QUATERNIONIC ARTIN REPRESENTATIONS AND NONTRADITIONAL ARITHMETIC STATISTICS

DAVID E. ROHRLICH

ABSTRACT. We classify and then attempt to count the real quadratic fields (ordered by the size of the totally positive fundamental unit, as in Sarnak [14], [15]) from which quaternionic Artin representations of minimal conductor can be induced. Some of our results can be interpreted as criteria for a real quadratic field to be contained in a Galois extension of $\mathbb{Q}$ with controlled ramification and Galois group isomorphic to a generalized quaternion group.

Traditionally, number fields of a given degree over $\mathbb{Q}$ are ordered by the size of their discriminant, and Artin representations of $\mathbb{Q}$ of a given dimension are ordered by the size of their conductor. But in [14] and [15], Sarnak obtained asymptotic averages of ring class numbers of real quadratic fields by enumerating the corresponding orders according to the size of their fundamental totally positive unit. Sarnak's method was subsequently used by Raulf [7], [8] to average the class number over *maximal* orders as well as over orders satisfying given congruence conditions. Here Sarnak's ordering will be used to count certain Artin representations induced from real quadratic fields.

In describing the results of Sarnak and Raulf, we have departed from the authors' own formulation, for they use the language of binary quadratic forms rather than the equivalent language – more suited to Artin representations – of ring class groups. Our notation will also depart from theirs in one important respect: While Sarnak and Raulf use h and ϵ to denote the narrow class number and fundamental totally positive unit of an order, we shall instead use h^{nar} and ϵ^+, reserving h and ϵ for the usual class number and fundamental unit. Thus if ϵ has norm -1 then $\epsilon^+ = \epsilon^2$. (Here ϵ and ϵ^+ are defined by the standard condition $\epsilon, \epsilon^+ > 1$, a condition which is meaningful because real quadratic fields will always be taken to be subfields of $\mathbb{R}$.) In principle, one could use ϵ rather than ϵ^+ as the basis of the ordering, but in this note we shall adhere to Sarnak's original ordering by ϵ^+.

Our group-theoretic conventions will be as follows: A *representation* of a group G is a homomorphism (continuous if G is endowed with a topology) $\rho : G \to \mathrm{GL}(V)$, where V is a finite-dimensional vector space over $\mathbb{C}$. An irreducible ρ is *dihedral* if its image is isomorphic to the dihedral group

$$D_{2m} = \langle a, b | a^m = 1, a^m = b^2 = 1, bab^{-1} = a^{-1} \rangle$$

of order $2m$ for some $m \geqslant 3$, and *quaternionic* if its image is isomorphic to the generalized quaternion group

$$Q_{4m} = \langle a, b | a^{2m} = 1, a^m = b^2, bab^{-1} = a^{-1} \rangle$$

2000 *Mathematics Subject Classification.* Primary 11R32; Secondary 11R20.

of order $4m$ for some $m \geqslant 2$. An irreducible two-dimensional monomial self-dual representation is dihedral or quaternionic according as it is orthogonal or symplectic, and conversely, a dihedral or quaternionic representation is othogonal or symplectic respectively and monomial of dimension two. In particular, a dihedral or quaternionic Artin representation of $\mathbb{Q}$ is induced from a quadratic field.

Dihedral Artin representations of $\mathbb{Q}$ enjoy a certain ubiquity in number theory that quaternionic representations lack. One reason is that dihedral representations often correspond to holomorphic cusp forms of weight one, whereas quaternionic representations are always associated to Maass forms. A related reason is that dihedral representations are simply more abundant. Indeed let $\vartheta^{\mathrm{di}}(x)$ be the number of isomorphism classes of dihedral Artin representations of $\mathbb{Q}$ of conductor $\leqslant x$, and let $\vartheta^{\mathrm{qu}}(x)$ be the analogous quantity for quaternionic representations. It follows from Siegel's asymptotic class number formulas (see [17] and [10]) that

$$\vartheta^{\mathrm{di}}(x) \sim \frac{\pi}{36\zeta(3)^2} x^{3/2}, \tag{1}$$

and while no counterpart to (1) is known for $\vartheta^{\mathrm{qu}}(x)$, one has at least that

$$x^{1-\varepsilon} \ll \vartheta^{\mathrm{qu}}(x) \ll x/\log x \tag{2}$$

for every $\varepsilon > 1/4\sqrt{e}$ (see [11]). A conjecture of Ambrose [1], whose work in the direction of his conjecture is the main ingredient in the lower bound in (2), would imply that the lower bound holds for all $\varepsilon > 0$, but our focus here is on the upper bound and the disparity in growth rates: $\vartheta^{\mathrm{di}}(x) \gg x^{3/2}$ versus $\vartheta^{\mathrm{qu}}(x) \ll x/\log x$.

This disparity is misleading. The dominant contribution to $\vartheta^{\mathrm{di}}(x)$ comes from dihedral representations induced from imaginary quadratic fields, whereas quaternionic representations can be induced from real quadratic fields only. If one counts only dihedral representations induced from real quadratic fields and orders them by conductor then nothing comparable to (1) is known, but as we have already indicated, Sarnak [14] was able to prove an asymptotic formula by ordering by fundamental totally positive units:

$$\sum_{\epsilon_d^+ \leqslant x} h_d^{\mathrm{nar}} = \mathrm{Li}(x^2) + O(x^{3/2}(\log x)^2), \tag{3}$$

where d runs over discriminants of orders in real quadratic fields. The connection between (3) and dihedral Artin representations induced from real quadratic fields is that after appropriate identifications, the inducing character can be chosen to be a ring class character of order $\geqslant 3$. Thus the left-hand side of (3) is a rough approximation to the function $\alpha^{\mathrm{di}}(x)$ which counts isomorphism classes of dihedral Artin representations of $\mathbb{Q}$ of conductor d with $\epsilon_d^+ \leqslant x$. The main reason why (3) is only a *rough* approximation to $\alpha^{\mathrm{di}}(x)$ is that if a ring class character is counted by h_d^{nar} then it is also counted by $h_{dm^2}^{\mathrm{nar}}$ for any positive integer m, whence a given Artin representation may be counted several times in (3). Or to put it differently, (3) counts imprimitive Artin representations along with true primitive Artin representations.

The issue of imprimitivity disappears, however, if we turn to Raulf's formula:

$$\sum_{\epsilon_K^+ \leqslant x} h_K^{\mathrm{nar}} = \frac{25\zeta(3)}{16} \prod_{p \geqslant 2} (1 - 2p^{-2} - p^{-3})\mathrm{Li}(x^2) + O(x^c) \tag{4}$$

for some $c < 2$ ([7], p. 222), where K runs over real quadratic fields and h_K^{nar} and ϵ_K^+ are associated to the ring of integers of K. We can view (4) as an asymptotic count of dihedral representations induced by narrow ideal class characters, and remarkably, even though (4) counts what appears at first to be a thin subclass of dihedral representations, a comparison with (3) shows that such representations account for a positive proportion of the representations counted by $\alpha^{\mathrm{di}}(x)$. More formally, let $\beta^{\mathrm{di}}(x)$ be the number of isomorphism classes of dihedral Artin representations of $\mathbb{Q}$ which are induced by one-dimensional unramified Galois characters of real quadratic fields K with $\epsilon_K^+ \leqslant x$. (Here "unramified" means "unramified outside infinity.") A straightforward deduction from (4) gives

$$\beta^{\mathrm{di}}(x) \sim \frac{25\zeta(3)}{64} \prod_{p \geqslant 2} (1 - 2p^{-2} - p^{-3}) x^2 / \log x, \tag{5}$$

whence in particular $\beta^{\mathrm{di}}(x) \gg \alpha^{\mathrm{di}}(x)$ by (3).

This note is an attempt to find a quaternionic analogue of the preceding circle of ideas. A quaternionic analogue of $\alpha^{\mathrm{di}}(x)$ is problematic, because quaternionic representations are not induced by ring class characters. However the quaternionic counterpart to a narrow ideal class character of order $\geqslant 3$ is easily identified: It is a nonquadratic character which is "conjugate-symplectic of minimal conductor." Such characters will be called *amplectic* (we embrace them!), and the function $\beta^{\mathrm{qu}}(x)$ which counts the representations induced by amplectic characters is thus the natural analogue of $\beta^{\mathrm{di}}(x)$. We will see that for every $\varepsilon > 0$,

$$x^{2-\varepsilon} \ll \beta^{\mathrm{qu}}(x) \ll x^2 / \log x. \tag{6}$$

While (6) falls far short of an asymptotic equality, taken together, (5) and (6) provide a perspective not apparent from (1) and (2): If we restrict attention to real quadratic fields and order representations by the size of the fundamental totally positive unit, then dihedral representations are not so much more abundant than quaternionic representations after all.

