a G -invariant \mathbb{F}_2 -bilinear form, and let $W, W' \subseteq V$ be irreducible $\mathbb{F}_2[G]$ -modules. If $W^\vee \not\cong W'$ as $\mathbb{F}_2[G]$ -modules, then $b(W, W') = \{0\}$.*

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

Lemma 3.2.2, although easy to prove, is fundamental in what follows: it shows that a decomposition of V into irreducibles is already *almost* an orthogonal decomposition.

We now proceed with our two applications.

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

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

The right-most isomorphism in each line is canonical.

Proof. We work with the first line, the others follow by the same argument. Applying the Artin map, we rewrite the Kummer pairing (2.3.2) as

$$\begin{aligned} \mathrm{Cl}(K)/\mathrm{Cl}(K)^2 \times \ker(\varphi_K) &\rightarrow \{\pm 1\} \\ ([\mathfrak{a}], [\alpha]) &= \left(\frac{\alpha}{\mathfrak{a}} \right), \end{aligned}$$

where $\mathfrak{a} \subseteq \mathcal{O}_K$ is an ideal of odd norm (which may be chosen to be prime by the Chebotarev density theorem), $\alpha \in (\mathcal{O}_K/\mathfrak{a})^\times$, and $\left(\frac{\alpha}{\mathfrak{a}} \right)$ is the Jacobi symbol. This pairing is G_K -equivariant, because for $\sigma \in G_K$ we have

$$\left(\frac{\sigma(\alpha)}{\sigma(\mathfrak{a})} \right) = \left(\frac{\alpha}{\mathfrak{a}} \right);$$

duality then gives the right-most isomorphism (3.2.3).

For the left-most (noncanonical) isomorphism, we use a general fact: if M is a torsion $\mathbb{Z}_{(2)}[G_K]$ -module, then there is a (noncanonical) isomorphism $M/M^2 \xrightarrow{\sim} M[2]$. To prove this, after decomposing M into irreducibles, we may suppose M is cyclic generated as an $\mathbb{Z}_{(2)}[G_K]$ -module by x of (necessarily even) order m and we map $x \mapsto x^{m/2} \in M[2]$; this map is surjective with kernel $M/2M$ and is visibly G_K -equivariant. \square

Theorem 3.2.4. *If K is a Galois number field of odd degree and $G_K = \mathrm{Gal}(K | \mathbb{Q})$, then as $\mathbb{F}_2[G_K]$ -modules*

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

As mentioned in the introduction, Theorem 3.2.4 follows as a special case of the reflection theorem of Gras [21, Théorème 5.18]; to be self-contained, and as it illustrates aspects of our approach, we give a short proof here.

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

Our proof considers the analogue for $\text{Sel}_2^+(K)$ 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 $K^\times \rightarrow P_K$ sending $\alpha \mapsto (\alpha)$ is surjective and G_K -equivariant with kernel \mathcal{O}_K^\times ; it induces the exact sequence

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

Since $K^\times / K_{>0}^\times \simeq \mathbb{F}_2[G_K]$ (counting idempotents, or as in Lemma 3.1.1), we obtain a canonical isomorphism of $\mathbb{F}_2[G_K]$ -modules

$$\mathbb{F}_2[G_K] \simeq (\mathcal{O}_K^\times / \mathcal{O}_{K,>0}^\times) \oplus (P_K / P_{K,>0}). \quad (3.2.5)$$

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

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

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

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

giving the isomorphism

$$P_K / P_{K,>0} \oplus \text{Sel}_2^+(K) \simeq \mathcal{O}_{K,>0}^\times / \mathcal{O}_K^{\times 2} \oplus \text{Cl}^+(K)[2]. \quad (3.2.6)$$

Adding $\mathcal{O}_K^\times / \mathcal{O}_{K,>0}^\times$ to both sides of (3.2.6), and using (3.2.5) and Lemma 3.1.1 we conclude

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

and cancelling gives the result. \square

3.3. Abelian Galois groups. From now on, we specialize further and suppose that the odd-order group G is *abelian*.

Denote $\overline{\mathbb{F}}_2$ as a (fixed) algebraic closure of \mathbb{F}_2 . As sketched in the introduction, the irreducible $\mathbb{F}_2[G]$ -modules are of the form $\mathbb{F}_2(\chi)$, where $\chi: G \rightarrow \overline{\mathbb{F}}_2^\times$ is a group homomorphism and $\mathbb{F}_2(\chi) \subseteq \overline{\mathbb{F}}_2$ is the subfield generated by the values of χ ; we call χ an $\overline{\mathbb{F}}_2$ -character of G . Note that $\sigma \in G$ acts on $\mathbb{F}_2(\chi)$ via multiplication by $\chi(\sigma)$; hence, $\mathbb{F}_2(\chi)$ is cyclic and generated by 1 as an $\mathbb{F}_2[G]$ -module. Furthermore, 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.

By character theory, two such modules $\mathbb{F}_2(\chi)$ and $\mathbb{F}_2(\chi')$ are isomorphic if and only if there exists $\psi \in \text{Gal}(\overline{\mathbb{F}}_2 | \mathbb{F}_2)$ 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, $\text{Aut}_{\mathbb{F}_2[G]}(\mathbb{F}_2(\chi)) \simeq \mathbb{F}_2(\chi)^\times$.

Theorem 3.3.1. *Let K be a cyclic number field of odd prime degree ℓ , and let f denote the order of 2 modulo ℓ . Then f divides each of $\text{rk}_2 \text{Cl}(K)$, $\text{rk}_2 \text{Cl}^+(K)$, and $\text{rk}_2 \text{Cl}_4(K)$.*

Proof. Combine Lemma 3.1.4 with the decomposition into irreducibles given in Example 3.3.6. \square

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 $*$: $\mathbb{F}_2[G] \rightarrow \mathbb{F}_2[G]$. 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 motivates the notation $\chi^* = \chi^{-1}$ from the introduction.

Remark 3.3.2. 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 3.3.3. *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

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

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

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

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

Lemma 3.3.4. *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 the order of χ be denoted by d . Since necessarily, $m \mid d$, 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 $k \in \mathbb{Z}$. The result follows. \square

Example 3.3.5. 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 3.3.6. 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 ℓ th 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.

3.4. The canonical orthogonal decomposition. 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 $V_{\chi^\pm} := V_\chi + V_{\chi^*}$ 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 3.4.1. 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, \mathbb{F}_2 -bilinear form, then by Lemma 3.2.2 the decomposition into the spaces V_{χ^\pm} is orthogonal, so we have a canonical decomposition as $\mathbb{F}_2[G]$ -modules

$$V = \bigsqcup_{\chi} V_{\chi^\pm}, \quad (3.4.2)$$

where the orthogonal direct sum is indexed by characters χ taken up to isomorphism and inverses. We call the decomposition given in (3.4.2) the **canonical orthogonal decomposition** of V .

