Received: 19 April 2021 | Revised: 19 August 2021 | Accepted: 25 August 2021

DOI: 10.1112/mtk.12123

RESEARCH ARTICLE

Mathematika

A sharp upper bound for the 2-torsion of class groups of multiquadratic fields

Peter Koymans | Carlo Pagano

Max Planck Institute for Mathematics, Bonn, Germany

Correspondence
Peter Koymans, Max Planck Institute for Mathematics, Vivatsgasse 7, 53111 Bonn, Germany.
Email: koymans@mpim-bonn.mpg.de

Funding information
Max Planck Institute for Mathematics

Abstract

Let K be a multiquadratic extension of $\mathbb{Q}$ and let $\mathrm{Cl}^+(K)$ be its narrow class group. Recently, the authors (Koymans and Pagano, Int. Math. Res. Not. **2022** (2022), no. 4, 2772–2823) gave a bound for $|\mathrm{Cl}^+(K)[2]|$ only in terms of the degree of K and the number of ramifying primes. In the present work we show that this bound is sharp in a wide number of cases. Furthermore, we extend this to ray class groups.

MSC 2020
11R29 (primary)

1 | INTRODUCTION

The class group is one of the most fundamental invariants of a number field K. Providing non-trivial upper bounds for the l-torsion of class groups in terms of the discriminant $\Delta_{K/\mathbb{Q}}$ of a general number field K has been an active area of research with connections to elliptic curves and diophantine approximation [1–3, 6, 9–11, 14, 15].

For extensions $K/\mathbb{Q}$ of degree a power of a prime l much more is known. For instance, for $l = 2$ and $K/\mathbb{Q}$ a quadratic extension, Gauss [4] showed that

$$\dim_{\mathbb{F}_2} \mathrm{Cl}^+(K)[2] = \omega(\Delta_{K/\mathbb{Q}}) - 1.$$

Here $\mathrm{Cl}^+(K)$ denotes the narrow class group of the field K and $\omega(a)$ denotes the number of prime factors of a non-zero integer a. Recently, the authors [7] generalized Gauss' result to multiquadratic fields. More specifically, we obtained the following result, which is Theorem 1.1 of [7]. Call a vector $(a_1, \dots, a_n) \in \mathbb{Z}_{\geqslant 2}^n$ *acceptable* if the a_i are squarefree, pairwise coprime and only have prime factors congruent to 1 modulo 4.

Theorem 1.1. *Let n be a positive integer and let $(a_1, \ldots, a_n) \in \mathbb{Z}_{\geqslant 2}^n$ be acceptable. Then we have*

$$dim_{\mathbb{F}_2} Cl^+(\mathbb{Q}(\sqrt{a_1}, \ldots, \sqrt{a_n}))[2] \leqslant \omega(a_1 \cdot \ldots \cdot a_n) \cdot 2^{n-1} - 2^n + 1.$$

A similar upper bound has subsequently been established by Klüners and Wang in [5, Theorem 2.1] for extensions $K/\mathbb{Q}$ of degree a power of l. However, when specialized to the multiquadratic fields considered above, their bound in the worst-case scenario is twice as large as the one in Theorem 1.1. This work is devoted to showing that the bound in Theorem 1.1 is sharp for every $n \in \mathbb{Z}_{\geqslant 1}$.

An acceptable vector $(a_1, \ldots, a_n)$ is said to be *maximal* in case the inequality of Theorem 1.1 is an equality. Among other things, we have given a recursive characterization of maximal vectors (see [7, Theorem 1.2]), which we reproduce here. Write π_S for the projection on the coordinates in S, write $H_2^+(K)$ for the maximal multiquadratic unramified (at all finite places) extension of K, and write $[n] := \{1, \ldots, n\}$.

Theorem 1.2. *Let n be a positive integer and let $(a_1, \ldots, a_n)$ be an acceptable vector. Then the following are equivalent.*

(a) *The vector $(a_1, \ldots, a_n)$ is maximal, that is,*

$$dim_{\mathbb{F}_2} Cl^+(\mathbb{Q}(\sqrt{a_1}, \ldots, \sqrt{a_n}))[2] = \omega(a_1 \cdot \ldots \cdot a_n) \cdot 2^{n-1} - 2^n + 1.$$

(b) *For every $j \in [n]$, the vector $\pi_{[n]-\{j\}}(a_1, \ldots, a_n)$ is maximal and every prime divisor p of a_j splits completely in $H_2^+(\mathbb{Q}(\{\sqrt{a_m}\}_{m \in [n]-\{j\}}))$.*

(c) *For every $j \in [n]$, the vector $\pi_{[n]-\{j\}}(a_1, \ldots, a_n)$ is maximal and for every prime divisor p of a_j, one (or equivalently any) prime above p in the field $\mathbb{Q}(\{\sqrt{a_m}\}_{m \in [n]-\{j\}})$ belongs to $2Cl^+(\mathbb{Q}(\{\sqrt{a_m}\}_{m \in [n]-\{j\}}))$.*

In particular, Theorem 1.2 recovers the equality of Gauss' theorem for $n = 1$ as a special case. It is then natural to ask whether for every positive integer n, one can find maximal vectors of dimension n. As the reader can sense from the characterization given in Theorem 1.2, it is not at all obvious how to do this. A naive inductive approach based on the Chebotarev density theorem runs into severe difficulties, since one needs to simultaneously guarantee splitting of a prime p in a field K_q depending on q and of q in a field K_p depending on p.

To circumvent this problem, we use combinatorial ideas from [12], which we explain here from first principles in order to make the present work self-contained (see Section 2). Our main theorem shows that one can find maximal vectors $(a_1, \ldots, a_n)$ for every n. Moreover, for any fixed n, we show that Theorem 1.1 is sharp for a wide number of choices of $(\omega(a_1), \ldots, \omega(a_n))$. More precisely, we establish the following.

Theorem 1.3.

(a) *Take $n \in \mathbb{Z}_{>3}$ and take $(k_1, \ldots, k_n) \in \mathbb{Z}_{\geqslant 1} \times (2 \cdot \mathbb{Z}_{\geqslant 1})^{n-1}$. Then there are infinitely many acceptable vectors $(a_1, \ldots, a_n)$ with $\omega(a_i) = k_i$ for each $i \in [n]$ and*

$$dim_{\mathbb{F}_2} Cl^+(\mathbb{Q}(\sqrt{a_1}, \ldots, \sqrt{a_n}))[2] = \omega(a_1 \cdot \ldots \cdot a_n) \cdot 2^{n-1} - 2^n + 1.$$

(b) *Take $(k_1, k_2, k_3) \in \mathbb{Z}_{\geqslant 1}^3$. Then there are infinitely many acceptable vectors (a_1, a_2, a_3) with $\omega(a_i) = k_i$ for each $i \in \{1, 2, 3\}$ and*

$$dim_{\mathbb{F}_2} Cl^+(\mathbb{Q}(\sqrt{a_1}, \sqrt{a_2}, \sqrt{a_3}))[2] = \omega(a_1 a_2 a_3) \cdot 4 - 7.$$

We speculate that the condition $(k_1, \dots, k_n) \in \mathbb{Z}_{\geqslant 1} \times (2 \cdot \mathbb{Z}_{\geqslant 1})^{n-1}$ can also be removed for $n > 3$, but this seems to be out of reach with the techniques employed in this work. We next turn our attention to ray class groups. First of all, let us notice that the 2-torsion of the ordinary class group of a number field K cannot be larger than the 2-torsion of the narrow class group of K. Hence the upper bound in Theorem 1.1 is also an upper bound for $|\mathrm{Cl}(\mathbb{Q}(\sqrt{a_1}, \dots, \sqrt{a_n}))[2]|$. Less obvious is whether also this bound is sharp.