Underlying (6) is our main result, a classification of the real quadratic fields which have an amplectic character. In contrast to the dihedral case, where K has a character relevant to $\beta^{\mathrm{di}}(x)$ if and only if the narrow ideal class group of K has an element of order $\geqslant 3$, the classification in the quaternionic case is a bit more complicated and is in fact the core around which the whole paper is organized: After an elementary remark about Dirichlet characters in Section 1, we introduce "conjugate-symplectic characters" in Section 2 and those of "minimal conductor" in Section 3, and then in Sections 4 and 5 we derive our classification, from which we deduce our bounds for $\beta^{\mathrm{qu}}(x)$ in Section 6 by quoting old results on square-free values of quadratic polynomials (Carlitz [2], Estermann [3], and especially Ricci [9]). We also use Siegel's half of the Brauer-Siegel theorem [16], rendering the lower bound in (6) ineffective. On the other hand, we do obtain effective constants, albeit weak ones, for a quantitative version of our main result:

Theorem 1. *When real quadratic fields are ordered by the size of the fundamental totally positive unit, between* 24% *and* 68% *have an amplectic character.*

The referee has requested more translations of our results into the language of classical Galois theory. One such translation was contained already in the original submission: If a real quadratic field K is contained in a Galois extension of $\mathbb{Q}$ with Galois group Q_{4m}, where m is odd, then the discriminant of K is a product of

primes congruent to 1 mod 4 or else 8 times such a product. This assertion and a few similar ones are collected in Section 7, the final section of the paper.

1. Quadratic reciprocity

We denote the ring of adeles of a number field K by $\mathbb{A}_K$ and the group of ideles by $\mathbb{A}_K^\times$, and as usual, we view K as a subring of $\mathbb{A}_K$ and $K^\times$ as a subgroup of $\mathbb{A}_K^\times$ via the respective diagonal embeddings. An idele class character of K is a continuous homomorphism $\mathbb{A}_K^\times \to \mathbb{C}^\times$ which is trivial on $K^\times$.

Given a primitive Dirichlet character χ, we write $\chi_\mathbb{A}$ for the corresponding idele class character of $\mathbb{Q}$ and χ_p for the component of $\chi_\mathbb{A}$ at a prime or place $p \leqslant \infty$. We also write a_p for the p-component of an idele $a \in \mathbb{A}_\mathbb{Q}^\times$. Then

$$\chi_\mathbb{A}(a) = \prod_{p \leqslant \infty} \chi_p(a_p). \tag{7}$$

Parallel to (7) is the expression for χ as a product of primitive Dirichlet characters $\chi_{(p)}$ of p-power conductor:

$$\chi = \prod_p \chi_{(p)}, \tag{8}$$

where p runs over primes dividing the conductor of χ (or indeed over all finite primes, $\chi_{(p)}$ being the trivial character of conductor 1 if p does not divide the conductor of χ). Connecting (7) and (8) is the equation

$$\chi_p(n) = \chi_{(p)}^{-1}(n) \tag{9}$$

for positive integers n prime to p, or simply $\chi_p(n) = \chi_{(p)}(n)$ if χ is quadratic.

Let c be a square-free integer > 1, and put $d = c$ or $d = 4c$ according as c is 1 mod 4 or 2 or 3 mod 4. Henceforth we take χ to be the primitive even quadratic Dirichlet character of conductor d.

Proposition 1. *Let p be a prime congruent to 3 mod 4 which divides c. Then $\chi_p(c) = -1$.*

Proof. Let δ be 0 or 1 according as c is odd or even, and let $\hat{c}$ be the product of the odd prime divisors of c/p. Then $c = 2^\delta \hat{c} p$, and consequently

$$\chi_p(c) = \chi_p(2)^\delta \chi_p(\hat{c}) \chi_p(p). \tag{10}$$

Now for odd primes q dividing c, $\chi_{(q)}$ is the Legendre symbol at q, and in particular $\chi_{(p)}$ is the Legendre symbol at p, so (9) gives

$$\chi_p(2)^\delta \chi_p(\hat{c}) = \left(\frac{2}{p}\right)^\delta \prod_{q|\hat{c}} \left(\frac{q}{p}\right). \tag{11}$$

On the other hand, taking a in (7) to be the principal idele $p \in \mathbb{Q}^\times$, we have

$$1 = \chi_2(p) \chi_p(p) \prod_{q|\hat{c}} \left(\frac{p}{q}\right), \tag{12}$$

because χ_q is unramified for $q \nmid d$ and χ_∞ is trivial (χ is even). Furthermore, putting

$$\Delta = \begin{cases} 1 & \text{if } c \equiv 1 \bmod 4 \\ -4 & \text{if } c \equiv 3 \bmod 4 \\ 8 & \text{if } c \text{ is even and } c/2 \equiv 1 \bmod 4 \\ -8 & \text{if } c \text{ is even and } c/2 \equiv 3 \bmod 4, \end{cases}$$

we see that $\chi_{(2)}$ is the Kronecker symbol at Δ, whence (9) gives

$$\chi_2(p) = \left(\frac{\Delta}{p}\right). \tag{13}$$

Now combine (10), (11), (12), and (13), and apply quadratic reciprocity. We obtain

$$\chi_p(c) = \left(\frac{2}{p}\right)^\delta \left(\frac{\Delta}{p}\right) (-1)^{(\hat{c}-1)(p-1)/4}. \tag{14}$$

The proof is completed by considering the cases $c \equiv 1$, 2, or 3 mod 4 separately. For example, if $c \equiv 1 \bmod 4$ then $\hat{c} = c/p$, whence $\hat{c} \equiv 3 \bmod 4$. Also $\delta = 0$ and $\Delta = 1$, so $\chi_p(c) = -1$. The other cases are handled similarly. □

2. Conjugate-symplectic characters

As we have already indicated, if ρ is a two-dimensional irreducible monomial self-dual representation of a finite group then ρ is dihedral if it is orthogonal and quaternionic if it is symplectic. In the latter case, the hypothesis that ρ is symplectic means simply that the determinant of ρ is trivial, because the symplectic and special linear groups coincide in dimension two. Now according to a standard formula for the determinant of an induced representation, we have

$$\det(\mathrm{ind}_H^G \xi) = (\mathrm{sign}_{G/H})(\xi \circ \mathrm{tran}_H^G), \tag{15}$$

where the notation is as follows: First of all, G is a finite group, H is a subgroup of index 2, ξ is a one-dimensional character of H, and $\mathrm{ind}_H^G \xi$ is the representation of G induced by ξ. In addition, $\mathrm{sign}_{G/H}$ is the isomorphism $G/H \cong \{\pm 1\}$ pulled back to G, and tran_H^G is the transfer map $G^{\mathrm{ab}} \to H^{\mathrm{ab}}$ from the abelianization of G to that of H. Note that ξ can be viewed as a function on H^{ab} and both sides of (15) as functions on G^{ab}. Thus by (15), $\rho = \mathrm{ind}_H^G \xi$ is symplectic if and only if

$$\xi \circ \mathrm{tran}_H^G = \mathrm{sign}_{G/H}. \tag{16}$$

Let us examine (16) in the context of Artin representations.

Let $\overline{\mathbb{Q}}$ denote the algebraic closure of $\mathbb{Q}$ in $\mathbb{C}$. In keeping with our convention that real quadratic fields are subfields of $\mathbb{R}$, we view arbitrary number fields F as subfields of $\mathbb{C}$ and hence of $\overline{\mathbb{Q}}$. In the first instance, an Artin representation of F is a continuous homomorphism $\rho : \mathrm{Gal}(\overline{\mathbb{Q}}/F) \to \mathrm{GL}(V)$, where V is a finite-dimensional vector space over $\mathbb{C}$, but since the preceding discussion referred to finite groups, it is convenient here to view ρ as a representation $\mathrm{Gal}(L/F) \to \mathrm{GL}(V)$, where L is the fixed field of the kernel of ρ on $\mathrm{Gal}(\overline{\mathbb{Q}}/F)$. In particular, take $F = \mathbb{Q}$ and ρ quaternionic, and put $G = \mathrm{Gal}(L/\mathbb{Q})$. Then ρ is induced from a subgroup of index 2 in G, say $H = \mathrm{Gal}(L/K)$. We write $\rho = \mathrm{ind}_{K/\mathbb{Q}} \xi$, where $\mathrm{ind}_{K/\mathbb{Q}}$ means ind_H^G and ξ is a character of H satisfying (16). Note that $\mathrm{sign}_{G/H}$ is now $\mathrm{sign}_{K/\mathbb{Q}}$, the nontrivial character of $\mathrm{Gal}(K/\mathbb{Q})$, viewed as a character of $\mathrm{Gal}(L/\mathbb{Q})$. Furthermore, K is a *real* quadratic field. Indeed, if K is imaginary then there is an involution in

$\mathrm{Gal}(L/\mathbb{Q})$ – namely complex conjugation – which restricts to the nontrivial element of $\mathrm{Gal}(K/\mathbb{Q})$. A calculation then shows that tran_H^G is trivial, contradicting (16).