Let V be a finitely generated $\mathbb{F}_2[G]$ -module equipped with a G -invariant, symmetric, non-degenerate, \mathbb{F}_2 -bilinear form, and consider its canonical orthogonal decomposition as given in (3.4.2). Let $W \subseteq V$ be a G -invariant subspace; then $W_{\chi^\pm} \subseteq V_{\chi^\pm}$. In particular, we can often reduce without loss of generality to the components of the canonical orthogonal decomposition.

Theorem 3.4.3. *If G is 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*

$$b : \mathbb{F}_2[G] \times \mathbb{F}_2[G] \rightarrow \mathbb{F}_2 \\ (x, y) \mapsto \text{Tr}(x^*y).$$

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

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

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

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

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

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

To show every such form arises as claimed, by the orthogonal decomposition (3.4.2) 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 $b'(x, y) = b(\nu x, y) = \text{Tr}(\nu x^*y)$. Since b' is symmetric, we have $\text{Tr}(\nu x^*y) = \text{Tr}(\nu^*y^*x) = \text{Tr}(\nu y^*x)$, so by nondegeneracy we must 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. \square

Example 3.4.4. As this will be central to our investigation, we write down explicitly the pairing in Theorem 3.4.3 restricted to orthogonal components as in (3.4.2).

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 $b(1, 1) = \text{Tr}(1) = 1$ 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 d th root of unity. Then an \mathbb{F}_2 -basis for $\mathbb{F}_2(\chi)$ is given by $\zeta, \zeta^2, \dots, \zeta^{2^{f-1}}$ where f is the order of 2 in $(\mathbb{Z}/d\mathbb{Z})^\times$. Since $\text{Tr}(1) = 0$ (as f is even), we have $b(\zeta^{2^k}, \zeta^{2^k}) = \text{Tr}(1) = 0$ for all k , so by linearity we conclude that b is alternating. (We also observe $\text{Tr}(\zeta) = \text{Tr}(\zeta^{2^k}) = 1$ 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) induces a natural pairing on $\mathbb{F}_2(\chi)^\vee \oplus \mathbb{F}_2(\chi)$, which can be described explicitly as

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

4. STRUCTURAL RESULTS

In this section, we apply the general observations of the previous section to prove the main structural results of the paper, first for class groups and then for unit signatures.

As before, we retain the notation and hypotheses from the previous section; in particular, K is a Galois number field of odd degree with abelian Galois group $G_K = \text{Gal}(K | \mathbb{Q})$.

4.1. Maximal totally isotropic subspaces. The image

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

of the 2-Selmer group under the signature map is a G_K -invariant maximal totally isotropic subspace of $V_\infty \boxplus V_2$ by Corollary 3.1.7. By the canonical orthogonal decomposition (3.4.2),

$$S(K) = \bigsqcup_{\chi} S(K)_{\chi^\pm}, \tag{4.1.1}$$

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

Definition 4.1.2. The archimedean χ -isotropy rank of K is

$$k_\chi^+(K) := \text{rk}_\chi \text{Cl}^+(K) - \text{rk}_\chi \text{Cl}(K).$$

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

$$k_{4,\chi}(K) := \text{rk}_\chi \text{Cl}_4^+(K) - \text{rk}_\chi \text{Cl}(K).$$

Lemma 4.1.3. *For an $\overline{\mathbb{F}}_2$ -character χ of G_K , we have*

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

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 $\text{Cl}^+(K)[2]$ and $\text{Cl}(K)[2]$ by Lemma 3.2.3, we have

$$\text{rk}_{\chi^*}(S(K) \cap V_\infty(K)) = \text{rk}_\chi \text{Cl}^+(K) - \text{rk}_\chi \text{Cl}(K).$$

The second equality follows similarly. \square

Summing contributions from each irreducible $\mathbb{F}_2[G_K]$ -module and recalling (2.2.5), we have

$$\sum_\chi k_\chi^+(K) \cdot [\mathbb{F}_2(\chi) : \mathbb{F}_2] = k^+(K) = k_4(K) = \sum_\chi k_{4,\chi}(K) \cdot [\mathbb{F}_2(\chi) : \mathbb{F}_2],$$

where χ runs over isomorphism classes of $\overline{\mathbb{F}}_2$ -characters of G_K . However, this *does not* imply that $k_\chi^+(K) = k_{4,\chi}(K)$. Instead, we have the following proposition.

Proposition 4.1.4. *For any $\overline{\mathbb{F}}_2$ -character χ of G_K ,*

$$k_\chi^+(K) + k_{\chi^*}^+(K) = k_{4,\chi}(K) + k_{4,\chi^*}(K).$$

Proof. This follows from Theorem 3.2.4 in conjunction with (3.4.2) and the fact that $S(K)_{\chi^\pm}$ is a maximal totally isotropic subspace. \square

Theorem 4.1.5. *Let K be an abelian number field of odd degree with Galois group G_K , and let χ be an $\overline{\mathbb{F}}_2$ -character of G_K . Then the following statements hold.*

- (a) *If χ is self-dual, then $S \subseteq V(K)_\chi$ is a G_K -invariant maximal totally isotropic subspace if and only if $S \simeq \mathbb{F}_2(\chi)$ and $S \cap V_\infty(K) = \{0\}$. There are $q - 1$ such subspaces, all in the same G_K -equivariant isometry class.*
- (b) *Suppose that χ is not self-dual, and let $q := \#\mathbb{F}_2(\chi)$. Then there are exactly $q + 3$ distinct G_K -invariant maximal totally isotropic subspaces $S \subseteq V(K)_{\chi^\pm}$:*
 - (i) $S = V_\infty(K)_\chi \oplus V_2(K)_\chi \simeq \mathbb{F}_2(\chi)^2$, where $S \cap V_\infty(K) \simeq \mathbb{F}_2(\chi)$.
 - (i') $S = V_\infty(K)_{\chi^*} \oplus V_2(K)_{\chi^*} \simeq \mathbb{F}_2(\chi^*)^2$, where $S \cap V_\infty(K) \simeq \mathbb{F}_2(\chi^*)$.
 - (ii) $S = V_\infty(K)_\chi \oplus V_2(K)_{\chi^*} \simeq \mathbb{F}_2(\chi) \oplus \mathbb{F}_2(\chi^*)$, where $S \cap V_\infty(K) \simeq \mathbb{F}_2(\chi)$.
 - (ii') $S = V_\infty(K)_{\chi^*} \oplus V_2(K)_\chi \simeq \mathbb{F}_2(\chi) \oplus \mathbb{F}_2(\chi^*)$, where $S \cap V_\infty(K) \simeq \mathbb{F}_2(\chi^*)$.
 - (iii) $S \simeq \mathbb{F}_2(\chi) \oplus \mathbb{F}_2(\chi^*)$ and $S \cap V_\infty(K) = \{0\}$; there are exactly $q - 1$ such subspaces, all in the same G_K -equivariant isometry class.