Similarly, fix an integer c, which we take in this paper to be a squarefree product of primes congruent to 1 modulo 4 (see the end of this introduction for some motivation on this assumption). Recall that the ray class group $\mathrm{Cl}(\mathbb{Q}(\sqrt{a_1}, \dots, \sqrt{a_n}), c)$ is by definition the quotient of the free abelian group on the set of prime ideals of $\mathbb{Q}(\sqrt{a_1}, \dots, \sqrt{a_n})$ coprime to c by the group of principal fractional ideals that admit a generator α congruent to 1 modulo c. From the definition one sees that $\mathrm{Cl}(\mathbb{Q}(\sqrt{a_1}, \dots, \sqrt{a_n}), c)$ fits into an exact sequence

$$0 \to \frac{(\mathcal{O}_{\mathbb{Q}(\sqrt{a_1}, \dots, \sqrt{a_n})}/c)^*}{\mathcal{O}^*_{\mathbb{Q}(\sqrt{a_1}, \dots, \sqrt{a_n})}} \to \mathrm{Cl}(\mathbb{Q}(\sqrt{a_1}, \dots, \sqrt{a_n}), c) \to \mathrm{Cl}(\mathbb{Q}(\sqrt{a_1}, \dots, \sqrt{a_n})) \to 0,$$

which we will call the *ray class group sequence*.

Then one obtains from Theorem 1.1 and the ray class group sequence

$$\dim_{\mathbb{F}_2} \mathrm{Cl}(\mathbb{Q}(\sqrt{a_1}, \dots, \sqrt{a_n}), c)[2] \leqslant \omega(a_1 \cdot \dots \cdot a_n) \cdot 2^{n-1} - 2^n + 1 + 2^n \cdot \omega(c),$$

where the bound can be reached only if all the prime divisors of c split completely in $\mathbb{Q}(\sqrt{a_1}, \dots, \sqrt{a_n})$. It is, once more, not obvious whether this bound is sharp. Our next theorem settles these questions.

Theorem 1.4. *Take $n \in \mathbb{Z}_{\geqslant 1}$ and take $(k_1, \dots, k_n) \in (2 \cdot \mathbb{Z}_{\geqslant 1})^n$. Let c be a squarefree positive integer divisible only by primes congruent to 1 modulo 4. Then there are infinitely many acceptable vectors $(a_1, \dots, a_n)$ with $\omega(a_i) = k_i$ for each $i \in [n]$ and*

$$dim_{\mathbb{F}_2} Cl(\mathbb{Q}(\sqrt{a_1}, \dots, \sqrt{a_n}), c)[2] = \omega(a_1 \cdot \dots \cdot a_n) \cdot 2^{n-1} - 2^n + 1 + 2^n \cdot \omega(c).$$

As a corollary of Theorem 1.4 we obtain the following result on unit groups.

Corollary 1.5. *Let $n \in \mathbb{Z}_{\geqslant 1}$. Let c be a squarefree positive integer with all factors congruent to 1 modulo 4. Then there exist infinitely many acceptable vectors $(a_1, \dots, a_n)$ such that all prime divisors of c split completely in $\mathbb{Q}(\sqrt{a_1}, \dots, \sqrt{a_n})$ and the unit group $\mathcal{O}^*_{\mathbb{Q}(\sqrt{a_1}, \dots, \sqrt{a_n})}$ reduced modulo c is entirely contained in the group*

$$\left(\frac{\mathcal{O}_{\mathbb{Q}(\sqrt{a_1}, \dots, \sqrt{a_n})}}{c\mathcal{O}_{\mathbb{Q}(\sqrt{a_1}, \dots, \sqrt{a_n})}}\right)^{*2}.$$

We remark that, in the context of Corollary 1.5, it is no real loss of generality to demand that all the prime divisors of c are 1 modulo 4. Indeed, we are aiming to construct multiquadratic extensions splitting completely at all prime divisors of c and whose unit group consists entirely of squares modulo c. This then in particular applies to -1, which is then a square in $\mathbb{F}_l$ for every

$l \mid c$ so that $l \equiv 1 \bmod 4$. We similarly remark that the bound for the ordinary class group in Theorem 1.4 (i.e., the case $c = 1$) is not sharp, whenever one of the a_i is divisible by a prime congruent to 3 modulo 4.

2 ADDITIVE SYSTEMS

For completeness we include a self-contained proof of [12, Proposition 3.1]; we claim no originality in this section.

We let $X_1, \dots, X_d$ be arbitrary non-empty finite sets and put $X := X_1 \times \cdots \times X_d$. In our application the sets X_i will consist of acceptable integers a_i with $\omega(a_i) = k_i/2$. A cube C is a product set $Y_1 \times \cdots \times Y_d$ with $Y_i \subseteq X_i$ and $|Y_i| = 2$; in our application we can think of C as an acceptable vector $(a_1, \dots, a_d)$ with $\omega(a_i) = k_i$. It is here that we make essential use of k_i being even. As we see in our next section, we need to find cubes C satisfying certain bilinear conditions. The aim of our next definition is to encapsulate this in an abstract framework.

We write X_i^2 for the set $X_i \times X_i$. For $S \subseteq [d]$ and $i \in [d]$, π_i denotes the natural projection from $\prod_{i \in S} X_i^2 \times \prod_{i \in [d]-S} X_i$ to X_i^2 if $i \in S$ and to X_i if $i \in [d] - S$, while pr_1 and pr_2 denote the natural projections from X_i^2 to its two factors.

Definition 2.1. Let $X_1, \dots, X_d$ be arbitrary non-empty finite sets and put $X := X_1 \times \cdots \times X_d$. An additive system $\mathfrak{A}$ on X is a family of tuples $(C_S, C_S^{\mathrm{acc}}, F_S, A_S)_{S \subseteq [d]}$, indexed by subsets $S \subseteq [d]$, satisfying the following properties:

- $C_S^{\mathrm{acc}} \subseteq C_S \subseteq \prod_{i \in S} X_i^2 \times \prod_{i \in [d]-S} X_i$ are sets, $F_S : C_S \to A_S$ is a map, and A_S is a finite $\mathbb{F}_2$-vector space;
- we have that
$$C_S^{\mathrm{acc}} := \{x \in C_S : F_S(x) = 0\}$$
and, for $S \neq \emptyset$
$$C_S := \left\{ x \in \prod_{i \in S} X_i^2 \times \prod_{i \in [d]-S} X_i : \text{ for all } j \in S \text{ and all } y \in \prod_{i \in S-\{j\}} X_i^2 \times \prod_{i \in [d]-(S-\{j\})} X_i \right.$$
$$\text{satisfying } \pi_k(x) = \pi_k(y) \text{ for } k \in [d] - \{j\} \text{ and } \pi_j(y) \in \{\mathrm{pr}_1(\pi_j(x)), \mathrm{pr}_2(\pi_j(x))\},$$
$$\left. \text{we have } y \in C_{S-\{j\}}^{\mathrm{acc}} \right\};$$
- suppose that $x_1, x_2, x_3 \in C_S$ and suppose that there exists $j \in S$ such that
$$\pi_k(x_1) = \pi_k(x_2) = \pi_k(x_3) \text{ for all } k \in [d] - \{j\}$$
and
$$\pi_j(x_1) = (a, b), \quad \pi_j(x_2) = (b, c), \quad \pi_j(x_3) = (a, c) \text{ for some } a, b, c \in X_j.$$
Then we have
$$F_S(x_1) + F_S(x_2) = F_S(x_3). \tag{2.1}$$

Note that we do not quite work with cubes in the above definition, but instead with elements of $X_1 \times X_1 \times \cdots \times X_d \times X_d$. The major difference is that we have also included elements with equal coordinates. This will be very convenient in the proof of our next counting result for C_S^{acc}. Later, we shall need to remove such elements, but it is not hard to show that they contribute a vanishingly small proportion.