It remains to elucidate (16). Using Artin reciprocity, we may identify characters of $\mathrm{Gal}(\overline{\mathbb{Q}}/K)$ with idele class characters of K of finite order, and we often refer to both types of characters simply as "characters of K," either because both interpretations are intended or because the preferred interpretation is apparent from context. In any case, Artin reciprocity identifies transfer on Galois groups with inclusion of idele class groups, so that (16) becomes

$$\xi|\mathbb{A}_{\mathbb{Q}}^{\times} = \mathrm{sign}_{K/\mathbb{Q}}. \tag{17}$$

Thus in the context of idele class characters, (17) is the condition for $\mathrm{ind}_{K/\mathbb{Q}}\xi$ to be symplectic. On a personal note, I want to acknowledge that my first encounter with quaternionic Artin representations was a lecture of Serre at Harvard in the late 1970's in which Serre related Galois extensions of $\mathbb{Q}$ with Galois group Q_8 to quartic characters ξ of real quadratic fields K satisfying (17).

An idele class character of finite order satisfying (17), or a Galois character satisfying (16) with G and H as above, will be called a *conjugate-symplectic* character of K. To illustrate the definition, we observe:

Proposition 2. *If ξ is a conjugate-symplectic character of K which is ramified at one of the two infinite places of K then it is ramified at both infinite places.*

Proof. Let $a \in \mathbb{A}_{\mathbb{Q}}^{\times}$ be the idele with $a_p = 1$ for all $p < \infty$ and $a_\infty = -1$. When a is viewed as an element of $\mathbb{A}_K^{\times}$, it becomes the idele with component 1 at all finite places and component -1 at the two infinite places. Thus if ξ is ramified at precisely one of the two infinite places then $\xi(a) = -1$. This contradicts (17), because the Dirichlet character corresponding to $\mathrm{sign}_{K/\mathbb{Q}}$ is even, whence $\mathrm{sign}_{K/\mathbb{Q}}(a) = 1$. □

For $\mathrm{ind}_{K/\mathbb{Q}}\xi$ to be quaternionic, it must be irreducible as well as conjugate-symplectic. Let τ be the nontrivial element of $\mathrm{Gal}(K/\mathbb{Q})$, which acts on $\mathbb{A}_K^{\times}$ via the identification $\mathbb{A}_K^{\times} = (K \otimes \mathbb{A}_{\mathbb{Q}})^{\times}$. By Mackey's criterion, the condition for irreducibility is $\xi^\tau \neq \xi$, where ξ^τ is the idele class character defined by $\xi^\tau(a) = \xi(a^\tau)$. Now it is immediate from (17) that $\xi(a^{\tau+1}) = 1$ for all $a \in \mathbb{A}_K^{\times}$; equivalently, $\xi^\tau = \xi^{-1}$. So Mackey's criterion becomes $\xi \neq \xi^{-1}$. Thus $\mathrm{ind}_{K/\mathbb{Q}}\xi$ is irreducible if and only ξ has order $\geqslant 3$. The facts just reviewed are summarized in the first sentence of the following proposition:

Proposition 3. *Given a real quadratic field K and a character ξ of K, the representation $\rho = \mathrm{ind}_{K/\mathbb{Q}}\xi$ is quaternionic if and only if ξ is conjugate-symplectic of order $\geqslant 3$, and all quaternionic Artin representations of $\mathbb{Q}$ are of this form for some such K and ξ. Furthermore, given two such characters ξ and ξ', we have $\mathrm{ind}_{K/\mathbb{Q}}\xi \cong \mathrm{ind}_{K/\mathbb{Q}}\xi'$ if and only if $\xi' = \xi$ or $\xi' = \xi^{-1}$. Finally, there exist two such pairs (K, ξ) and (K', ξ') with $K' \neq K$ and $\mathrm{ind}_{K/\mathbb{Q}}\xi \cong \mathrm{ind}_{K'/\mathbb{Q}}\xi'$ if and only if the image of ρ is isomorphic to Q_8, and in that case there are exactly six such pairs, say $(K, \xi^{\pm 1})$, $(K', (\xi')^{\pm 1})$, and $(K'', (\xi'')^{\pm 1})$, with K, K', and K'' all distinct.*

Proof. The first assertion has already been verified, the second follows from Frobenius reciprocity and the self-duality of ρ, and the third is a consequence of the fact that among the groups Q_{4m}, only Q_8 has an irreducible "triply monomial" representation (cf. [12], Proposition 18). □

By virtue of (16) or (17), a conjugate-symplectic character is nontrivial. Thus the phrase "of order $\geqslant 3$" in Proposition 3 is equivalent to "nonquadratic." We now consider a case in which the equivalent phrases "of order $\geqslant 3$" and "nonquadratic" can be dispensed with entirely. Fix a real quadratic field K and let c be the squarefree integer > 1 such that $K = \mathbb{Q}(\sqrt{c})$.

Proposition 4. *Suppose that c is divisible by a prime congruent to 3 mod 4. If ξ is any conjugate-symplectic character of K then the order of ξ is divisible by 4. Hence the representation $\rho = \mathrm{ind}_{K/\mathbb{Q}}\xi$ is quaternionic.*

Proof. Let p be a prime congruent to 3 mod 4 which divides c, and let $\mathfrak{p}$ be the prime of K above p. We write $\xi_\mathfrak{p}$ for the component of ξ at $\mathfrak{p}$ and χ for the primitive quadratic Dirichlet character such that $\chi_\mathbb{A} = \mathrm{sign}_{K/\mathbb{Q}}$. By (17) and Proposition 1, we have $\xi_\mathfrak{p}(\sqrt{c})^2 = \chi_p(c) = -1$. Hence the order of $\xi_\mathfrak{p}$ is divisible by 4, and consequently so is the order of ξ. □

3. Conjugate-symplectic characters of minimal conductor

So far we have encountered idele class characters, Galois characters, and primitive Dirichlet characters, and primitive ray class characters will soon appear as well. If ξ is a character of any of these types, then $\mathfrak{q}(\xi)$ will denote its conductor, and we put $q(\xi) = \mathbf{N}\mathfrak{q}(x)$, where $\mathbf{N}$ denotes the absolute norm. Thus $\mathfrak{q}(\xi)$ is an integral ideal of the base field K of ξ and $q(\xi)$ is a positive integer. But if $K = \mathbb{Q}$ then $q(\xi)$ is the unique positive generator of $\mathfrak{q}(\xi)$, and we call $q(\xi)$ itself the conductor. All of these notations and conventions carry over to Artin representations of dimension > 1 as well.

Given a real quadratic field K, we let d_K be its discriminant and $\mathfrak{d}_K$ its different ideal. When K is fixed we usually drop the subscript, writing simply d and $\mathfrak{d}$. The same goes for other invariants of K, such as the ring of integers $\mathcal{O}_K$, the class number h_K, and the fundamental unit ϵ_K, which will often be written $\mathcal{O}$, h, and ϵ. However the norm to $\mathbb{Q}$ of an element $\alpha \in K$ will always be denoted $N_{K/\mathbb{Q}}(\alpha)$.

If d is even then $\mathfrak{t}$ denotes the prime ideal of $\mathcal{O}$ above 2. Put

$$\mathfrak{d}^\circ = \begin{cases} \mathfrak{d} & \text{if } d \equiv 1 \bmod 4 \\ \mathfrak{t}\mathfrak{d} & \text{if } d \equiv 4 \bmod 8 \\ \mathfrak{t}^2\mathfrak{d} & \text{if } d \equiv 0 \bmod 8. \end{cases} \tag{18}$$

Then $\mathfrak{d}^\circ \cap \mathbb{Z} = d\mathbb{Z}$. The following remark (Proposition 6 of [11]) is elementary:

Proposition 5. *If ξ is a conjugate-symplectic character of K then $\mathfrak{d}^\circ$ divides $\mathfrak{q}(\xi)$.*

We say that ξ is *of minimal conductor* if $\mathfrak{q}(\xi) = \mathfrak{d}^\circ$. With this definition in place, another bears repeating: We call a nonquadratic character which is conjugate-symplectic of minimal conductor *amplectic*. Put

$$d^\circ = \begin{cases} d & \text{if } d \equiv 1 \pmod 4 \\ 2d & \text{if } d \equiv 4 \pmod 8 \\ 4d & \text{if } d \equiv 0 \pmod 8. \end{cases}, \tag{19}$$

so that $d^\circ = \mathbf{N}\mathfrak{d}^\circ$. If $\rho = \mathrm{ind}_{K/\mathbb{Q}}\xi$ for some character ξ of K then the standard formula for the conductor of an induced representation gives $q(\rho) = dq(\xi)$, so Proposition 5 has the following consequence:

Proposition 6. *If ρ is a quaternionic Artin representation of $\mathbb{Q}$ induced from K then dd° divides $q(\rho)$.*

Given a quaternionic Artin representation ρ of $\mathbb{Q}$, we say that ρ is of *minimal conductor* if $q(\rho) = d_K d_K^\circ$ for some K, or in other words if ρ is induced by an amplectic character of K for some K. If such a K exists, then it is unique. Indeed by Proposition 3, the uniqueness is automatic unless the image of ρ is isomorphic to Q_8, but even without mentioning Q_8 we can verify the uniqueness as follows. By (19), $d_K d_K^\circ = 2^\nu d_K^2$ with $\nu = 0, 1$, or 2 according as d_K is 1 mod 4 or 4 mod 8 or 0 mod 8. Thus the highest power of 2 dividing $q(\rho)$ is 1, 32, or 256 respectively. So ν is determined by $q(\rho)$ and then K is determined by the formula $d_K = \sqrt{q(\rho)/2^\nu}$.