Proof. For (a), we have $V(K)_{\chi^\pm} \simeq V_\infty(K)_\chi \boxplus V_2(K)_\chi \simeq \mathbb{F}_2(\chi)^2$, equipped with the unique (restricted) nondegenerate, symmetric, G_K -invariant bilinear forms $b_{\infty,\chi}, b_{2,\chi}$ (see Example 3.4.4), so under the above identification we have $b_{\infty,\chi} = b_{2,\chi}$. A subspace is G_K -invariant if and only if it is an $\mathbb{F}_2(\chi)$ -subspace, and the G_K -equivariant isometry group is $\text{Isom}_{G_K}(V_\chi, b_\chi) \simeq \mathbb{F}_2(\chi)^\times \times \mathbb{F}_2(\chi)^\times$ (acting coordinatewise). For (\Rightarrow) , if $S \subseteq V(K)_\chi$ is totally isotropic and $S \cap V_\infty(K) \neq \{0\}$ then by dimensions $S = V_\infty(K)$, but the bilinear

form b_∞ on V_∞ is nondegenerate, a contradiction. For (\Leftarrow) , if $S \cap V_\infty(K) = \{0\}$ then $S = \mathbb{F}_2(\chi)(1, \nu) \in \mathbb{F}_2(\chi)^2$ and for all $\mu \in \mathbb{F}_2(\chi)^\times$ we have

$$\begin{aligned} b_\chi((1, \nu), \mu(1, \nu)) &= b_\chi((1, \nu), (\mu, \mu\nu)) = b_{\infty, \chi}(1, \mu) + b_{2, \chi}(\nu, \mu\nu) \\ &= b_{\infty, \chi}(1, \mu) + b_{2, \chi}(1, \mu) = 0 \end{aligned}$$

so S is totally isotropic.

We now proceed with part (b): we have

$$V(K)_{\chi^\pm} \simeq V_\infty(K)_{\chi^\pm} \boxplus V_2(K)_{\chi^\pm} \simeq \mathbb{F}_2(\chi)^2 \oplus \mathbb{F}_2(\chi^*)^2$$

and the bilinear form b_{χ^\pm} obtained by restricting b . Let $S \subseteq V(K)_{\chi^\pm}$ be a G_K -invariant, maximal totally isotropic subspace. Since S has half of the \mathbb{F}_2 -dimension of the bilinear space, as an $\mathbb{F}_2[G_K]$ -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 the only option is $S = V(K)_\chi$ which is totally isotropic since the restriction b_χ of b to $V(K)_\chi$ is identically zero by Lemma 3.2.2. Similarly for $S \simeq \mathbb{F}_2(\chi^*)^2$; this handles cases (i)-(i').

What remains is to consider the possibilities for $S \simeq \mathbb{F}_2(\chi) \oplus \mathbb{F}_2(\chi^*)$. First we give a construction. Let $S_\chi \subseteq V(K)_\chi$ have $S_\chi \simeq \mathbb{F}_2(\chi)$ (i.e., χ -rank 1). Given S_χ , let $S_{\chi^*} := S_\chi^\perp \cap V(K)_{\chi^*}$, i.e.,

$$S_{\chi^*} := \{y \in V(K)_{\chi^*} : b(x, y) = 0 \text{ for all } x \in S_\chi\} \quad (4.1.6)$$

and let $S := S_\chi \oplus S_{\chi^*}$. Then S is totally isotropic by construction, recalling again that $b_\chi = b_{\chi^*} = 0$; and S is G_K -stable, as $b(x, \sigma y) = b(\sigma^{-1}x, y) = 0$ since S_χ is G_K -stable. Finally, S is maximal by dimensions: since S_χ has rank 1 and $V(K)_{\chi^*}$ has rank 2, the subspace S_{χ^*} has rank 1. Conversely, if $S \subseteq V(K)_\chi$ is maximal totally isotropic of the given type, then S has isotypic parts $S = S_\chi \oplus S_{\chi^*}$ and by maximality S_{χ^*} arises as in (4.1.6). The maximal isotropic subspaces of this form are indexed by $S_\chi \subseteq V(K)_\chi$, so total $\#\mathbb{P}^1(\mathbb{F}_2(\chi)) = q + 1$. There are two distinguished coordinate subspaces as in (ii) and (ii'); the remaining $q - 1$ subspaces yield (iii) and are all G_K -equivariant by the same argument as in part (a). \square

The following corollary is the cornerstone result of Taylor [35], and Theorem 4.1.5 can be viewed as a precise refinement.

Corollary 4.1.7 (Taylor [35, (*)]). *For an abelian Galois number field K such that G_K is odd, 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. Again, this is immediate from the classification in Theorem 4.1.5. \square

Another corollary we obtain is the following result, proven by Oriat [31].

Corollary 4.1.8 (Oriat [31, 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 $\text{Cl}^+(K)[2] \simeq \text{Cl}(K)[2]$ as $\mathbb{F}_2[G_K]$ -modules.*

Proof. By Lemma 3.3.4, every $\mathbb{F}_2[G]$ -module is self-dual so the conclusion of Corollary 4.1.7 implies that $k^+(K) = 0 = k_4(K)$ in the notation of Definition 2.2.4. \square

Example 4.1.9. 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 $\text{rk}_2 \text{Cl}(K) = \text{rk}_2 \text{Cl}^+(K)$ by Corollary 4.1.8.

Example 4.1.10. More generally, if 2 has even order modulo ℓ , then Corollary 4.1.8 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 4.1.11. Corollary 4.1.8 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 4.1.8 implies that $\text{rk}_2 \text{Cl}(K) = \text{rk}_2 \text{Cl}^+(K)$.

Remark 4.1.12. Edgar–Mollin–Peterson [16, Theorem 2.5] reprove Corollary 4.1.8, 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 [25, 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 $\text{Cl}(K)$ is trivial and $\text{Cl}^+(K) \simeq (\mathbb{Z}/2\mathbb{Z})^6$.

4.2. The non-self-dual case. In view of the self-dual results of the previous section, we next turn to studying properties in the non-self-dual case.

Theorem 4.2.1. *Let K be an abelian number field of odd degree with Galois group G_K , and let $S(K) = \text{img } \varphi_K$ be the image of the 2-Selmer signature map for K . Let χ be an $\overline{\mathbb{F}}_2$ -character of G_K that is not self-dual. Then*

$$|\rho_\chi(K) - \rho_{\chi^*}(K)| \leq 1.$$

Moreover, as $\mathbb{F}_2[G_K]$ -modules we have:

$$\begin{aligned} S(K)_{\chi^\pm} &\simeq \mathbb{F}_2(\chi) \oplus \mathbb{F}_2(\chi^*) &\iff \rho_\chi(K) &= \rho_{\chi^*}(K); \\ S(K)_{\chi^\pm} &\simeq \mathbb{F}_2(\chi) \oplus \mathbb{F}_2(\chi) &\iff \rho_\chi(K) &= \rho_{\chi^*}(K) + 1; \text{ and} \\ S(K)_{\chi^\pm} &\simeq \mathbb{F}_2(\chi^*) \oplus \mathbb{F}_2(\chi^*) &\iff \rho_\chi(K) &= \rho_{\chi^*}(K) - 1. \end{aligned}$$

The same conclusions hold with k_χ^+ replaced by $k_{4,\chi}$ and $k_{\chi^*}^+$ replaced by k_{4,χ^*} throughout.