Proposition 2.2. *Let $X_1, \dots, X_d$ be arbitrary non-empty finite sets and put $X := X_1 \times \cdots \times X_d$. Let $\mathfrak{A}$ be an additive system on X such that $|A_S| \leqslant N$ for all $S \subseteq [d]$ and write δ for the density of $C_{\emptyset}^{\mathrm{acc}}$ in X. Then we have that*

$$\frac{|C_{[d]}^{\mathrm{acc}}|}{\prod_{i \in [d]} |X_i^2|} \geqslant \delta^{2^d} \cdot N^{-3^d}.$$

Proof. We proceed by induction on d with the case $d = 0$ being trivial (recall that the empty cartesian product is by definition the set of cardinality 1 containing the empty tuple). Fix an element

$$x \in \prod_{i \in [d-1]} X_i^2.$$

Define

$$V(x) := \{(x, a) \in C_{[d-1]}^{\mathrm{acc}} : a \in X_d\}, \quad W(x) := \{(x, (a, b)) \in C_{[d]}^{\mathrm{acc}} : (a, b) \in X_d^2\}.$$

By definition of an additive system, we see that $W(x)$ naturally injects in $V(x) \times V(x)$. From now on we shall identify $W(x)$ with its image in $V(x) \times V(x)$. We claim that $W(x)$ defines an equivalence relation on $V(x)$.

If we apply Equation (2.1) with $a = b = c$, we conclude that for all $S \subseteq [d-1]$, all $y \in \prod_{i \in S} X_i^2 \times \prod_{i \in [d-1]-S} X_i$ and all $a \in X_d$

$$F_{S \cup \{d\}}(y, (a, a)) = 0.$$

From this, it follows quickly that $W(x)$ is reflexive. Applying Equation (2.1) with $a = c$, we then get

$$F_{S \cup \{d\}}(y, (a, b)) + F_{S \cup \{d\}}(y, (b, a)) = F_{S \cup \{d\}}(y, (a, a)) = 0,$$

so that $W(x)$ is symmetric. Finally, Equation (2.1) with a, b, and c arbitrary implies the transitivity of $W(x)$, which establishes the claim.

Our next step is to estimate the number of equivalence classes. To do so, take $(x, a), (x, b) \in V(x)$ and $\{d\} \subseteq S \subseteq [d]$. Then we write $(x, a) \sim_S (x, b)$ if $(x, a) \sim_{S'} (x, b)$ for all $\{d\} \subseteq S' \subsetneq S$ and

$$F_S(y, (a, b))) = 0$$

for all $y \in \prod_{i \in S-\{d\}} X_i^2 \times \prod_{i \in [d-1]-S} X_i$ satisfying $\pi_i(y) = \pi_i(x)$ for $i \in S - \{d\}$ and $\pi_i(y) \in \{\mathrm{pr}_1(\pi_i(x)), \mathrm{pr}_2(\pi_i(x))\}$ for $i \in [d-1] - S$. Note that the equivalence relation $\sim_{[d]}$ is precisely $W(x)$.

To upper bound the number of equivalence classes, take a collection of points $(x, a_i) \in V(x)$ such that $(x, a_i) \sim_S (x, a_j)$ for all strict subsets S of $[d]$. Suppose that among this collection there are R equivalence classes for $\sim_{[d]}$, with representatives $(x, b_1), \dots, (x, b_R)$. Then we see that the map

$$(x, b_i) \mapsto F_{[d]}(x, (b_1, b_i))$$

is injective and hence we conclude that $R \leqslant N$. Therefore we conclude that the total number of equivalence classes is at most

$$N \cdot B,$$

where B is the number of equivalence classes for the intersection of all the equivalence relations $\sim_S$, where S runs among all strict subsets of $[d]$. We can now iterate the above reasoning on each such S, where we have to run over all the $2^{d-|S|}$ choices of y, tracking at each step how many additional classes one obtains when passing from $\cap_{S' \subsetneq S}(\sim_{S'})$ to S. In this manner we see that the total number of equivalence classes for $\sim_{[d]}$ is bounded by

$$\prod_{\{d\} \subseteq S \subseteq [d]} N^{2^{d-|S|}} \leqslant \prod_{i=0}^{d-1} N^{\binom{d-1}{i} 2^i} = N^{3^{d-1}}.$$

Define

$$\delta(x) = \frac{|V(x)|}{|X_d|}.$$

Observe that $V(x)$ naturally injects in X_d by projecting on the dth component. This allows us to view $V(x) \times V(x)$ as a subset of X_d^2. Then it follows that the density of $V(x) \times V(x)$ in X_d^2 is $\delta(x)^2$. Then Cauchy's inequality and our bound for the total number of equivalence classes imply that

$$\frac{|W(x)|}{|X_d^2|} \geqslant \frac{\delta(x)^2}{N^{3^{d-1}}}.$$

So far we have proven that

$$\frac{|C_{[d]}^{\mathrm{acc}}|}{\prod_{i \in [d]} |X_i^2|} = \frac{\sum_{x \in \prod_{i \in [d-1]} X_i^2} |W(x)|}{\prod_{i \in [d]} |X_i^2|} \geqslant \frac{1}{\prod_{i \in [d-1]} |X_i^2|} \cdot \sum_{x \in \prod_{i \in [d-1]} X_i^2} \frac{\delta(x)^2}{N^{3^{d-1}}}. \tag{2.2}$$

Another application of Cauchy's inequality shows that

$$\sum_{x \in \prod_{i \in [d-1]} X_i^2} \frac{\delta(x)^2}{N^{3^{d-1}}} \geqslant \frac{\left(\sum_{x \in \prod_{i \in [d-1]} X_i^2} \delta(x)\right)^2}{N^{3^{d-1}} \cdot \prod_{i \in [d-1]} |X_i^2|}. \tag{2.3}$$

The average of $\delta(x)$ over all choices of x equals the density of $C^{\mathrm{acc}}_{[d-1]}$ in $X_d \times \prod_{i\in[d-1]} X_i^2$, which gives the equality

$$\left(\sum_{x\in\prod_{i\in[d-1]} X_i^2} \delta(x)\right)^2 = \prod_{i\in[d-1]} |X_i|^4 \cdot \left(\frac{\sum_{a\in X_d} |\{z \in C^{\mathrm{acc}}_{[d-1]} : \pi_d(z) = a\}|}{|X_d| \cdot \prod_{i\in[d-1]} |X_i^2|}\right)^2. \tag{2.4}$$