The function $\beta^{\mathrm{qu}}(x)$ which figures in formula (6) of the introduction can now be defined precisely. Let g_K be the number of amplectic characters of K; then

$$\beta^{\mathrm{qu}}(x) = \frac{1}{2} \sum_{\epsilon_K^+ \leqslant x} g_K. \tag{20}$$

Since ξ and ξ^{-1} induce the same isomorphism class, the factor $1/2$ in (20) ensures that $\beta^{\mathrm{qu}}(x)$ is the number of *distinct* isomorphism classes of quaternionic Artin representations of minimal conductor such that $\epsilon_K^+ \leqslant x$ for the appropriate K.

The key to proving (6) is knowing when $g_K > 0$. Thus in the next two sections we give necessary and sufficient conditions on K for the existence of an amplectic character of K. There are two cases, depending on whether d_K is or is not divisible by a prime congruent to 3 mod 4. In the latter case, Fouvry and Klüners [4] call d_K *special*, and we shall also call d_K *nonspecial* in the former case.

4. Special discriminants

Since K will again be fixed, we revert to writing d_K as d. Throughout this section, we assume that d is not divisible by any prime congruent to 3 mod 4. Equivalently, d is either a product of primes congruent to 1 mod 4 or else 8 times such a product. The main point of this section is the following theorem, which will be deduced from Proposition 8 below.

Theorem 2. *Suppose that the discriminant of the real quadratic field K is special. If $N_{K/\mathbb{Q}}(\epsilon) = 1$ then K has an amplectic character.*

If ξ is any idele class character of K and ∞ is either of the two infinite places of K then $\xi_\infty(-1)$ is 1 or -1. By Proposition 2, if ξ is conjugate-symplectic then the value of $\xi_\infty(-1)$ is independent of the choice of ∞, and we say that ξ is even or odd, or that its parity is even or odd, according as $\xi_\infty(-1)$ is 1 or -1.

Proposition 7. *There exists a quadratic character ζ of K which is conjugate-symplectic of minimal conductor, and if 8 divides d then the parity of ζ can be chosen arbitrarily.*

Proof. If d is a product of primes congruent to 1 mod 4 the assertion follows from Proposition 11 of [11]. The argument in the case $d \equiv 0$ mod 8 is similar, but for the sake of completeness we provide the details. To begin with, observe that $(\mathbb{Z}/16\mathbb{Z})^\times \cong (\mathbb{Z}/2\mathbb{Z}) \times (\mathbb{Z}/4\mathbb{Z})$ but $(\mathbb{Z}/8\mathbb{Z})^\times \cong (\mathbb{Z}/2\mathbb{Z})^2$, whence there are four primitive Dirichlet characters of conductor 16: two even characters and two odd. The square of all four characters is the unique primitive even Dirichlet character of conductor 8. Furthermore, since every odd prime p dividing d is congruent to

1 mod 4, the corresponding Legendre symbol is the square of a primitive Dirichlet character of conductor p (which is even or odd according as p is 1 or 5 mod 8). It follows from these remarks that there is a primitive Dirchlet character ψ of conductor $2d$ and arbitrarily prescribed parity such that $\chi = \psi^2$ (recall that χ is the primitive quadratic Dirichlet character of conductor d corresponding to K). Switching to an adelic framework, we put $\zeta = \psi_{\mathbb{A}} \circ N_{K/\mathbb{Q}}$, where in this setting $N_{K/\mathbb{Q}}$ is the idelic norm. Note that the parity of ζ coincides with that of ψ and thus can be chosen at will. Since the restriction of $N_{K/\mathbb{Q}}$ to $\mathbb{A}_{\mathbb{Q}}^{\times}$ is the map $x \mapsto x^2$, we have $\zeta|\mathbb{A}_{\mathbb{Q}}^{\times} = \chi_{\mathbb{A}}$, so ζ is conjugate-symplectic. Also $\zeta^2 = \chi_{\mathbb{A}} \circ N_{K/\mathbb{Q}} = 1$, so ζ is quadratic. It remains to check that the conductor of ζ is $\mathfrak{d}^{\circ}$.

Let $\mathcal{O}$ be the ring of integers of K. For a prime ideal $\mathfrak{p}$ of $\mathcal{O}$ dividing $\mathfrak{d}$, let $K_{\mathfrak{p}}$ be the completion of K at $\mathfrak{p}$ and $\mathcal{O}_{\mathfrak{p}}$ its ring of integers. Let $\zeta_{\mathfrak{p}} : K_{\mathfrak{p}}^{\times} \to \{\pm 1\}$ be the corresponding component of ζ. We write $\mathfrak{q}(\zeta_{\mathfrak{p}})$ for the conductor of $\zeta_{\mathfrak{p}}$, which we view as an ideal of $\mathcal{O}$. Thus

$$\mathfrak{q}(\zeta) = \prod_{\mathfrak{p}|\mathfrak{d}} \mathfrak{q}(\zeta_{\mathfrak{p}}) \tag{21}$$

If $\mathfrak{p}$ is of odd residue characteristic then $\mathfrak{q}(\zeta_p) = \mathfrak{p}$ because $\zeta_{\mathfrak{p}}$ is quadratic. Now let $\mathfrak{t}$ be the prime above 2 and τ a uniformizer of $\mathcal{O}_{\mathfrak{t}}$. Then every element of $1 + 4\tau\mathcal{O}_{\mathfrak{t}}$ is a square. Since $\zeta_{\mathfrak{t}}$ is quadratic it follows that $\zeta_{\mathfrak{t}}$ is trivial on $1 + 4\tau\mathcal{O}_{\mathfrak{t}}$, whence the right-hand side of (21) divides $\mathfrak{d}^{\circ}$ and so equals $\mathfrak{d}^{\circ}$ by Proposition 5.. □

Proposition 8. *If the narrow ideal class group of K has an element of order $\geqslant 3$ then K has an amplectic character.*

Proof. Let ζ be as in Proposition 7. If the narrow ideal class group of K has an element of order $\geqslant 3$, then there is an idele class character λ of K of finite order $\geqslant 3$ which is unramified at all finite places. Such a character is trivial on $\mathbb{A}_{\mathbb{Q}}^{\times}$, so the product $\xi = \zeta\lambda$ is conjugate-symplectic of order $\geqslant 3$, and ξ is of minimal conductor because $\mathfrak{q}(\xi) = \mathfrak{q}(\zeta) = \mathfrak{d}^{\circ}$. □

Theorem 2 follows from Proposition 8, because for special discriminants, the condition $N_{K/\mathbb{Q}}(\epsilon) = 1$ implies that the narrow ideal class group of K has an element of order 4 (cf. Lemmas 1 and 2 of [4] and the references cited there).

Remark. The case $N_{K/\mathbb{Q}}(\epsilon) = -1$, which will now be treated for the sake of completeness, is not used elsewhere in the paper but is nonetheless statistically significant. Indeed Stevenhangen [18] has conjectured that among real quadratic fields with special discriminant, the case $N_{K/\mathbb{Q}}(\epsilon) = -1$ occurs roughly 58% of the time (the fields are ordered by discriminant), and in the direction of Stevenhagen's conjecture, Fouvry and Klüners [4] have proved that the case $N_{K/\mathbb{Q}}(\epsilon) = -1$ occurs between 41% and 67% of the time.