Proof. Since the short exact sequence in (2.3.1) splits, decomposing $\text{Sel}_2(K)$ under φ_K gives

$$\mathcal{O}_K^\times / (\mathcal{O}_K^\times)^2 \oplus \text{Cl}(K)[2] \simeq \text{Sel}_2(K) \simeq S(K) \oplus \ker(\varphi_K) \quad (4.2.2)$$

as $\mathbb{F}_2[G_K]$ -modules. By Lemma 3.1.1 and Example 3.4.1, we have

$$\text{rk}_\chi \mathcal{O}_K^\times / (\mathcal{O}_K^\times)^2 = \text{rk}_{\chi^*} \mathcal{O}_K^\times / (\mathcal{O}_K^\times)^2 = 1.$$

By Lemma 3.2.3 in conjunction with Lemma 3.3.3, we have $\text{Cl}(K)[2] \simeq \ker(\varphi_K)^*$, and so it follows that $\rho_\chi(K) = \text{rk}_\chi \text{Cl}(K)[2] = \text{rk}_{\chi^*} \ker(\varphi_K)$. Combining these observations and counting multiplicities in (4.2.2) yields:

$$\begin{aligned} 1 + \rho_\chi(K) &= \text{rk}_\chi S(K) + \rho_{\chi^*}(K) \\ 1 + \rho_{\chi^*}(K) &= \text{rk}_{\chi^*} S(K) + \rho_\chi(K) \end{aligned} \tag{4.2.3}$$

We recover $\text{rk}_\chi S(K) + \text{rk}_{\chi^*} S(K) = 2$ (this is also a consequence of the fact that $S(K)$ is a maximal totally isotropic subspace). Considering the three possibilities for the quantities $\text{rk}_\chi S(K)$ and $\text{rk}_{\chi^*} S(K)$ when plugging into (4.2.3) gives the result, and in particular, $|\rho_\chi(K) - \rho_{\chi^*}(K)| \leq 1$. \square

Corollary 4.2.4. *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 $\mathbb{F}_2(\chi) \not\cong \mathbb{F}_2(\chi^*)$.*

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

Proof. By Lemma 3.3.4, 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 3.3.6. In addition, $\text{Cl}(K)[2]$ is not self-dual if and only if $\rho_\chi(K) \neq \rho_{\chi^*}(K)$, and so the second statement follows from the two cases in Theorem 4.2.1 which correspond to Theorem 4.1.5(b)(i)-(i'). \square

More generally, we combine cases (b)(i)-(iii) in Theorem 4.1.5 with Theorem 4.2.1 to describe the relation between the maximal totally isotropic subspaces $S_{\chi^\pm}(K) \subseteq V(K)_{\chi^\pm}$ and quantities associated to the class group and narrow class group. For ease, define $\rho_\chi^+(K) := \text{rk}_\chi \text{Cl}^+(K)$, and $\rho_{4,\chi}(K) := \text{rk}_\chi \text{Cl}_4(K)$. In the following table, we work under the hypotheses of Theorem 4.1.5(b).

Case	$\mathbb{F}_2[G_K]$ -module structure		Comparison		Isotropy Ranks	
	$S(K)_{\chi^\pm}$	$S(K)_{\chi^\pm} \cap V_\infty(K)$	ρ_χ and ρ_{χ^*}	ρ_χ^+ and $\rho_{\chi^*}^+$	k_χ^+	$k_{\chi^*}^+$
(b)(i)	$\mathbb{F}_2(\chi)^2$	$\mathbb{F}_2(\chi)$	$\rho_\chi = \rho_{\chi^*} + 1$	$\rho_\chi^+ = \rho_{\chi^*}^+$	0	1
(b)(i')	$\mathbb{F}_2(\chi^*)^2$	$\mathbb{F}_2(\chi^*)$	$\rho_\chi = \rho_{\chi^*} - 1$	$\rho_\chi^+ = \rho_{\chi^*}^+$	1	0
(b)(ii)	$\mathbb{F}_2(\chi) \oplus \mathbb{F}_2(\chi^*)$	$\mathbb{F}_2(\chi)$	$\rho_\chi = \rho_{\chi^*}$	$\rho_\chi^+ = \rho_{\chi^*}^+ - 1$	0	1
(b)(ii')	$\mathbb{F}_2(\chi) \oplus \mathbb{F}_2(\chi^*)$	$\mathbb{F}_2(\chi^*)$	$\rho_\chi = \rho_{\chi^*}$	$\rho_\chi^+ = \rho_{\chi^*}^+ + 1$	1	0
(b)(iii)	$\mathbb{F}_2(\chi) \oplus \mathbb{F}_2(\chi^*)$	$\{0\}$	$\rho_\chi = \rho_{\chi^*}$	$\rho_\chi^+ = \rho_{\chi^*}^+$	0	0

Table 4.2.5: Quantities for cases (b)(i)–(iii) of Theorem 4.1.5 (using Theorem 4.2.1)

The same relations hold with $V_\infty(K)$ replaced by $V_2(K)$ and ρ_χ^+ , $\rho_{\chi^*}^+$, k_χ^+ , and $k_{\chi^*}^+$ replaced by $\rho_{4,\chi}$, ρ_{4,χ^*} , $k_{4,\chi}$, and k_{4,χ^*} , respectively.

Table 4.2.5 implies the following results.

Theorem 4.2.6. *Let K be an abelian number field of odd degree with Galois group G_K . Let χ be an irreducible $\overline{\mathbb{F}}_2$ -character. Then we have*

$$|\rho_\chi^+(K) - \rho_{\chi^*}^+(K)| \leq 1$$

as well as $|\rho_{4,\chi}(K) - \rho_{4,\chi^*}(K)| \leq 1$.

Proof. The inequalities follow from Table 4.2.5. □

Corollary 4.2.7. *If χ is an irreducible $\overline{\mathbb{F}}_2$ -character such that $\rho_\chi(K) \neq \rho_{\chi^*}(K)$, then*

$$k_\chi^+(K) + k_{\chi^*}^+(K) = 1 = k_{4,\chi}(K) + k_{4,\chi^*}(K).$$

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

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

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

$$\text{rk}_2 \mathcal{O}_{K,>0}^\times = n - \text{sgnrk}(\mathcal{O}_K^\times) = \text{rk}_2 \text{Cl}^+(K) - \text{rk}_2 \text{Cl}(K) \leq \text{rk}_2 \text{Cl}^+(K)$$

In addition, recall from (1.3.1) that $\text{sgnrk}_\chi(\mathcal{O}_K^\times)$ is equal to the multiplicity of $\mathbb{F}_2(\chi)$ in $\text{sgn}_\infty(\mathcal{O}_K^\times)$. 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

$$0 \leq \text{sgnrk}_\chi(\mathcal{O}_K^\times) \leq 1. \tag{4.3.1}$$

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

Theorem 4.3.2. *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*

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

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

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

Proof. The statement $\text{sgnrk}_\chi(\mathcal{O}_K^\times) = 0$ is equivalent to $(\mathcal{O}_K^\times / (\mathcal{O}_K^\times)^2)_\chi \subseteq \ker(\varphi_{K,\infty})_\chi$. We can determine $\ker(\varphi_{K,\infty})_\chi$ by combining Theorem 3.2.4 with Lemma 3.2.3 to get