For each $a \in X_d$, consider the additive system $\mathfrak{A}_a$ on $X_1 \times \cdots \times X_{d-1}$ obtained from the additive system $\mathfrak{A}$ in the statement of the proposition and a in the natural way. The induction hypothesis applied to each $\mathfrak{A}_a$ yields

$$\frac{|\{z \in C^{\mathrm{acc}}_{[d-1]} : \pi_d(z) = a\}|}{\prod_{i\in[d-1]} |X_i^2|} \geqslant \delta_a^{2^{d-1}} \cdot N^{-3^{d-1}}, \tag{2.5}$$

where δ_a is the density of $\{\pi_{[d-1]}(z') : z' \in C^{\mathrm{acc}}_{\emptyset}, \pi_d(z') = a\}$ in $\prod_{i\in[d-1]} X_i$. Since $d \geqslant 1$, the generalized mean inequality (with $2^{d-1} \geqslant 1$) shows that

$$\left(\frac{\sum_{a\in X_d} \delta_a^{2^{d-1}}}{|X_d|}\right)^2 \geqslant \left(\frac{\sum_{a\in X_d} \delta_a}{|X_d|}\right)^{2^d} = \delta^{2^d}. \tag{2.6}$$

We deduce from Equations (2.2)–(2.6) that

$$\frac{|C^{\mathrm{acc}}_{[d]}|}{\prod_{i\in[d]} |X_i^2|} \geqslant \frac{\delta^{2^d}}{N^{3^{d-1}}} \cdot N^{-2\cdot 3^{d-1}} = \delta^{2^d} \cdot N^{-3^d}$$

as desired. □

3 | THE CATEGORY OF EXPANSION GROUPS

In this section we summarize the main results from [7] that we will use in Section 4. We start by introducing n-expansion groups. For the motivation behind our next definition and Definition 3.3, see Proposition 4.1.

Definition 3.1. Write e_i for the ith standard basis vector of $\mathbb{F}_2^n$. An n-expansion group is a triple $(G, \varphi, (g_1, \dots, g_n))$ satisfying the following properties:

(i) G is a group, $g_i \in G$ for all $i \in [n]$ and $\varphi : G \to \mathbb{F}_2^n$ is a group homomorphism such that $\varphi(g_i) = e_i$ for all $i \in [n]$;
(ii) $\ker(\varphi)$ is a vector space over $\mathbb{F}_2$;
(iii) we have $[G, G] = \ker(\varphi)$;
(iv) we have $g_i^2 = \mathrm{id}$ for all $i \in [n]$.

We define a morphism f between two n-expansion groups $(G, \varphi, (g_1, \dots, g_n))$ and $(G', \varphi', (g'_1, \dots, g'_n))$ to be a group homomorphism $f : G \to G'$ satisfying $f(g_i) = g'_i$ for all

$i \in [n]$. Let $\mathcal{C}_n$ be the category of n-expansion groups, which contains as objects n-expansion groups up to isomorphism and morphisms as defined above.

We will now explicitly construct the categorical product of two expansion groups following [7, Definition 3.12]. Define g_i'' be the element (g_i, g_i') of $G \times G'$ and let G'' be the group generated by the g_i''. Furthermore, let $\varphi'' : G'' \to \mathbb{F}_2^n$ be given by

$$\varphi''(g, g') := \varphi(g).$$

We remark that $\varphi''(g, g') = \varphi'(g')$. Then it follows that the triple $(G'', \varphi'', (g_1'', \dots, g_n''))$ is an n-expansion group, see [7, Proposition 3.13]. There are natural projection morphisms π_1, π_2 to, respectively, $(G, \varphi, (g_1, \dots, g_n))$ and $(G', \varphi', (g_1', \dots, g_n'))$. Then a routine verification shows that $(G'', \varphi'', (g_1'', \dots, g_n''))$ (together with π_1 and π_2) is the product of $(G, \varphi, (g_1, \dots, g_n))$ and $(G', \varphi', (g_1', \dots, g_n'))$ in the category of n-expansion groups.

Theorem 3.2. *Let $(G, \varphi, (g_1, \dots, g_n)) \in Ob(\mathcal{C}_n)$. Then G is a finite 2-group with*

$$|G| \leqslant 2^{n2^{n-1}-2^n+n+1}.$$

Furthermore, $\{g_1, \dots, g_n\}$ is a generating set for G.

Let $(G', \varphi', (g_1', \dots, g_n')) \in Ob(\mathcal{C}_n)$. Then we have

$$|Hom((G, \varphi, (g_1, \dots, g_n)), (G', \varphi', (g_1', \dots, g_n')))| \leqslant 1.$$

If there exists a morphism f between $(G, \varphi, (g_1, \dots, g_n))$ and $(G', \varphi', (g_1', \dots, g_n'))$, then the map f is a surjective group homomorphism satisfying $f(g_i) = g_i'$ and $\varphi = \varphi' \circ f$.

Moreover, $|Ob(\mathcal{C}_n)| < \infty$. The category $\mathcal{C}_n$ has all finite products and an initial object.

Proof. For the first part, we cite [7, Proposition 3.9]. Since $\{g_1, \dots, g_n\}$ is a generating set for G, it is clear that

$$|\mathrm{Hom}((G, \varphi, (g_1, \dots, g_n)), (G', \varphi', (g_1', \dots, g_n')))| \leqslant 1.$$

Furthermore, it is also clear that f is surjective and that $\varphi = \varphi' \circ f$.

From the fact that $|G| \leqslant 2^{n2^{n-1}-2^n+n+1}$, it follows immediately that $|\mathrm{Ob}(\mathcal{C}_n)| < \infty$. Then since, as explained right above the statement of the present Theorem, $\mathcal{C}_n$ has all finite products, the product over all objects is an initial object. □

For us it will be important to describe the initial object of $\mathcal{C}_n$ more explicitly. Let F_n be the free group on the set $\{x_1, \dots, x_n\}$. Consider the quotient group

$$\mathcal{G}_n := \frac{F_n}{N},$$

where N is the smallest normal subgroup of F_n containing $\{x_i^2\}_{i \in [n]}$ and the square of any element in the commutator subgroup $[F_n, F_n]$. Denote by φ the unique homomorphism from $\mathcal{G}_n$ to $\mathbb{F}_2^n$ sending (the class of) each x_i to e_i. Then the triple

$$\mathcal{G}([n]) := (\mathcal{G}_n, \varphi, (g_1, \dots, g_n))$$

is an n-expansion group and is the initial object of $\mathcal{C}_n$, see [7, Proposition 3.10]. Here g_i denotes the class of x_i in $\mathcal{G}_n$. Instead of appealing to [7, Proposition 3.10], one can also use Theorem 3.2 to show that $\mathcal{G}([n])$ is the initial object of $\mathcal{C}_n$. Indeed, since the kernel of the natural surjective group homomorphism from F_n to an arbitrary n-expansion group G contains N, $\mathcal{G}([n])$ admits a morphism to every expansion group G. Hence $\mathcal{G}([n])$ is the initial object by Theorem 3.2.

Let $(k_1, \dots, k_n) \in \mathbb{Z}^n_{\geqslant 1}$. Consider the vector space $\mathbb{F}_2^{k_1} \times \cdots \times \mathbb{F}_2^{k_n}$ and write $\pi_{(k_1,\dots,k_n)} : \mathbb{F}_2^{k_1} \times \cdots \times \mathbb{F}_2^{k_n} \to \mathbb{F}_2^n$ for the surjective homomorphism obtained by summing each block of k_i coordinates for all $i \in [n]$.

Definition 3.3. We call a $k_1 + \cdots + k_n$-expansion group $(G, \varphi, (g_1, \dots, g_{k_1+\cdots+k_n}))$ a $[(k_1, \dots, k_n)]$-expansion group in case $\varphi^{-1}(\ker(\pi_{(k_1,\dots,k_n)}))$ is a $\mathbb{F}_2$-vector space.