Theorem 3. *Suppose that $N_{K/\mathbb{Q}}(\epsilon) = -1$. Then K has an amplectic character if and only if the ideal class group of K has an element of order $\geqslant 3$.*

Proof. Sufficiency follows from Proposition 8. For necessity, suppose that K has an ampletic character ξ. We will show that the ideal class group of K has an element of order $\geqslant 3$. Suppose first that $d \equiv 1$ mod 4, and let ζ be as in Proposition 7. Let p be a prime dividing d, and let $\mathfrak{p}$ be the prime ideal of K lying over p. Viewing ζ and ξ as idele class characters, let $\zeta_{\mathfrak{p}}$ and $\xi_{\mathfrak{p}}$ be the components of ζ and ξ at $\mathfrak{p}$. Since p is odd, the conductors $\mathfrak{q}(\zeta_{\mathfrak{p}})$ and $\mathfrak{q}(\xi_{\mathfrak{p}})$ both coincide with $\mathfrak{p}$,

and consequently the restrictions $\zeta_{\mathfrak{p}}|\mathcal{O}_{\mathfrak{p}}^{\times}$ and $\xi_{\mathfrak{p}}|\mathcal{O}_{\mathfrak{p}}^{\times}$ both factor through $(\mathcal{O}_{\mathfrak{p}}/\mathfrak{p})^{\times}$. Now the latter quotient is the image of $(\mathbb{Z}_p/p\mathbb{Z}_p)^{\times}$ under the natural map, and on $\mathbb{Z}_p^{\times}$ both $\zeta_{\mathfrak{p}}$ and $\xi_{\mathfrak{p}}$ coincide with the component of $\mathrm{sign}_{K/\mathbb{Q}}$ at p, hence with each other. Since this conclusion holds for every $\mathfrak{p}$ dividing $\mathfrak{d}^{\circ}$, the character $\lambda = \zeta\xi$ is unramified at all finite places of K. Hence λ is (or can be identified with) a narrow ideal class character. As ζ has order 2 while ξ has order $\geqslant 3$, the product λ also has order $\geqslant 3$, whence the narrow ideal class group has an element of order $\geqslant 3$. But the narrow and ordinary ideal class groups coincide, because $N_{K/\mathbb{Q}}(\epsilon) = -1$.

Next suppose that $d \equiv 0 \bmod 8$. Once again, we choose ζ as in Proposition 7, but now with the same parity as ξ, so $\zeta\xi$ is unramified at infinity. Therefore $\zeta\xi$ can be identified with a character of the wide ray class group of K to the modulus $\mathfrak{d}^{\circ}$. Recall that this group may be viewed as an extension of the ideal class group of K by the cokernel of the natural map $\mathcal{O}^{\times} \to (\mathcal{O}/\mathfrak{d}^{\circ})^{\times}$. Now as idele class characters of K, both ζ and ξ coincide with $\mathrm{sign}_{K/\mathbb{Q}}$ on $\mathbb{A}_{\mathbb{Q}}$, so when we restrict $\zeta\xi$ to the above cokernel and then view it by pullback to $(\mathcal{O}/\mathfrak{d}^{\circ})^{\times}$ as a character of the latter group it is trivial on the image of $(\mathbb{Z}/d\mathbb{Z})^{\times}$ in $(\mathcal{O}/\mathfrak{d}^{\circ})^{\times}$. Thus we may view $\zeta\xi$ as giving a character of $(\mathcal{O}/\mathfrak{d}^{\circ})^{\times}$ trivial on both the image of $(\mathbb{Z}/d\mathbb{Z})^{\times}$ and the image of $\mathcal{O}^{\times}$. We claim that $(\mathcal{O}/\mathfrak{d}^{\circ})^{\times}$ is generated by these two images, whence $\zeta\xi$ factors through the ideal class group of K, which therefore has characters, hence elements, of order $\geqslant 3$.

To verify the claim, recall from (18) that the natural map $(\mathbb{Z}/d\mathbb{Z})^{\times} \to (\mathcal{O}/\mathfrak{d}^{\circ})^{\times}$ is injective. A complement to the image of $(\mathbb{Z}/d\mathbb{Z})^{\times}$ is provided by the cyclic group of order 4 generated by the coset of any element of the form $m + n\sqrt{c}$, where $c = d/4$, m is prime to c, and n is odd. On the other hand, $\epsilon = a + b\sqrt{c}$ with positive integers a and b, and $a^2 - b^2c = -1$ by assumption. Reading the latter equation modulo 8, mindful of the fact that c is even, we deduce that b is odd, whence the coset of ϵ does indeed generate the desired complement. □

To a large extent, the results of this section can be summarized in a single inequality. Let h^{nar} be the narrow class number of K, and write $\omega(n)$ for the number of distinct prime factors of an integer $n \geqslant 1$.

Proposition 9. *Let g be the number of amplectic characters of K. Then*

$$g \geqslant h^{\mathrm{nar}} - 2^{\omega(d)-1},$$

with equality if d is odd or $N_{K/\mathbb{Q}}(\epsilon) = -1$.

Proof. By genus theory, $2^{\omega(d)-1}$ is the number of elements of the narrow ideal class group of K of order dividing 2 (cf. [6], p. 179, Satz 132). Hence $h^{\mathrm{nar}} - 2^{\omega(d)-1}$ is the number of elements of order $\geqslant 3$, or equivalently, the number of narrow ideal class characters of K of order $\geqslant 3$. Let Λ be the set of such characters and Ξ the set of amplectic characters of K, and let ζ be as in Proposition 7. Then we have an injective map $\Lambda \to \Xi$ given by $\lambda \mapsto \zeta\lambda$, and the stated inequality follows. If d is odd or $N_{K/\mathbb{Q}}(\epsilon) = -1$ then the proof of Theorem 3 shows that $\lambda \mapsto \zeta\lambda$ is invertible with inverse $\xi \mapsto \zeta\xi$. (While the hypothesis of Theorem 3 is that $N_{K/\mathbb{Q}}(\epsilon) = -1$, when d is odd this hypothesis is used only to deduce that the narrow and wide ideal class groups of K coincide, a deduction that is irrelevant here). □

5. Nonspecial discriminants

Next we assume that $K = \mathbb{Q}(\sqrt{c})$ with a square-free positive integer c divisible by some prime congruent to 3 mod 4. In this case it is a standard remark that $N_{K/\mathbb{Q}}(\epsilon) = 1$, so that

$$\begin{cases} a^2 - b^2 c = 1 & \text{if } \epsilon = a + b\sqrt{c} \text{ with positive integers } a \text{ and } b, \\ a^2 - b^2 c = 4 & \text{if } \epsilon = (a + b\sqrt{c})/2 \text{ with odd positive integers } a \text{ and } b. \end{cases} \tag{22}$$

Furthermore, if ξ is a conjugate-symplectic character of K then ξ is nonquadratic by Proposition 4. Thus if it is also of minimal conductor then it is amplectic.

Let d be the discriminant of K, and let χ denote the even primitive quadratic Dirichlet character of conductor d, so that $\chi_{\mathbb{A}} = \mathrm{sign}_{K/\mathbb{Q}}$. The analogue for nonspecial discriminants of Theorems 2 and 3 is the following statement:

Theorem 4. *Suppose that the discriminant of the real quadratic field K is not special. An amplectic character of K exists if and only if one of the following statements holds:*

(a) *$\epsilon = a + b\sqrt{c}$ with positive integers a and b, and $b \equiv c \equiv 2 \bmod 4$.*
(b) *$\epsilon = a + b\sqrt{c}$ with positive integers a and b, and $\chi(a) = 1$.*
(c) *$\epsilon = (a + b\sqrt{c})/2$ with odd positive integers a and b, and $\chi(a) = -1$.*

Furthermore, if an amplectic character of K exists then its parity can be prescribed.

Proof. We may think of the theorem as consisting of two assertions:

(i) There is an *even* amplectic character if and only if (a), (b), or (c) holds.
(ii) If an amplectic character of K exists then its parity can be prescribed.

We first prove (i).

Recall once again from (18) that the natural map

$$(\mathbb{Z}/d\mathbb{Z})^\times \longrightarrow (\mathcal{O}/\mathfrak{d}^\circ)^\times \tag{23}$$

is an embedding. So we may view $(\mathbb{Z}/d\mathbb{Z})^\times$ as a subgroup of $(\mathcal{O}/\mathfrak{d}^\circ)^\times$ and χ as a character of this subgroup. Recalling the defining property (17) of a conjugate-symplectic character, we claim that (i) is equivalent to the following assertion:

(i)′ There is an extension of χ to a character ξ of $(\mathcal{O}/\mathfrak{d}^\circ)^\times$ satisfying $\xi(\epsilon) = 1$ if and only if (a), (b), or (c) holds.

Indeed if such a character ξ exists, then $\xi(-1) = \chi(-1) = 1$, and consequently $\xi(u) = 1$ for all $u \in \mathcal{O}^\times$. Thus we can view ξ as a character of the cokernel of $\mathcal{O}^\times \to (\mathcal{O}/\mathfrak{d}^\circ)^\times$. This cokernel is naturally a subgroup of the wide ray class group of K to the modulus $\mathfrak{d}^\circ$, and after extending ξ arbitrarily to the latter group we may view it as a wide ray class character of K. In view of Proposition 5, the conductor of ξ is automatically $\mathfrak{d}^\circ$ rather than a proper divisor of $\mathfrak{d}^\circ$, so ξ is in fact a *primitive* ray class character. Given the correspondence between primitive ray class characters and idele class characters of finite order, we see that every even conjugate-symplectic idele class character of K of minimal conductor arises from an extension of χ to a character ξ as above. By Proposition 4, ξ is nonquadratic and hence amplectic.

We turn now to the proof of (i)′. The argument depends on the congruence class of c modulo 4.