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

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

$$\begin{aligned} \text{rk}_\chi \text{Sel}_2(K) &= \rho_\chi(K) + 1 \\ \text{rk}_\chi \ker(\varphi_{K,\infty}) &= \rho_\chi(K) + k_\chi^+(K) = \rho_\chi^+(K). \end{aligned}$$

When $k_\chi^+(K) = 1$, then $(\mathcal{O}_K^\times / \mathcal{O}_K^{\times 2})_\chi \subseteq \text{Sel}_2(K)_\chi = \ker(\varphi_{K,\infty})_\chi$ and so $\text{sgnrk}_\chi(\mathcal{O}_K^\times) = 0$. 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 $\text{rk}_\chi \ker(\varphi_{K,\infty})_\chi \neq 0$ which does not occur if $k_\chi^+(K) = \rho_\chi(K) = 0$. □

Example 4.3.3. 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 $\text{sgnrk}_\chi(\mathcal{O}_K^\times) = 1$: 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 4.3.2, note that from Lemma 3.1.4 we have $\rho_\chi(K) = 0$ and hence $\text{sgnrk}_\chi(\mathcal{O}_K^\times) = 1$.

Summing the contributions of each irreducible gives the following corollary.

Corollary 4.3.4. *Let K be a cyclic number field of odd prime degree ℓ , and let f be the order of 2 modulo ℓ . Then*

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

and the following statements hold:

(a) *If f is odd, then*

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

(b) *If f is even, then*

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

Proof. By Example 3.3.6, 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 3.3.4, hence Corollary 4.1.7 implies that $k_\chi^+(K) = 0$. By adding up Theorem 4.3.2(b) for all $1 + \frac{\ell-1}{f}$ irreducible $\mathbb{F}_2[G_K]$ -modules as in Example 3.3.6, we conclude the result.

For statement (a), every nontrivial $\mathbb{F}_2[G]$ -module is not self-dual by Lemma 3.3.4. If $k_\chi^+(K) = 1$, then $k_{\chi^*}^+(K) = 0$ by Corollary 4.1.7, and $\text{sgnrk}_\chi(\mathcal{O}_K^\times) = 0$ so

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

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

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

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

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

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

Corollary 4.3.5. *If K is a cyclic number field of prime degree ℓ where 2 is a primitive root modulo ℓ , then $\text{sgnrk}(\mathcal{O}_K^\times) = 1$ or ℓ . If the class number of K is odd, then $\text{sgnrk}(\mathcal{O}_K^\times) = \ell$.*

5. 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.

5.1. 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 $\text{Gal}(K | \mathbb{Q}) \simeq G$), where G is a fixed finite abelian group of odd order. In light of Theorem C, a heuristic is only necessary 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 behavior is 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 (4.1.1) is distributed as a uniformly random G -invariant maximal totally isotropic subspace of $\mathbb{F}_2[G]_{\chi^\pm}^2$ (see Example 3.4.1).

The assumption (H1), combined with the restriction on $S(K)_{\chi^\pm}$ implied by Theorem 4.2.1 and the counts in Theorem 4.1.5(b)(ii)–(iii) lead us to one of our main conjectures.

Conjecture 5.1.1. *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:*

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

Recall that by Corollary 4.1.4, we have $k_\chi^+(K) + k_{\chi^*}^+(K) = k_{4,\chi}(K) + k_{4,\chi^*}(K)$, hence Conjecture 5.1.1 also gives probabilities for $k_{4,\chi}(K) + k_{4,\chi^*}(K)$. In addition, a particularly simple case of Conjecture 5.1.1 is complementary to Corollary 4.2.4.

Conjecture 5.1.2. *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 $\text{Cl}(K)[2]$ is a self-dual $\mathbb{F}_2[G_K]$ -module, we have*

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

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

We predict the same probabilities as in Conjectures 5.1.1 and 5.1.2 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 $\text{rk}_2 \text{Cl}(K) = 0$).

5.2. Unit signature ranks. We now extend these heuristics to the unit signature rank. Recall that the 2-Selmer group $\text{Sel}_2(K)$ is an $\mathbb{F}_2[G_K]$ -module containing $\mathcal{O}_K^\times/(\mathcal{O}_K^\times)^2$ and the subspace $\ker(\varphi_{K,\infty}) \subseteq \text{Sel}_2(K)$ 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 $\text{Sel}_2(K)$ generated by $\mathcal{O}_K^\times/(\mathcal{O}_K^\times)^2$ is distributed as a uniformly random G -invariant subspace of $\mathbb{F}_2[G]$ containing -1 .

Decomposing into irreducibles, since $\mathcal{O}_K^\times/(\mathcal{O}_K^\times)^2 \simeq \mathbb{F}_2[G]$ we have $\text{rk}_\chi \mathcal{O}_K^\times = 1$ 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 $\text{Sel}_2(K)_\chi$ 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 $\text{Sel}_2(K)$.

Remark 5.2.1. To make assumption (H2), we consider $\mathcal{O}_K^\times/(\mathcal{O}_K^\times)^2 \subseteq \text{Sel}_2(K)$ 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 4.1.7 will have an effect on the subspace $\ker(\varphi_{K,\infty}) \subseteq \text{Sel}_2(K)$; 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 $\text{Sel}_2(K)_\chi$.

We now state a conjecture for collections of G -number fields that are not completely determined by Theorem 4.3.2. We recall from (4.3.1) that $\text{sgnrk}_\chi(\mathcal{O}_K^\times) = 0$ or 1 for any $\overline{\mathbb{F}}_2$ -character χ of G_K .

Conjecture 5.2.2. *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 $\text{rk}_\chi \text{Cl}^+(K) = \text{rk}_\chi \text{Cl}(K) = r$, we have*

$$\begin{aligned} \text{Prob}(\text{sgnrk}_\chi(\mathcal{O}_K^\times) = 0) &= \frac{q^r - 1}{q^{r+1} - 1}; \\ \text{Prob}(\text{sgnrk}_\chi(\mathcal{O}_K^\times) = 1) &= \frac{q^{r+1} - q^r}{q^{r+1} - 1}. \end{aligned}$$

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

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

Therefore, under (H2') we would have

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

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 . In light of Corollary 4.3.4, we conclude that $\text{sgnrk}(\mathcal{O}_K^\times) = 1$ or ℓ .

Conjecture 5.2.3. *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 $\text{rk}_2 \text{Cl}(K) = (\ell - 1)r$, we have*

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

Note that under the hypotheses of Conjecture 5.2.3, there is a unique nontrivial $\overline{\mathbb{F}}_2$ -character χ of $\mathbb{Z}/\ell\mathbb{Z}$, and so $\text{rk}_2 \text{Cl}(K) = (\ell - 1)r$ if and only if $\text{rk}_\chi \text{Cl}(K) = r$.