The resulting category $\mathcal{C}_{(k_1,\dots,k_n)}$ is a full subcategory of $\mathcal{C}_{k_1+\cdots+k_n}$ and has all finite products and an initial object. The initial object is explicitly constructed in the text preceding [7, Theorem 3.20]. We now summarize that construction for the convenience of the reader. Let $x \in [k_1 + \cdots + k_n]$ and suppose that x is in the ith block, that is,

$$k_1 + \cdots + k_{i-1} < x \leqslant k_1 + \cdots + k_i.$$

Then, as we explain below, we have a unique, surjective homomorphism

$$\varphi_x : \mathcal{G}_{k_1+\cdots+k_n} \to \mathbb{F}_2[\mathbb{F}_2^{[n]-\{i\}}] \rtimes \mathbb{F}_2^{[n]-\{i\}}$$

of abstract groups extending the following assignment:

$$g_j \mapsto \begin{cases} (0, e_h) & \text{if } j \in [k_1 + \cdots + k_n] \text{ is in the } h\text{th block with } h \neq i \\ (1 \cdot \mathrm{id}, 0) & \text{if } j = x \\ (0, 0) & \text{otherwise.} \end{cases}$$

Here we view $\mathbb{F}_2^{[n]-\{i\}}$ as the free $\mathbb{F}_2$-vector space over $[n] - \{i\}$ and e_h is the corresponding standard basis vector.

The initial object $\widetilde{\mathcal{G}}_{(k_1,\dots,k_n)}$ in $\mathcal{C}_{(k_1,\dots,k_n)}$ is then explicitly given by the quotient of $\mathcal{G}_{k_1+\cdots+k_n}$ by the intersection of $\ker(\varphi_x)$ as x varies in $[k_1 + \cdots + k_n]$, where we make $\widetilde{\mathcal{G}}_{(k_1,\dots,k_n)}$ in a $[(k_1, \dots, k_n)]$-expansion group by taking the same map φ and the same generators g_j as for $\mathcal{G}([k_1 + \cdots + k_n])$. We refer the reader to [7, Theorem 3.20] for the complete proof of this fact, while in the next paragraph we summarize the salient features of the argument, which will clarify the claim made above about φ_x and the fact that the map naturally factors through $\widetilde{\mathcal{G}}_{(k_1,\dots,k_n)}$.

We now describe the group $\widetilde{\mathcal{G}}_{(k_1,\dots,k_n)}$ in $\mathcal{C}_{(k_1,\dots,k_n)}$ as a quotient of $\mathcal{G}_{k_1+\cdots+k_n}$. In order to make sure that $\ker(\pi_{(k_1,\dots,k_n)})$ is a $\mathbb{F}_2$-vector space, we need to add to N the following relations. Define N' to be the smallest normal subgroup of $F_{k_1+\cdots+k_n}$ containing the set N and R, which we now describe. For h_1, h_2 in the i_1th block and h_3, h_4 in the i_2th block, we have that $[x_{h_1}x_{h_2}, x_{h_3}x_{h_4}]$, $(x_{h_1}x_{h_2})^2$, and $(x_{h_3}x_{h_4})^2$ are all in R. Furthermore, $[x_{h_1}x_{h_2}, c]$ is in R for any element $c \in [F_{k_1+\cdots+k_n}, F_{k_1+\cdots+k_n}]$. Having described R and therefore N', one can then show that

$$\frac{\mathcal{G}_{k_1+\cdots+k_n}}{N'} = \widetilde{\mathcal{G}}_{(k_1,\dots,k_n)}.$$

Let us now show that the assignment φ_x defines a homomorphism

$$\varphi_x : \mathcal{G}_{k_1+\cdots+k_n} \to \mathbb{F}_2[\mathbb{F}_2^{[n]-\{i\}}] \rtimes \mathbb{F}_2^{[n]-\{i\}},$$

which factors through $\widetilde{\mathcal{G}}_{(k_1,\ldots,k_n)}$. But indeed, when φ_x is viewed as a homomorphism from $F_{k_1+\cdots+k_n}$, it factors through N', because it vanishes on each of the elements of the set R.

In the next section it will be convenient to describe explicitly the homomorphisms φ_x, which is done in [7, Section 3.3] summarized now. If A is a set, we write $\mathbb{F}_2^A$ for the free $\mathbb{F}_2$-vector space on A.

Definition 3.4. Let G be a profinite group and let $A \subseteq \mathrm{Hom}(G, \mathbb{F}_2)$ be a finite, linearly independent set with $|A| \geqslant 2$ and $\chi_0 \in A$. An expansion map for G with support A and pointer χ_0 is a continuous group homomorphism

$$\psi : G \to \mathbb{F}_2[\mathbb{F}_2^{A-\{\chi_0\}}] \rtimes \mathbb{F}_2^{A-\{\chi_0\}},$$

satisfying the following two properties:

- for every $\chi \in A - \{\chi_0\}$, we have $\pi_\chi \circ \psi = \chi$, where π_χ is the projection on the coordinate of χ in $\mathbb{F}_2^{A-\{\chi_0\}}$;
- we have $\widetilde{\chi} \circ \psi = \chi_0$, where $\widetilde{\chi}$ is the unique non-trivial character of $\mathbb{F}_2[\mathbb{F}_2^{A-\{\chi_0\}}] \rtimes \mathbb{F}_2^{A-\{\chi_0\}}$ that sends the subgroup $\{0\} \rtimes \mathbb{F}_2^{A-\{\chi_0\}}$ to 0.

We shall need further understanding of expansion maps, and to this end we recall some more material from [7, Section 3.3]. Write $S = A - \{\chi_0\}$ and $n = |S|$. Let e_i be the ith basis vector of $\mathbb{F}_2^S$, which we can naturally view as an element of $\mathbb{F}_2[\mathbb{F}_2^S]$. There is a ring isomorphism

$$\mathbb{F}_2[\mathbb{F}_2^S] \cong \mathbb{F}_2[t_1, \ldots, t_n]/(t_1^2, \ldots, t_n^2)$$

by sending t_i to $1 \cdot \mathrm{id} + 1 \cdot e_i$. Under this isomorphism, the action of $e_i \in \mathbb{F}_2^S$ on $\mathbb{F}_2[t_1, \ldots, t_n]/(t_1^2, \ldots, t_n^2)$ becomes multiplication by $1 + t_i$. If ψ is an expansion map, then projection on the monomials $t_{S'} := \prod_{i \in S'} t_i$ gives a system of 1-cochains

$$\varphi_{S'}(\psi) : G \to \mathbb{F}_2$$

for each $S' \subseteq S$. These 1-cochains satisfy the recursive equation

$$\varphi_{S'}(\sigma\tau) - \varphi_{S'}(\sigma) - \varphi_{S'}(\tau) = \sum_{\emptyset \neq T \subseteq S'} \chi_T(\sigma)\varphi_{S'-T}(\tau) \tag{3.1}$$

with $\varphi_\emptyset = \chi_0$ and $\chi_T = \prod_{\chi \in T} \chi$, where the product is taken in $\mathbb{F}_2$. Reversely, a system of 1-cochains satisfying Equation (3.1) naturally gives rise to an expansion map.

4 | PROOF OF THEOREM 1.3

In this section we prove Theorem 1.3. The work is divided in two parts. In Subsection 4.1 we will use the theoretical results from Section 3, we prove Proposition 4.5, and we recall a version of

Rédei reciprocity, Theorem 4.6, that will be used later. With these tools in hand, we give the proof of Theorem 1.3 in Subsection 4.2.