Suppose first that $c \equiv 1 \bmod 4$. Then $d = c$ and $\mathfrak{d}^\circ = \sqrt{c}\mathcal{O}$, whence the embedding (23) is an isomorphism. So there is a unique extension ξ of χ, namely

χ itself when viewed as a character of $(\mathcal{O}/\mathfrak{d}^\circ)^\times$. The question is whether $\xi(\epsilon) = 1$. There are two cases.

If $\epsilon = a + b\sqrt{c}$ with positive integers a and b then $\epsilon \equiv a \bmod \mathfrak{d}^\circ$. So $\xi(\epsilon) = 1$ if and only if $\chi(a) = 1$, which is precisely condition (b). Note that (a) and (c) do not hold, so it is correct to say that $\xi(\epsilon) = 1$ if and only if (a), (b), or (c) holds.

If $\epsilon = (a + b\sqrt{c})/2$ with odd positive integers a and b then $2\epsilon \equiv a \bmod \mathfrak{d}^\circ$, and consequently $\chi(2)\xi(\epsilon) = \chi(a)$. But $\chi(2) = -1$, because $c \equiv 5 \bmod 8$ (else $c \equiv 1 \bmod 8$, and then (22) gives $a^2 - b^2 \equiv 4 \bmod 8$, a contradiction since $a^2 \equiv b^2 \equiv 1 \bmod 8$). We conclude that $\xi(\epsilon) = 1$ if and only if (c) holds. Note that (a) and (b) do not hold, so it is again correct to say that $\xi(\epsilon) = 1$ if and only if (a), (b), or (c) holds.

Suppose next that $c \equiv 2 \bmod 4$. Then $d = 4c$, so $\mathcal{O} = \mathbb{Z}[\sqrt{c}]$ and in particular $\epsilon = a + b\sqrt{c}$ with positive integers a and b. Since c is even and ϵ is a unit, a is odd. But if b is also odd then (22) gives a contradiction: If $c \equiv 2 \bmod 8$ then $1 \equiv 7 \bmod 8$ and if $c \equiv 6 \bmod 8$ then $1 \equiv 3 \bmod 8$. Thus b is even. We consider the cases $b \equiv 0 \bmod 4$ and $b \equiv 2 \bmod 4$ separately, mindful in both cases that $\mathfrak{d}^\circ = 4\sqrt{c}\mathcal{O}$.

If $b \equiv 0 \bmod 4$ then $\epsilon \equiv a \bmod \mathfrak{d}^\circ$. So any extension ξ of χ to $(\mathcal{O}/\mathfrak{d}^\circ)^\times$ will satsify $\xi(\epsilon) = \chi(a)$. Thus $\xi(\epsilon) = 1$ if and only if (b) holds. Note that (a) and (c) do not hold in this case.

If $b \equiv 2 \bmod 4$ then (a) holds, so it is enough to show that the desired extension ξ exists. While ϵ does not belong to the image of (23), its square does; in fact, $\epsilon^2 \equiv a^2 \bmod \mathfrak{d}^\circ$. Thus any extension ξ of χ satisfies $\xi(\epsilon^2) = \chi(a)^2 = 1$, and therefore we can choose ξ to satisfy $\xi(\epsilon) = 1$.

Suppose finally that $c \equiv 3 \bmod 4$. Then again we have $d = 4c$ and $\mathcal{O} = \mathbb{Z}[\sqrt{c}]$, whence $\epsilon = a + b\sqrt{c}$ with positive integers a and b. Thus (a) and (c) do not hold. By (22), exactly one of a and b is odd. We consider the cases a odd and a even separately, mindful in both cases that $\mathfrak{d}^\circ = 2\mathfrak{t}\sqrt{c}\mathcal{O}$.

Suppose first that a is odd and b is even. Then 4 divides b, else (22) gives $a^2 \equiv 5 \bmod 8$. So $b\sqrt{c} \in \mathfrak{d}^\circ$ and consequently $\epsilon \equiv a \bmod \mathfrak{d}^\circ$. Thus every extension of χ to a character ξ of $(\mathcal{O}/\mathfrak{d}^\circ)^\times$ satisfies $\xi(\epsilon) = \chi(a)$, confirming (b).

Suppose next that a is even. Then $\chi(a) = 0$; in particular, $\chi(a) \neq 1$. So given any extension ξ of χ to $(\mathcal{O}/\mathfrak{d}^\circ)^\times$ we must show that $\xi(\epsilon) \neq 1$. As a is even, $\epsilon^2 \equiv a^2 + b^2c \bmod \mathfrak{d}^\circ$, whence it suffices to see that $\chi(a^2 + b^2c) = -1$. Now

$$\chi(a^2 + b^2c) = \left(\frac{-4}{a^2 + b^2c}\right) \prod_{p|c} \left(\frac{a^2 + b^2c}{p}\right),$$

where p runs over primes dividing c. Since $a^2 + b^2c \equiv a^2 \bmod p$, all of the Legendre symbols in the product are 1. But the Kronecker symbol in front of the product is -1, because $a^2 + b^2c \equiv 3 \bmod 4$ (recall that a is even and b is odd). It follows that indeed, $\chi(a^2 + b^2c) = -1$.

This completes the proof of (i)′. It remains to prove (ii). It suffices to exhibit an idele class character ψ of finite order which is unramified at all finite places but ramified at both infinite places and trivial on $\mathbb{A}_{\mathbb{Q}}^\times$. Indeed, if such a character ψ exists, and if ξ is an amplectic character of K, then so is $\psi\xi$, but ξ and $\psi\xi$ have opposite parity.

The desired ψ is most easily exhibited as a narrow ideal class character, or in other words as a character of I/P^{nar}, where I is the group of nonzero fractional ideals of K and P^{nar} is the subgroup of principal fractional ideals with a totally

positive generator. Let P be the group of all principal fractional ideals, and as before, write $\mathcal{O}$ for the ring of integers of K. Since $N_{K/\mathbb{Q}}(\epsilon) = 1$, we obtain a well-defined quadratic character ψ of P by setting $\psi(\alpha\mathcal{O}) = N_{K/\mathbb{Q}}(\alpha)/|N_{K/\mathbb{Q}}(\alpha)|$. Clearly ψ is trivial on P^{nar}, and by extending ψ arbitarily from P to I we obtain the desired character of I/P^{nar}. □

We end this section with an analogue of Proposition 9.

Proposition 10. *Let g be the number of amplectic characters of K, and suppose that $g \neq 0$. Then $g \geqslant h^{\mathrm{nar}}$, with equality if d is odd.*

Proof. Let Λ to be the set of narrow ideal class characters of K and Ξ the set of amplectic characters of K. Fix a character $\xi_0 \in \Xi$. Then we have an injective map $\Lambda \to \Xi$ sending $\lambda \in \Lambda$ to $\lambda\xi_0$, and consequently $g \geqslant h^{\mathrm{nar}}$. If d is odd then we can argue as in the first paragraph of the proof of Theorem 3 to see that $\lambda \mapsto \lambda\xi_0$ is surjective. (Note that $\lambda\xi$ is nonquadratic by Proposition 4.) □

6. Asymptotics

Let $\mathcal{K}$ be the set of real quadratic fields, and let $\kappa(x)$ be the number of $K \in \mathcal{K}$ with $\epsilon_K^+ \leqslant x$. Then $\kappa(x) \sim x$ ([7], p. 256, Theorem 5.3). Let $\mathcal{H} \subset \mathcal{K}$ be the subset consisting of those K which have an amplectic character, and let $\eta(x)$ be the number of $K \in \mathcal{H}$ with $\epsilon_K^+ \leqslant x$. Put $\theta = \prod_p(1 - 2/p^2) \approx .3226$. Since $\kappa(x) \sim x$, the following assertion amounts to a slightly more precise version of Theorem 1:

Theorem 5. $3\theta/4 - o(1) \leqslant \eta(x)/x \leqslant 1 - \theta + o(1)$.

Proof. Let $\mathcal{M}$ be the set of integers $m \geqslant 3$ such that $m(m-1)$ is square-free, and let $\mu(x)$ be the number of $m \in \mathcal{M}$ with $m \leqslant x$. If $m \in \mathcal{M}$ and $K = \mathbb{Q}(\sqrt{m(m-1)})$ then $d = 4m(m-1)$ and $\epsilon = (2m-1)+2\sqrt{m(m-1)}$. In particular, $N_{K/\mathbb{Q}}(\epsilon) = 1$. It follows that $K \in \mathcal{H}$, either by Theorem 2 if d is special or by Theorem 4 otherwise, because condition (a) of the latter theorem is satisfied. Also, if $m \leqslant x/4$ then $\epsilon = \epsilon^+ \leqslant x$. Thus

$$\mu(x/4) \leqslant \eta_0(x), \tag{24}$$

where $\eta_0(x)$ is the number of $K \in \mathcal{H}$ with $\epsilon^+ \leqslant x$ and $d \equiv 0 \bmod 8$.