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 4.3.2(b) has $\text{sgnrk}_\chi(\mathcal{O}_K^\times) = 1 - k_\chi^+(K)$. Using Conjecture 5.1.1 and summing over the contributions we end up with the following binomial distribution.

Conjecture 5.2.4. *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 $m := \frac{\ell-1}{2^f} \in \mathbb{Z}_{>0}$. Then as K varies over cyclic number fields of degree ℓ with odd class number, we have*

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

for $0 \leq s \leq m$.

5.3. 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 [28] 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 $\text{Cl}(K)[2]$ is equal to $(1 + 2^{-f})^{\frac{\ell-1}{f}}$, where f is the order of 2 in $(\mathbb{Z}/\ell\mathbb{Z})^\times$. However, computations by Malle [28] 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 [28, (1),(2)] goes on to make predictions for the distribution of $\text{rk}_2 \text{Cl}(K)$ as K ranges over cyclic fields of degrees 3 and 5.

Conjecture 5.3.1 (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*

$$\text{Prob}(\text{rk}_2 \text{Cl}(K) = (\ell - 1)r) = \left(1 + \frac{1}{\sqrt{q}}\right) \frac{(\sqrt{q})_\infty (q^2)_\infty}{(q)_\infty^2} \cdot \frac{1}{\sqrt{q}^{r(r+2)} \cdot (q)_r} \quad (5.3.2)$$

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

Note that under the hypotheses of Conjecture 5.3.1, we have $\text{rk}_2 \text{Cl}(K) = \text{rk}_2 \text{Cl}^+(K)$ by Corollary 4.1.8, hence the left-hand side of (5.3.2) is equal to $\text{Prob}(\text{rk}_2 \text{Cl}^+(K) = (\ell - 1)r)$. (For a discussion about class group heuristics for cyclic fields of prime degree $\ell \geq 7$, see Remark 6.2.3.)

Combining Conjecture 5.3.1 with Conjecture 5.2.3 and summing gives the following.

Conjecture 5.3.3. *As K varies over cyclic number fields of degree $\ell = 3$ or 5 , we predict*

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

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

5.4. 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 $\text{rk}_2 \text{Cl}(K)$ is always even. Malle [28, (1)] (as in Conjecture 5.3.1) predicts

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

the remaining cyclic cubic fields (having $\text{rk}_2 \text{Cl}(K) \geq 6$) conjecturally comprise less than 0.004% of all cyclic cubic fields. By Corollary 4.1.8, we have $\text{Cl}(K)[2] \simeq \text{Cl}^+(K)[2]$.

In this case, Conjecture 5.2.3 predicts $\text{Prob}(\text{sgnrk}(\mathcal{O}_K^\times) = s \mid \text{rk}_2 \text{Cl}(K) = r)$ 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 $\text{rk}_2 \text{Cl}(K) = 4$, 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 $\text{sgnrk}(\mathcal{O}_K^\times)$ yields

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

Conjecture 5.3.3 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 cardinality 16 . Malle [28, (2)] predicts

$$\text{Prob}(\text{rk}_2 \text{Cl}(K) = 0) \approx 98.35\%,$$

$$\text{Prob}(\text{rk}_2 \text{Cl}(K) = 4) \approx 1.63\%,$$

and $\text{Prob}(\text{rk}_2 \text{Cl}(K) \geq 8) \leq 0.02\%$. Again, by Corollary 4.1.8 we have $\text{Cl}(K)[2] \simeq \text{Cl}^+(K)[2]$. Here, Conjecture 5.2.3 predicts $\text{Prob}(\text{sgnrk}(\mathcal{O}_K^\times) = s \mid \text{rk}_2 \text{Cl}(K) = r)$ 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

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

and so Conjecture 5.3.3 predicts that 99.9% of cyclic quintic fields have units of all possible signatures. The smallest conductor of a cyclic quintic field with $\text{sgnrk}(\mathcal{O}_K^\times) = 1$ 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 $\mathbb{F}_2(\chi) \not\cong \mathbb{F}_2(\chi^*)$ with $\#\mathbb{F}_2(\chi) = \#\mathbb{F}_2(\chi^*) = 2^3 = 8$. In this case, we may or may not have $\text{Cl}^+(K)[2] \simeq \text{Cl}(K)[2]$. We refer to Theorem C and recall Definition 2.2.4.

- If $\text{Cl}(K)[2]$ is not self-dual, then $k^+(K) = 3$.
- If $\text{Cl}(K)[2]$ is self-dual, then $k^+(K) = 0$ or 3, and Conjecture 5.1.1 predicts that

$$\text{Prob}(k^+(K) = 3) = \frac{2}{9}.$$

Example 5.4.1. 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 $\text{Cl}(K)[2]$ 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 $\text{Cl}(K)[2]$ 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 $\text{Cl}(K)[2]$ is self-dual and $k^+(K) = 3$.

For unit signature ranks, using the formulas in Conjectures 5.2.2 and 5.2.4 we make the following predictions for class groups of cyclic septic fields with low 2-rank.

- Suppose $\text{rk}_2 \text{Cl}(K) = 0$. Conjecture 5.2.4 then implies:

$$\begin{aligned} \text{Prob}(\text{sgnrk}(\mathcal{O}_K^\times) = 4 \mid \text{rk}_2 \text{Cl}(K) = 0) &= \frac{2}{9}; \\ \text{Prob}(\text{sgnrk}(\mathcal{O}_K^\times) = 7 \mid \text{rk}_2 \text{Cl}(K) = 0) &= \frac{7}{9}. \end{aligned}$$

- Suppose $\text{rk}_2 \text{Cl}(K) = 3$. Without loss of generality, assume $\rho_\chi(K) = 1$ and $\rho_{\chi^*}(K) = 0$. By Theorems C(b)(i) and 4.3.2(a), we have $\text{sgnrk}_{\chi^*}(\mathcal{O}_K^\times) = 0$. Using Conjecture 5.2.2 with $\rho_\chi(K) = 1$, we predict that $\text{sgnrk}_\chi(\mathcal{O}_K^\times) = 0$ occurs with probability $\frac{7}{63}$, so

$$\begin{aligned} \text{Prob}(\text{sgnrk}(\mathcal{O}_K^\times) = 1 \mid \text{rk}_2 \text{Cl}(K) = 3) &= \frac{7}{63}; \\ \text{Prob}(\text{sgnrk}(\mathcal{O}_K^\times) = 4 \mid \text{rk}_2 \text{Cl}(K) = 3) &= \frac{56}{63}. \end{aligned}$$

6. 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 $\#\text{Aut}(G_K)$), 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.

6.1. Cubic fields. We sampled cyclic cubic fields in this manner, performing our computations in MAGMA [27]; 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]. In the tables below, when the prediction is a theorem, we indicate it in bold.