4.1 | Preparations

First we will show how expansion groups naturally occur in the study of class groups. By a character χ of a field K we mean a continuous group homomorphism $\chi : G_K \to \mathbb{F}_2$, where G_K is by definition the Galois group $\mathrm{Gal}(K^{\mathrm{sep}}/K)$ with K^{sep} a fixed choice of a separable closure of K. Denote by χ_a the character corresponding to $\mathbb{Q}(\sqrt{a})$. Take an acceptable vector $(a_1, \dots, a_n)$ and write $k_i := \omega(a_i)$. Then we see that for all $i \in [n]$ and for all primes p dividing a_i, the prime p has ramification degree 2 in $H_2^+(\mathbb{Q}(\sqrt{a_1}, \dots, \sqrt{a_n}))$. In particular any inertia subgroup at p has size 2. So every inertia subgroup has exactly one non-trivial element, and by a choice of inertia at p we mean the choice of such an involution in $\mathrm{Gal}(H_2^+(\mathbb{Q}(\sqrt{a_1}, \dots, \sqrt{a_n}))/\mathbb{Q})$. Now write

$$a_i := p_{h_i+1} \cdot \dots \cdot p_{h_i+k_i}$$

with $h_i := \sum_{1 \leqslant j \leqslant i-1} k_j$. In this way there is an obvious bijection between $[k_1 + \cdots + k_n]$ and the prime factors of $a_1 \cdot \dots \cdot a_n$. The following proposition is the reason why $[(k_1, \dots, k_n)]$-expansion groups play a central role in our work.

Proposition 4.1. *Choose an inertia element σ_j at p_j for every $j \in [k_1 + \cdots + k_n]$. Then*

$$(\mathrm{Gal}(H_2^+(\mathbb{Q}(\sqrt{a_1}, \dots, \sqrt{a_n}))/\mathbb{Q}), (\chi_{p_1}, \dots, \chi_{p_{k_1+\cdots+k_n}}), (\sigma_1, \dots, \sigma_{k_1+\cdots+k_n}))$$

is a $[(k_1, \dots, k_n)]$-expansion group.

Proof. This is not hard to prove, but for the sake of brevity we refer to [7, Proposition 4.1]. □

The shape of Theorem 1.2 presents a striking resemblance with Definition 2.1. To make the analogy more stringent one would like to turn the splitting conditions in part (*b*) of Theorem 1.2 into an *additive system*: this is precisely the route we are going to follow. To do so we recall a refinement of Theorem 1.2.

Theorem 4.2. *Let n be a positive integer and let $(a_1, \dots, a_n)$ be an acceptable vector. Then the following are equivalent.*

(a) *The vector $(a_1, \dots, a_n)$ is maximal, that is,*

$$dim_{\mathbb{F}_2} Cl^+(\mathbb{Q}(\sqrt{a_1}, \dots, \sqrt{a_n}))[2] = \omega(a_1 \cdot \dots \cdot a_n) \cdot 2^{n-1} - 2^n + 1.$$

(b) *For every $T \subsetneq [n]$, every $j \in [n] - T$ and every prime $p \mid a_j$, there exists an expansion map*

$$\psi_{T,p} : Gal(H_2^+(\mathbb{Q}(\sqrt{a_1}, \dots, \sqrt{a_n}))/\mathbb{Q}) \to \mathbb{F}_2[\mathbb{F}_2^{\{\chi_{a_h}\}_{h \in T}}] \rtimes \mathbb{F}_2^{\{\chi_{a_h}\}_{h \in T}}$$

with support $\{\chi_{a_h}\}_{h \in T} \cup \{\chi_p\}$ and pointer χ_p.

Proof. Let us first prove that (a) implies (b). Recall that $\mathrm{Gal}(H_2^+(\mathbb{Q}(\sqrt{a_1}, \dots, \sqrt{a_n}))/\mathbb{Q})$ is naturally a $[(k_1, \dots, k_n)]$-expansion group by Proposition 4.1, which we call $\mathcal{G}$. Since $\mathcal{G}$ is of maximal cardinality, it follows from Theorem 3.2 that it must be canonically isomorphic to the initial object $\widetilde{\mathcal{G}}_{(k_1,\dots,k_n)}$. Recall that we constructed $\widetilde{\mathcal{G}}_{(k_1,\dots,k_n)}$ in Section 3 as the quotient of $\mathcal{G}([k_1 + \cdots + k_n])$ by the intersection of $\ker(\varphi_x)$, where

$$\varphi_x : \mathcal{G}_{k_1+\cdots+k_n} \to \mathbb{F}_2[\mathbb{F}_2^{[n]-\{i\}}] \rtimes \mathbb{F}_2^{[n]-\{i\}}$$

is also constructed in Section 3 for $x \in [k_1 + \cdots + k_n]$.

This induces a group homomorphism $\overline{\varphi_x} : \widetilde{\mathcal{G}}_{(k_1,\dots,k_n)} \to \mathbb{F}_2[\mathbb{F}_2^{[n]-\{i\}}] \rtimes \mathbb{F}_2^{[n]-\{i\}}$, which are the desired expansion maps for $|T| = n - 1$. If $|T| < n - 1$, we also get the remaining expansion maps, since $\mathbb{F}_2[\mathbb{F}_2^{T'}] \rtimes \mathbb{F}_2^{T'}$ is naturally a quotient of $\mathbb{F}_2[\mathbb{F}_2^{T}] \rtimes \mathbb{F}_2^{T}$ for $T' \subseteq T$.

Next we show that (b) implies (a). Recall again that $\mathrm{Gal}(H_2^+(\mathbb{Q}(\sqrt{a_1}, \dots, \sqrt{a_n}))/\mathbb{Q})$ is naturally a $[(k_1, \dots, k_n)]$-expansion group by Proposition 4.1, which we call $\mathcal{G}$. By Theorem 3.2, we see that $\mathcal{G}$ is a quotient of $\mathcal{G}_{k_1+\cdots+k_n}$ (as groups) and the expansion map $\psi_{[n]-\{i\},p}$ fits in a commutative diagram (of groups)

$$\begin{tikzcd}
\mathcal{G}_{k_1+\cdots+k_n} \arrow[d] \arrow[dr, "\varphi_x"] & \\
\mathcal{G} \arrow[r, "\psi_{[n]-\{i\},p}"] & \mathbb{F}_2[\mathbb{F}_2^{[n]-\{i\}}] \rtimes \mathbb{F}_2^{[n]-\{i\}},
\end{tikzcd}$$

where p is the xth prime and x is in the ith block. From this it is clear that the kernel (as groups) of the unique surjection $\mathcal{G}_{k_1+\cdots+k_n} \to \mathcal{G}$ of $(k_1 + \cdots + k_n)$-expansion groups is contained in the intersection of the $\ker(\varphi_x)$. Hence $\mathcal{G}$ is isomorphic to $\widetilde{\mathcal{G}}_{(k_1,\dots,k_n)}$ and therefore of maximal cardinality. □

Let $n \in \mathbb{Z}_{\geqslant 1}$, let $(k_1, \dots, k_n) \in \mathbb{Z}_{\geqslant 1} \times (2 \cdot \mathbb{Z}_{\geqslant 1})^{n-1}$ and let $M \in \mathbb{Z}_{\geqslant 1}$. Take

$$Y := Y_1 \times \cdots \times Y_n$$

to be a product space, where each Y_i is a set of cardinality M consisting of acceptable squarefree integers. We further require that any two distinct elements in $\cup_{i=1}^n Y_i$ are pairwise coprime and that $\omega(z) = \frac{k_i}{2}$ for each $i \in [n] - \{1\}$ and $z \in Y_i$, while $\omega(z) = k_1$ for $z \in Y_1$. We call such a Y a $((k_1, \dots, k_n), M)$-space.