Next let $\mathcal{N}$ be the set of integers $n \geqslant 7$ such that $n^2 - 4$ is square-free and $n \equiv 3 \bmod 4$, and let $\nu(x)$ be the number of $n \in \mathcal{N}$ with $n \leqslant x$. If $n \in \mathcal{N}$ and $K = \mathbb{Q}(\sqrt{n^2-4})$ then $d = n^2 - 4$ and $\epsilon = (n + \sqrt{n^2-4})/2$, so again $N_{K/\mathbb{Q}}(\epsilon) = 1$. Thus $K \in \mathcal{H}$ if d is special. This is also the case if d is nonspecial, for we claim that condition (c) of Theorem 4 is satisfied. Indeed let χ be the primitive quadratic Dirichlet character of conductor d. Since $d = n^2 - 4$, we have

$$\chi(n) = \left(\frac{n}{n^2-4}\right) = \left(\frac{n^2-4}{n}\right) \tag{25}$$

whence $\chi(n) = (-1/n) = -1$, as claimed. Now if $n \leqslant x$ then $\epsilon = \epsilon^+ \leqslant x$. So

$$\nu(x) \leqslant \eta_5(x), \tag{26}$$

where $\eta_5(x)$ is the number of $K \in \mathcal{H}$ with $\epsilon^+ \leqslant x$ and $d \equiv 5 \bmod 8$.

Combining (24) and (26), and observing that the sets counted by $\eta_0(x)$ and $\eta_5(x)$ are disjoint, we see that $\mu(x/4) + \nu(x) \leqslant \eta(x)$. The lower bound for $\eta(x)/x$ now follows from the asymptotic relations $\mu(x) \sim \theta x$ and $\nu(x) \sim \theta x/2$. (See [2] and pp.

436-437 of [9]. To apply [9], observe that the square-free values of n^2-4 with $n \equiv 3 \bmod 4$ are just the square-free values of $(4k+1)(4k+5)$ for arbitrary k.)

To derive the upper bound for $\eta(x)/x$, put $\mathcal{H}' = \mathcal{K} \smallsetminus \mathcal{H}$ and $\eta'(x) = \kappa(x) - \eta(x)$, so that $\eta'(x)$ is the number of $K \in \mathcal{H}'$ such that $\epsilon^+ \leqslant x$. Let $\mathcal{M}'$ be the set of integers $m \geqslant 2$ such that m^2-1 is square-free (and m is therefore even), and let $\mu'(x)$ be the number of $m \in \mathcal{M}'$ with $m \leqslant x$. If $m \in \mathcal{M}'$ and $K = \mathbb{Q}(\sqrt{m^2-1})$ then $d = 4(m^2-1)$ and $\epsilon = \epsilon^+ = m + \sqrt{m^2-1}$. Note that d is nonspecial because $m^2 - 1 \equiv 3 \bmod 4$. Let χ be the even primitive quadratic Dirichlet character of conductor d. Since m and d are both even, we have $\chi(m) = 0$, whence condition (b) of Theorem 4 is violated, as are also (a) and (c). Hence $K \in \mathcal{H}'$. Also, if $m \leqslant x/2$ then $\epsilon^+ \leqslant x$, so

$$\mu'(x/2) \leqslant \eta_4'(x), \tag{27}$$

where $\eta_4'(x)$ is the number of $K \in \mathcal{H}'$ with $\epsilon^+ \leqslant x$ and $d \equiv 4 \bmod 8$.

Next let $\mathcal{N}'$ be the set of integers $n \geqslant 5$ such that n^2-4 is square-free and $n \equiv 1 \bmod 4$, and let $\nu'(x)$ be the number of $n \in \mathcal{N}'$ with $n \leqslant x$. If $n \in \mathcal{N}'$ and $K = \mathbb{Q}(\sqrt{n^2-4})$ then $d = n^2-4$ and $\epsilon = \epsilon^+ = (n + \sqrt{n^2-4})/2$. Furthermore, $d = (4k+3)(4k-1)$ with $k = (n-1)/4$, whence d is nonspecial. Let χ be the primitive quadratic Dirichlet character of conductor d, as before. The calculation (25) is still valid, but this time we have $\chi(n) = (-1/n) = 1$. So condition (c) of Theorem 4 is violated, as are conditions (a) and (b), and therefore $K \in \mathcal{H}'$. As $n \leqslant x$ implies $\epsilon = \epsilon^+ \leqslant x$, we have

$$\nu'(x) \leqslant \eta_5'(x), \tag{28}$$

where $\eta_5'(x)$ is the number of $K \in \mathcal{H}'$ with $\epsilon^+ \leqslant x$ and $d \equiv 5 \bmod 8$.

The upper bound for $\eta(x)$ now follows much as the lower bound did. Combining (27) and (28), we have $\mu'(x/2) + \nu'(x) \leqslant \eta'(x)$, or in other words

$$\eta(x) \leqslant \kappa(x) - \mu'(x/2) - \nu'(x).$$

Using the relations $\kappa(x) \sim x$, $\mu'(x) \sim \theta x$, and $\nu'(x) \sim \theta x/2$ ([7], [3], and [9]), we obtain the stated upper bound for $\eta(x)/x$. □

Remark. In principle we could improve our lower bound for $\eta(x)/x$ by using the square-free values of two more expressions, n^2+1 and n^2+4. Indeed $\mathbb{Q}(\sqrt{n^2+1})$ and $\mathbb{Q}(\sqrt{n^2+4})$ are also fields for which the fundamental unit can be identified explicitly: We have $\epsilon = n + \sqrt{n^2+1}$ $(n > 2)$ and $\epsilon = (n + \sqrt{n^2+4})/2$ respectively. But in these cases $\epsilon^+ = \epsilon^2$, so the condition $\epsilon^+ \leqslant x$ would force us to take $n < \sqrt{x}$, and thus the contribution to $\eta(x)$ would be negligible.

Finally we come to the proof of (6). We begin with the lower bound in (6). Let $\mathcal{N}$ and ν be as in the second paragraph of the proof of Theorem 5. For $n \in \mathcal{N}$ we modify the notation of that paragraph in a self-explanatory way: $K_n = \mathbb{Q}(\sqrt{n^2-4})$, $d_n = n^2-4$, and $\epsilon_n = \epsilon_n^+ = (n + \sqrt{n^2-4})/2$. Also, we write g_n for the number of amplectic characters of K_n. If $n \leqslant x$ then $\epsilon_n \leqslant x$, so (20) gives

$$\beta^{\mathrm{qu}}(x) \geqslant \frac{1}{2} \sum_{\substack{n \in \mathcal{N} \\ n \leqslant x}} g_n.$$

Denote the right-hand side of this inequality by $\gamma(x)$. Then the lower bound for $\beta^{\mathrm{qu}}(x)$ in (6) is a consequence of the following statement:

Proposition 11. *Fix $\varepsilon > 0$. Then $\gamma(x) \gg x^{2-\epsilon}$ for x sufficiently large.*

To prove the proposition we need a lemma. Write h_n and h_n^{nar} for the ordinary and narrow class numbers of K_n. Then $h_n^{\mathrm{nar}} = 2h_n$, because $\epsilon_n = \epsilon_n^+$.

Lemma. *Fix $\varepsilon > 0$. Then $h_n^{\mathrm{nar}} \gg n^{1-\varepsilon}$.*

Proof. Let χ_n be the primitive quadratic Dirichlet character of conductor d_n, and choose δ so that $0 < \delta < \varepsilon/2$. Combining Siegel's estimate $L(1,\chi_n) \gg d_n^{-\delta}$ with the Dirichlet class number formula $L(1,\chi_n) = (2h_n \log \epsilon_n)/\sqrt{d_n}$, we obtain

$$h_n \gg (n^2-4)^{1/2-\delta}/\log(n+\sqrt{n^2-4}).$$

Hence $h_n \gg n^{1-2\delta}/\log(2n)$, from which the stated estimate follows. □

We now prove Proposition 11. If d_n is special then $g_n = 2h_n^{\mathrm{nar}} - 2^{\omega(d_n)-1}$ (Proposition 9), and since $\omega(d_n) \ll \log d_n/\log\log d_n$ and $d_n = n^2-4$ the lemma implies that $g_n \gg n^{1-\varepsilon}$. This conclusion is even easier if d_n is nonspecial; we simply refer to Proposition 10 instead of Proposition 9. Thus it is enough to prove that for large x,

$$\sum_{\substack{n\in\mathcal{N}\\ n\leqslant x}} n^{1-\varepsilon} \gg x^{2-\varepsilon}. \tag{29}$$

A crude argument suffices: The sum on the left-hand side has $\nu(x)$ terms, so there are at least $\lfloor \nu(x)/2 \rfloor$ terms in the sum corresponding to $n \geqslant \nu(x)/2$. The contribution of these terms is at least $\lfloor \nu(x)/2 \rfloor (\nu(x)/2)^{1-\varepsilon}$, and as $\nu(x) \gg x$, the estimate (29) follows, proving Proposition 11.