Let $\mathcal{N}_3(X)$ denote the set of sampled cyclic cubic fields K (having $\text{Cond}(K) \leq X$), and let $\mathcal{N}_3(X, \rho = r) \subseteq \mathcal{N}_3(X)$ denote the subset of fields K with $\text{rk}_2 \text{Cl}(K) = r$. 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 $c_3 \approx 0.159$, due to Cohn [11] (see also Cohen–Diaz y Diaz–Olivier [8, Corollary 4.7]).

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

Table 6.1.1: Data for class group and signature ranks of sampled cyclic cubic fields

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

Table 6.1.2: Data for moments of (narrow) class groups of sampled cyclic cubic fields

6.2. 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 $\text{Cond}(K) < X$, and let $\mathcal{N}_7(X, \rho = r) \subseteq \mathcal{N}_7(X)$ denote the subset of fields K satisfying $\text{rk}_2 \text{Cl}(K) = r$. Asymptotically, we have $\mathcal{N}_7(X) \sim c_7 \cdot X$ where $c_7 \approx 0.033$ by Cohen–Diaz y Diaz–Olivier [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 6.2.1 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:

$$\begin{aligned} &x^7 - 1491x^5 + 29323x^4 - 118783x^3 - 662004x^2 + 1844864x - 899641, \\ &x^7 + x^6 - 3360x^5 + 54087x^4 + 1523280x^3 - 24904626x^2 - 194909041x + 2439485891, \\ &x^7 - x^6 - 8274x^5 - 249021x^4 + 3000578x^3 + 60235500x^2 + 152710207x + 67428091, \end{aligned}$$

These computations took approximately 1 CPU day. Further computations are take much longer time, owing to the difficulty of computing class groups of fields with large discriminants. As before, 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	$\text{rk}_2 \text{Cl}(K) = 0$	0.967	?
	$\text{rk}_2 \text{Cl}(K) = 3$	0.030	?
	$\text{rk}_2 \text{Cl}(K) \geq 6$	0.002	?
$\mathcal{N}_7(X, \rho = 0)$ # = 7739	$\text{rk}_2 \text{Cl}^+(K) = 0$	0.772	$0.777 = \frac{7}{9}$
	$\text{rk}_2 \text{Cl}^+(K) = 3$	0.228	$0.222 = \frac{2}{9}$
$\mathcal{N}_7(X, \rho = 0)$ # = 7739	$\text{sgnrk}(\mathcal{O}_K^\times) = 4$	0.228	$0.222 = \frac{2}{9}$
	$\text{sgnrk}(\mathcal{O}_K^\times) = 7$	0.772	$0.777 = \frac{7}{9}$
$\mathcal{N}_7(X, \rho = 3)$ # = 241	$\text{rk}_2 \text{Cl}^+(K) = 3$	0.00	0
	$\text{rk}_2 \text{Cl}^+(K) = 6$	1.00	1
$\mathcal{N}_7(X, \rho = 3)$ # = 241	$\text{sgnrk}(\mathcal{O}_K^\times) = 1$	0.082	$0.111 = \frac{7}{63}$
	$\text{sgnrk}(\mathcal{O}_K^\times) = 4$	0.917	$0.888 = \frac{56}{63}$
	$\text{sgnrk}(\mathcal{O}_K^\times) = 7$	0.000	0

Table 6.2.1: 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 Theorem 4.2.6, one may wonder how often the inequality

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

is an equality! In the first 8000 cyclic septic fields, 77.9% have $\mathrm{rk}_\chi \mathrm{Cl}^+(K) = \mathrm{rk}_{\chi^*} \mathrm{Cl}^+(K)$, i.e., a large majority of the 2-torsion subgroups of narrow class groups of $\mathcal{N}_7(X_0)$ are self-dual and therefore do *not* satisfy the equality $|\mathrm{rk}_\chi \mathrm{Cl}^+(K) - \mathrm{rk}_{\chi^*} \mathrm{Cl}^+(K)| = 1$. This data suggests that it may be much more likely for class groups and narrow class groups to be 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	?
	$(\# \mathrm{Cl}^+(K)[2])^2$	277.5	?
	$(\# \mathrm{Cl}^+(K)[2])^3$	75643.8	?

Table 6.2.2: Data for moments of class groups of the first 8000 cyclic septic fields

Remark 6.2.3. 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 6.2.2) 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 5.3.1 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 6.2.2).

APPENDIX A. CYCLIC CUBIC FIELDS WITH SIGNATURE RANK 1 (WITH NOAM ELKIES)

In this appendix, using Diophantine methods we 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

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

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., there exists $c \in \mathbb{Z}$ such that

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

The equation (A.1.1) describes a surface S in $\mathbb{A}_{\mathbb{Z}}^3$ in the variables (a, b, c) . Several curves on the surface S have been studied; for example, the *simplest cubics* of Shanks [32] 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.*

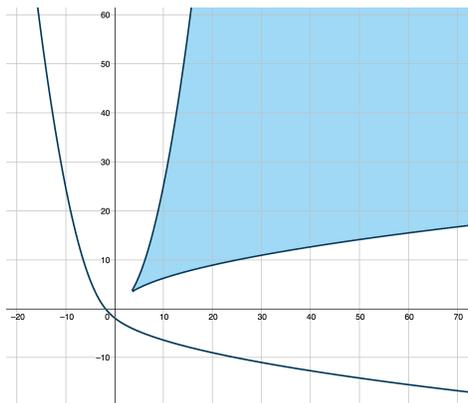
More precisely, we find families of Fermat–Pell curves on S that have infinitely many integral points $(a, b, c) \in S(\mathbb{Z})$ and such that:

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

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 [13, 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 Dummit–Kisilevsky [14, 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,

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

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

$$c^2 = (a^2 + 3a + 9)^2 Q_m(a),$$

where Q_m is the quadratic polynomial

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

Thus the change of variable $c = (a^2 + 3a + 9)y$ transforms the Diophantine equation $D(a, b) = c^2$ into $y^2 = Q_m(a)$, which is a Fermat–Pell curve for suitable choices of m . 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, if 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.

To go further, recall that $m = p/q$ in lowest terms, and multiply $y^2 = Q_m(a)$ by q^3 to give the equivalent curve

$$C_m : q^3 y^2 = Aa^2 + Ba + C \tag{A.2.2}$$

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

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

Proposition A.2.3. *Let $m \in \mathbb{Q}$ be such that the following conditions hold:*

- (i) $C_m(\mathbb{Z}) \neq \emptyset$;
- (ii) $0 < m < 1/4$; and
- (iii) $1 - 4m$ is not a square.