Let Y now be a $((k_1, \dots, k_n), M)$-space. We denote by $K(Y)$ the multiquadratic number field obtained by adding all the square roots of the prime divisors of the elements in $\cup_{i=1}^n Y_i$ to $\mathbb{Q}$. Observe again that for each prime p ramifying in $K(Y)/\mathbb{Q}$, the inertia subgroups of p in $\mathrm{Gal}(H_2^+(K(Y))/\mathbb{Q})$ are cyclic of size 2. For each such prime p we fix a choice of such an inertia element σ_p. We will denote this choice by $\mathfrak{G} := \{\sigma_p\}_{p \mid \prod_{i=1}^n (\prod_{y \in Y_i} y)}$ and refer to it as *a choice of inertia* for Y. Once each set Y_i is ordered, we see that this choice $\mathfrak{G}$ turns $\mathrm{Gal}(H_2^+(K(Y))/\mathbb{Q})$ into a $|Y_1| + \cdots + |Y_n|$-expansion group.

If ψ is an expansion map for $G_{\mathbb{Q}}$, we define its *field of definition* to be $L(\psi) := \overline{\mathbb{Q}}^{\ker(\psi)}$. In case G is a Galois group and ψ is an expansion map for G, we shall sometimes implicitly view ψ as an expansion map for $G_{\mathbb{Q}}$ through the canonical projection $G_{\mathbb{Q}} \to G$. In this way it also makes sense to speak of the field of definition for expansion maps from a Galois group G.

Proposition 4.3.

(a) *Let Y be a $((k_1, \dots, k_n), M)$-space together with a choice of inertia $\mathfrak{G}$. Let $S \subsetneq [n]$ and let $j \in [n] - S$. Pick a divisor $d \neq 1$ of an element in Y_j and pick $\{a_i\}_{i \in S}$ with a_i a product of elements in Y_i for each $i \in S$. Then there exists at most one expansion map*

$$\psi_{(a_i)_{i \in S};d}(\mathfrak{G}) : Gal(H_2^+(K(Y))/\mathbb{Q}) \to \mathbb{F}_2[\mathbb{F}_2^{\{\chi_{a_i} : i \in S \text{ and } \chi_{a_i} \neq 0\}}] \rtimes \mathbb{F}_2^{\{\chi_{a_i} : i \in S \text{ and } \chi_{a_i} \neq 0\}}$$

with support $\{\chi_{a_i} : i \in S \text{ and } \chi_{a_i} \neq 0\} \cup \{\chi_d\}$ and pointer χ_d such that

$$\varphi_T(\psi_{(a_i)_{i \in S};d}(\mathfrak{G}))(\sigma) = 0$$

for each $\emptyset \neq T \subseteq S$ and each $\sigma \in \mathfrak{G}$.

(b) *If $\psi_{(a_i)_{i \in S};d}(\mathfrak{G})$ exists, then it factors through $Gal(H_2^+(\mathbb{Q}(\{\sqrt{a_i}\}_{i \in S}, \sqrt{d}))/\mathbb{Q})$.*

Proof. As we explained above, Proposition 4.1 implies that the group $\mathrm{Gal}(H_2^+(K(Y))/\mathbb{Q})$ equipped with $\mathfrak{G}$ becomes a $|Y_1| + \cdots + |Y_n|$-expansion group. In particular this implies that $\mathfrak{G}$ generates $\mathrm{Gal}(H_2^+(K(Y))/\mathbb{Q})$ by Theorem 3.2. This gives part (a) immediately, since the requirement $\varphi_T(\psi_{(a_i)_{i \in S};d}(\mathfrak{G}))(\sigma) = 0$ for each $\emptyset \neq T \subseteq S$ determines the image of σ under $\psi_{(a_i)_{i \in S};d}(\mathfrak{G})$.

To obtain part (b) we start by noticing that $L(\psi_{(a_i)_{i \in S};d}(\mathfrak{G}))$ is an abelian extension of $\mathbb{Q}(\{\sqrt{a_i}\}_{i \in S}, \sqrt{d})$. We only need to guarantee that it is unramified at all finite places. For this it is enough to notice that for each prime q not dividing a_i nor d one has that

$$\psi_{(a_i)_{i \in S};d}(\mathfrak{G})(\sigma_q) = \mathrm{id}$$

precisely due to our requirement that $\varphi_T(\psi_{(a_i)_{i \in S};d}(\mathfrak{G}))(\sigma_q) = 0$ for each $\emptyset \neq T \subseteq S$. □

In case there is an expansion map

$$\psi_{(a_i)_{i \in S};d}(\mathfrak{G}) : \mathrm{Gal}(H_2^+(K(Y))/\mathbb{Q}) \to \mathbb{F}_2[\mathbb{F}_2^{\{\chi_{a_i} : i \in S \text{ and } \chi_{a_i} \neq 0\}}] \rtimes \mathbb{F}_2^{\{\chi_{a_i} : i \in S \text{ and } \chi_{a_i} \neq 0\}}$$

as in Proposition 4.3, we will simply say that $\psi_{(a_i)_{i \in S};d}(\mathfrak{G})$ exists. Note that Theorem 1.2 implies that a maximal vector $(a_1, \dots, a_n)$ must be *strongly quadratically consistent*, that is, we have $(\frac{p}{q}) = 1$ for every distinct $i, j \in [n]$ and every two primes $p \mid a_i, q \mid a_j$. We call a $((k_1, \dots, k_n), M)$-space Y *quadratically consistent* in case each of its vectors are strongly quadratically consistent.

For convenience we introduce the following notation. Let $S \subseteq [n]$ and let $U \subseteq [n] - S$. Let

$$x \in \prod_{i \in S} Y_i^2 \times \prod_{j \in U} Y_j,$$

then we write

$$c(x) := ((\mathrm{pr}_1(\pi_i(x))\mathrm{pr}_2(\pi_i(x)))_{i \in S}, (\pi_j(x))_{j \in U})$$

for the vector obtained by multiplying out the double entries of x and leaving unchanged the single entries of x.

Theorem 4.4. *Let Y be a quadratically consistent $((k_1, \dots, k_n), M)$-space, together with a choice of inertia $\mathfrak{G}$. Let $S \subsetneq [n]$ and let $j \in [n] - S$. Pick a divisor $d \neq 1$ of an element in Y_j. Pick furthermore $U \subseteq [n] - S - \{j\}$. Let a be an element of $\prod_{i \in S} Y_i^2 \times \prod_{u \in U} Y_u$. Then the following are equivalent.*

(a) *The map $\psi_{c(a);d}(\mathfrak{G})$ exists.*

(b) *For each $h \in S \cup U$ the map $\psi_{\pi_{S \cup U - \{h\}}(c(a));d}(\mathfrak{G})$ exists and every prime ramifying in $\mathbb{Q}(\sqrt{x})/\mathbb{Q}$ splits completely in the field of definition of $\psi_{\pi_{S \cup U - \{h\}}(c(a));d}(\mathfrak{G})$, where x equals $\pi_h(a)$ for $h \in U$ and $pr_1(\pi_h(a))pr_2(\pi_h(a))$ for $h \in S$.*