It remains to verify the upper bound in (6). Using Raulf's formula (4), we can make a more precise assertion for x sufficiently large:

Proposition 12. $\beta^{\mathrm{qu}}(x) \leqslant \dfrac{25\zeta(3)}{8} \prod_{p\geqslant 2}(1-2p^{-2}-p^{-3}) \dfrac{x^2}{\log x}(1+o(x))$.

The proposition is a consequence of (4), (20), and the following lemma:

Lemma. $g_K \leqslant 8h_K$.

Proof. Since K is now fixed we drop the subscript K. If $g = 0$ there is nothing to prove, so suppose that ξ_0 is an amplectic character of K. Let Ξ be the set of all amplectic characters of K, and let $\Xi^+ \subset \Xi$ and $\Xi^- \subset \Xi$ be the subsets consisting of characters with the same parity as ξ_0 and the opposite parity respectively. Let $g^\pm$ be the cardinality of $\Xi^\pm$. We will show that $g^+ \leqslant 4h$. If $g^- \neq 0$ then ξ_0 can be replaced by an element of Ξ^- and the argument will show that $g^- \leqslant 4h$ also.

If $\xi \in \Xi^+$ then the product $\xi_0\xi$ is unramified at infinity and so may be viewed as an element of the wide ray class group of K to the modulus $\mathfrak{d}^\circ$. As we recalled in the proof of Theorem 3, this wide ray class group is an extension of the ordinary ideal class group of K by the cokernel of the map $\mathcal{O}^\times \to (\mathcal{O}/\mathfrak{d}^\circ)^\times$. So by restriction to this cokernel and pullback to $(\mathcal{O}/\mathfrak{d}^\circ)^\times$ we may view $\xi_0\xi$ as a character of $(\mathcal{O}/\mathfrak{d}^\circ)^\times$. As idele class characters, ξ_0 and ξ both coincide with $\mathrm{sign}_{K/\mathbb{Q}}$ on $\mathbb{A}_\mathbb{Q}$, so when we view $\xi_0\xi$ as a character of $(\mathcal{O}/\mathfrak{d}^\circ)^\times$ it is trivial on the image in this group of $(\mathbb{Z}/d\mathbb{Z})^\times$. Now the index of $(\mathbb{Z}/d\mathbb{Z})^\times$ as a subgroup of $(\mathcal{O}/\mathfrak{d}^\circ)^\times$ is at most 4. Thus we may view $\xi_0\xi$ as a character of a group which is an extension of the ideal class group of K by a group of order at most 4. It follows that the map $\xi \mapsto \xi_0\xi$ has image of order at most $4h$. □

7. Galois theory

We shall state a few corollaries illustrating the applicability of our results to questions about the existence or nonexistence of Galois extensions of $\mathbb{Q}$ with Galois group Q_{4m}. As before, we denote the discriminant of a real quadratic field K by d_K, and we call d_K *nonspecial* or *special* according as it is or is not divisible by a prime congruent to 3 mod 4. The following corollary of Proposition 4 was mentioned in the introduction:

Corollary 1. *Suppose that m is an odd integer $\geqslant 3$ and L is a Galois extension of $\mathbb{Q}$ with $\mathrm{Gal}(L/\mathbb{Q}) \cong Q_{4m}$. Let K be the real quadratic field contained in L. Then d_K is special.*

Proof. If a prime congruent to 3 mod 4 divides d_K then Proposition 4 implies that $[L:K]$ is divisible by 4, whence $[L:\mathbb{Q}]$ by 8. □

Recall that ϵ_K denotes the fundamental unit of K and h_K the class number. The next statement is an immediate consequence of Theorems 2 and 3:

Corollary 2. *Let K be a real quadratic field with special discriminant d_K. If either $N_{K/\mathbb{Q}}(\epsilon_K) = 1$ or $h_K \geqslant 3$ then there exists a Galois extension L of $\mathbb{Q}$ containing K, unramified outside the prime divisors of d_K, such that $\mathrm{Gal}(L/\mathbb{Q}) \cong Q_{4m}$ for some $m \geqslant 2$.*

Example. Let $K = \mathbb{Q}(\sqrt{229})$. Then $\epsilon_K = (15+\sqrt{229})/2$, whence $N_{K/\mathbb{Q}}(\epsilon_K) = -1$. But $h_K = 3$, so Corollary 2 is in force. In fact put $L = \mathbb{Q}(\alpha, \beta)$, where α is a root of the polynomial $x^3 - 4x + 1$ (of discriminant 229) and β generates the quartic subfield of $\mathbb{Q}(e^{2\pi i/229})$. Then

$$\mathrm{Gal}(L/\mathbb{Q}) \cong (\mathbb{Z}/3\mathbb{Z}) \rtimes (\mathbb{Z}/4\mathbb{Z}) \cong Q_{12}.$$

(Note that $Q_{4m} \cong (\mathbb{Z}/m\mathbb{Z}) \rtimes (\mathbb{Z}/4\mathbb{Z})$ if and only if m is odd.)

Our final corollary illustrates the possible uses of Theorem 4. The reader will readily supply other illustrations.

Corollary 3. *Let $K = \mathbb{Q}(\sqrt{c})$, where c is a positive square-free integer satisfying $c \equiv 7$ modulo 8. Let χ be the primitive quadratic Dirichlet character of conductor $4c$, and write $\epsilon_K = a + b\sqrt{c}$ with positive integers a and b. If $\chi(a) = 1$ then there is a Galois extension L of $\mathbb{Q}$ containing K, unramified outside the prime divisors of $2c$, such that $\mathrm{Gal}(L/\mathbb{Q}) \cong Q_{4m}$ with an even integer $m \geqslant 4$.*

Proof. Since condition (b) of Theorem 4 is satisfied, there exists some such L, but *a priori* we can say only that $m \geqslant 2$. However Corollary 1 implies that m is even, and $m \neq 2$ because the well-known criterion for $\mathbb{Q}(\sqrt{c})$ to be contained in a Galois extension of $\mathbb{Q}$ with Galois group Q_8 – namely that $c \not\equiv 7$ mod 8 and $c > 0$; cf. Rosenblüth [13] or Fröhlich [5], p. 146 – is not satisfied in this case. □

References

[1] C. Ambrose, *On Artin's primitive root conjecture and a problem of Rohrlich*, Math. Proc. Cambridge Philos. Soc. 157 (2014), 79–99.

[2] L. Carlitz, *On a problem in additive arithmetic. II.*, Quart. J. Math. Oxford 3 (1932), 273 – 290.

[3] Th. Estermann, *Einige Sätze über quadratfreie Zahlen*, Math. Annalen 105 (1931), 653 – 662.

[4] É. Fouvry and J. Klüners, *On the negative Pell equation*, Annals of Math. 172 (2010), 2035–2104.

[5] A. Fröhlich, *Artin root numbers and normal integral bases for quaternion fields*, Inventiones math. 17 (1972), 143 – 166.
[6] E. Hecke, *Vorlesungen über die Theorie der algebraischen Zahlen*, 2nd ed., Chelsea Publ. Co. (1970).
[7] N. Raulf, *Asymptotics of class numbers for progressions and for fundamental discriminants*, Forum Math. 21 (2009), 221–257.
[8] N. Raulf, *Limit distribution of class numbers for discriminants in progressions and fundamental discriminants*, Internat. J. of Number Thy. 12 (2016), 1237 – 1258.
[9] G. Ricci, *Ricerche aritmetiche sui polinomi*, Rend. Circ. Matem. Palermo 57 (1933) 433-475.
[10] D. E. Rohrlich, *Artin representations of $\mathbb{Q}$ of dihedral type*, Mathematical Research Letters 22 (2015), 1767-1789.
[11] D. E. Rohrlich, *Quaternionic Artin representations of $\mathbb{Q}$*, Math. Proc. Cambridge Phil. Soc. 163 (2017), 95-114.
[12] D. E. Rohrlich, *Almost abelian Artin representations of $\mathbb{Q}$*, Michigan Mathematical J., to appear.
[13] E. Rosenblüth, *Die arithmetische Theorie und Konstruktion der Quaternionenkörper auf klassenkörpertheoretischer Grundlage*, Monathsh. Math. Phys. 41 (1934), 85-125.
[14] P. Sarnak, *Class numbers of indefinite binary quadratic forms*, J. Number Thy. 15 (1982), 229-247.
[15] P. Sarnak, *Class numbers of indefinite binary quadratic forms II*, J. Number Thy. 21 (1985), 333-346.
[16] C. L. Siegel, *Über die Classenzahl quadratischer Zahlkörper*, Acta Arithmetica 1 (1935), 83-86.
[17] C. L. Siegel, *The average measure of quadratic forms with given determinant and signature*, Ann. of Math. 45 (1944), 667 - 685.
[18] P. Stevenhagen, *The number of real quadratic fields having units of negative norm*, Experimental Math. 2 (1993), 121-136.

Department of Mathematics and Statistics, Boston University, Boston, MA 02215
E-mail address: rohrlich@math.bu.edu