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

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

Proof. Completing the square, we obtain the standard form:

$$x^2 - (4Aq^3)y^2 = B^2 - 4AC \tag{A.2.4}$$

where $x = 2Aa + B$. By (i), we have $C_m(\mathbb{Z}) \neq \emptyset$ so we start with a point $(x_0, y_0) \in \mathbb{Z}^2$ on (A.2.4). By (ii), we have $0 < m^2(1 - 4m) = A/q^3$ so $4Aq^3 > 0$. By (iii), we conclude $4Aq^3 = (1 - 4m)(2mq^3)^2$ is not a square. Therefore, by the theory of Pell equations, we have infinitely many solutions $(x, y) \in \mathbb{Z}^2$ to (A.2.4) with $x \equiv x_0 \equiv B \pmod{2A}$: explicitly, there exists a power of the fundamental unit for the real quadratic field $\mathbb{Q}(\sqrt{Aq})$ of the form $\epsilon = r + s\sqrt{4Aq^3}$ with $r, s \in \mathbb{Z}$ and $r \equiv 1 \pmod{2A}$, so the solutions (x, y) generated by powers of ϵ have $x \equiv rx_0 \equiv x_0 \pmod{2A}$. Letting $a = (x - B)/(2A)$ and reversing the steps gives infinitely many $(a, y) \in C_m(\mathbb{Z})$. We may of course take $x > 0$ and then $a > 0$ as well.

To conclude, we claim that if $y^2 = Q_m(a)$ with $a, y \in \mathbb{Z}$, then

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

Indeed, in order for $P_m(\mathbb{Z}) \neq \emptyset$ we must have q odd. Reducing (A.2.2) modulo q then gives

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

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

Remark A.2.5. The method for getting infinitely many $(a, y) \in C_m(\mathbb{Z})$ from an initial solution was already known to Euler [18]; see Dickson [12, 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.2.3, 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

$$m = \frac{a + b + 3}{a^2 + 3a + 9}. \tag{A.2.6}$$

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

$$C_m: 163^3y^2 = 38700a^2 - 157740a - 924893$$

and yields a sequence of solutions

$$(a, b) = (149, 4018), (395449, 28781401718), \\ (655993191035058918, 79201300616753245838398841511537549), \dots$$

Example A.2.8. Similarly for $(a, b) = (269, 10986)$, we obtain $m = 2/13$,

$$C_m: 13^3 y^2 = 20a^2 - 148a - 275,$$

and

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

Remark A.2.9. Having found one m satisfying the conditions of Proposition A.2.3, 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.2.6) 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.2.3. 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.2.7 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 $m_k \rightarrow 0$ because $a_k \rightarrow \infty$ 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.2.3 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 Euler [17] 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

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

The discriminant of (A.3.2) factors as $m(1 - 8m)^2g(m)$ where $g(m)$ is irreducible of degree 7. So for $m \neq 0, 1/8, 1/4$, this equation defines a genus 1 curve in the variables A, B . By Siegel's theorem [33, Corollary IX.3.2.2] it has finitely many integral points. \square

Next, we now 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:

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

Lemma A.3.3. *Let $m \in \mathbb{Q}$ satisfy conditions (i)–(iii) of Proposition A.2.3. 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 $3 \nmid \text{ord}_\ell(a^2 + 3a + 9)$ is infinite. Moreover, $\alpha_{a,b}$ generates a totally ramified extension of \mathbb{Q}_ℓ 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.2.3, so t 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 $\ell \nmid 27(27m^2 - 9m + 1)q$, we have

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

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

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.2.3, 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.2.7 and A.2.8. 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 Theorem 4.3.2, we have $\text{sgnrk } \mathcal{O}_{K_{a,b}}^{\times} = 1, 3$, so we must have unit signature rank 1, i.e., there is a basis of totally positive units. \square

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. Cohn, *The density of abelian cubic fields*, *Proc. Amer. Math. Soc.* **5** (1954), 476–477.
- [12] L. E. Dickson, *History of the theory of numbers. Vol. II: Diophantine analysis*, Stechert & Co., Mineola, NY 1934.
- [13] 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.
- [14] 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>.
- [15] 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.
- [16] 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.
- [17] N.D. Elkies, *On $A^4 + B^4 + C^4 = D^4$* , *Math. of Comp.* **51** (Oct. 1988), 825–835.
- [18] 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.
- [19] É. Fouvry and J. Klüners, *On the negative Pell equation*, *Ann. of Math.* **172** (2010), no. 3, 2035–2104.
- [20] A. Fröhlich, *Galois module structure of algebraic integers*, Springer, New York, 1983.
- [21] G. Gras *Théorèmes de réflexions*, *J. Théor. Nombres Bordeaux* **10** (1998), no. 2, 399–499.
- [22] G. Gras, *Class field theory: from theory to practice*, Springer Monographs in Mathematics, Springer-Verlag, Berlin, 2005, corrected 2nd printing.
- [23] Y. Lee, *Cohen–Lenstra Heuristics and the Spiegelungssatz: Number Fields*, *J. Number Theory* **92** (2002), 37–66.
- [24] H.W. Leopoldt, *Zur Struktur der ℓ -Klassengruppe galoisscher Zahlkörper*, *J. Reine Angew. Math.* **199** (1958), 165–174.

- [25] F. Lemmermeyer, *Selmer groups and quadratic reciprocity*, Abh. Math. Sem. Univ. Hamburg **76** (2006), 279–293.
- [26] The LMFDB Collaboration, *The L-functions and Modular Forms Database*, <http://www.lmfdb.org>, 2019.
- [27] W. Bosma, J. Cannon, and C. Playoust, *The Magma algebra system. I. The user language*, J. Symbolic Comput. **24** (3–4), 1997, 235–265.
- [28] G. Malle, *Cohen-Lenstra heuristic and roots of unity*, J. Number Theory **128** (2008), no. 10, 2823–2835.
- [29] G. Malle, *On the distribution of class groups of number fields*, Exp. Math. **19** (2010), vol. 4, 465–474.
- [30] 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.
- [31] 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.
- [32] D. Shanks, *The simplest cubic fields*, Math. Comp. **28** (1974), no. 128, 1137–1152.
- [33] J.H. Silverman, *The arithmetic of elliptic curves*, 2nd ed., Grad. Texts in Math., vol. 106, Springer, Dordrecht, 2009.
- [34] P. Stevenhagen, *The number of real quadratic fields having units of negative norm*, Experiment. Math. **2** (1993), issue 2, 121–136.
- [35] M. Taylor, *Galois module structure of classgroups and units*, Mathematika **22** (1975), no. 2, 156–160.
- [36] L.C. Washington, *Class numbers of the simplest cubic fields*, Math. Comp. **48** (1987), no. 177, 371–384.
- [37] M.M. Wood, *On the probabilities of local behaviors in abelian field extensions*, Compos. Math. **146** (2010), no. 1, 102–128.

DEPARTMENT OF MATHEMATICS, DARTMOUTH COLLEGE, 6188 KEMENY HALL, HANOVER, NH 03755
Email address: benjamin.k.breen.gr@dartmouth.edu

DEPARTMENT OF MATHEMATICS, UC SAN DIEGO, 9500 GILMAN DRIVE #0112, LA JOLLA, CA 92093
Email address: ila@math.ucsd.edu

DEPARTMENT OF MATHEMATICS, DARTMOUTH COLLEGE, 6188 KEMENY HALL, HANOVER, NH 03755
Email address: jvoight@gmail.com
URL: <http://www.math.dartmouth.edu/~jvoight/>