Proof. We first show that (a) implies (b). So suppose that $\psi_{c(a);d}(\mathfrak{G})$ exists and write $\varphi_T(\psi_{c(a);d}(\mathfrak{G}))$ for the corresponding 1-cochains, where $\emptyset \subsetneq T \subseteq S \cup U$. Also set $\varphi_\emptyset = \chi_d$. Take any $h \in S \cup U$. Then we see that $\{\varphi_T(\psi_{c(a);d}(\mathfrak{G}))\}_{\emptyset \subsetneq T \subseteq S \cup U - \{h\}}$ together with $\varphi_\emptyset = \chi_d$ is a system of 1-cochains satisfying Equation (3.1), hence $\psi_{\pi_{S \cup U - \{h\}}(c(a));d}(\mathfrak{G})$ exists. Furthermore, we see that

$$\varphi_{S \cup U}(\psi_{c(a);d}(\mathfrak{G}))(\sigma\tau) - \varphi_{S \cup U}(\psi_{c(a);d}(\mathfrak{G}))(\sigma) - \varphi_{S \cup U}(\psi_{c(a);d}(\mathfrak{G}))(\tau)$$

equals

$$\theta(\sigma, \tau) := \sum_{\emptyset \subsetneq T \subseteq S \cup U} \chi_T(\sigma)\varphi_{S \cup U - T}(\psi_{c(a);d}(\mathfrak{G}))(\tau),$$

where χ_T is the product of the characters χ_i with $i \in T$, where χ_i equals $\chi_{\mathrm{pr}_1(\pi_i(a))\mathrm{pr}_2(\pi_i(a))}$ for $i \in S$ and $\chi_{\pi_i(a)}$ for $i \in U$. It follows that $\theta(\sigma, \tau)$ is trivial when inflated to $H^2(G_\mathbb{Q}, \mathbb{F}_2)$. In particular, it is locally trivial everywhere. Using that Y is quadratically consistent, this implies that every prime ramifying in $L(\chi_h)/\mathbb{Q}$ splits completely in the field of definition of $\psi_{\pi_{S \cup U - \{h\}}(c(a));d}(\mathfrak{G})$.

Indeed, take such a prime p ramifying in $L(\chi_h)/\mathbb{Q}$. We see that, locally at p, all the terms appearing in the definition of θ corresponding to a subset T different from $\{h\}$ vanish. Hence the expression reduces to the product $\chi_h(\sigma)\varphi_{S \cup U - \{h\}}(\psi_{c(a);d}(\mathfrak{G}))(\tau)$. Recalling that p is unramified in $\varphi_{S \cup U - \{h\}}(\psi_{c(a);d}(\mathfrak{G}))$, the desired conclusion readily follows.

To show that (b) implies (a), take for every subset $\emptyset \subsetneq T \subsetneq S \cup U$ a map $\varphi_{S \cup U - T}$ that equals $\varphi_{S \cup U - T}(\psi_{\pi_{S \cup U - \{h\}}(c(a));d}(\mathfrak{G}))$ for all $h \in T$. Define $\varphi_\emptyset = \chi_d$ and consider

$$\theta(\sigma, \tau) := \sum_{\emptyset \subsetneq T \subseteq S \cup U} \chi_T(\sigma)\varphi_{S \cup U - T}(\tau). \tag{4.1}$$

Using Equation (3.1), one sees that θ is a 2-cocycle. By assumption its class in $H^2(G_\mathbb{Q}, \mathbb{F}_2)$ is locally trivial at all the places that ramify in some $L(\chi_h)/\mathbb{Q}$. Furthermore, θ is clearly locally trivial at all other odd places. Since the χ_h are real, we see that θ is also locally trivial at infinity. Then it follows from Hilbert reciprocity that θ is locally trivial everywhere, hence trivial in $H^2(G_\mathbb{Q}, \mathbb{F}_2)$ by class field theory. This gives a map $\varphi_{S \cup U} : G_\mathbb{Q} \to \mathbb{F}_2$ satisfying

$$\varphi_{S \cup U}(\sigma\tau) - \varphi_{S \cup U}(\sigma) - \varphi_{S \cup U}(\tau) = \theta(\sigma, \tau).$$

We claim that there exists a quadratic character $\chi : G_\mathbb{Q} \to \mathbb{F}_2$ such that $\varphi_{S \cup U} + \chi$ factors through $\mathrm{Gal}(H_2^+(K(Y))/\mathbb{Q})$. First we observe that $\varphi_{S \cup U}$ is a quadratic character of $K(Y)$. Indeed, from Equation (4.1) we see that $\theta(\sigma, \tau) = 0$ for all $\sigma \in G_\mathbb{Q}$ that restrict to the identity in $\mathrm{Gal}(K(Y)/\mathbb{Q})$.

It remains to prove that $\varphi_{S\cup U}$ can be made an unramified character of $K(Y)$ by twisting with a character χ.

Define the field E to be the compositum of $K(Y)$ with all $L(\psi_{\pi_{S\cup U-\{h\}}(c(a));d}(\mathfrak{G}))$ as h runs through $S \cup U$. Then E is an unramified (at all finite places), abelian extension of $K(Y)$ of exponent 2. Since $\theta(\sigma, \tau) \in H^2(\mathrm{Gal}(E/\mathbb{Q}), \mathbb{F}_2)$, it follows that $\varphi_{S\cup U}$ gives a central $\mathbb{F}_2$-extension F of E. Let p be an odd place that is unramified in E, but suppose that it ramifies in F. Then twisting by χ_p removes the ramification at p. Furthermore, 2 is unramified in E, and if 2 ramifies in F, then we can remove the ramification at 2 by twisting with χ_{-1} and χ_2.

Now consider the resulting extension F', which has the property that $F'/\mathbb{Q}$ can only ramify at places that are already ramified in $E/\mathbb{Q}$. Hence a place p ramifying in $F'/\mathbb{Q}$ must be odd and ramify in one of the $L(\chi_h)/\mathbb{Q}$. Now we compute

$$\theta(\sigma_p, \sigma_p) = 0,$$

which implies that any lift of σ_p has order 2 in $\mathrm{Gal}(F'/\mathbb{Q})$. Since p is tame, it must be that F'/E is unramified at p. We conclude there exists a character χ such that $\varphi_{S\cup U} + \chi$ factors through $\mathrm{Gal}(H_2^+(K(Y))/\mathbb{Q})$. Further twisting by characters χ_p with p ramifying in $K(Y)$ ensures that the resulting map vanishes at all $\sigma \in \mathfrak{G}$. □

In order to prove part (a) of Theorem 1.3, we aim to combine Theorem 4.2 and Theorem 4.4 with Proposition 2.2. An import stepping stone is to guarantee equation (2.1) for the various cochains $\varphi_S(\psi_{T,p})$ attached to an expansion map $\psi_{T,p}$. We now explain what this means and how to achieve this.

Proposition 4.5. *Let Y be a $((k_1, \dots, k_n), M)$-space together with a choice of inertia $\mathfrak{G}$. Let $S \subsetneq [n]$, and let $j \in [n] - S$ and $i_0 \in S$. Pick a divisor $d \neq 1$ of an element in Y_j. Let $U \subseteq [n] - S - \{j\}$. Let x_1, x_2, x_3 be three elements of $\prod_{i\in S} Y_i^2 \times \prod_{u\in U} Y_u$ such that they coincide outside i_0 and such that*

$$pr_1(\pi_{i_0}(x_1)) = pr_2(\pi_{i_0}(x_3)), \quad pr_1(\pi_{i_0}(x_2)) = pr_2(\pi_{i_0}(x_1)), \quad pr_1(\pi_{i_0}(x_3)) = pr_2(\pi_{i_0}(x_2)).$$

Suppose that $\psi_{c(x_1);d}(\mathfrak{G})$ and $\psi_{c(x_2);d}(\mathfrak{G})$ exist. Then the map $\psi_{c(x_3);d}(\mathfrak{G})$ exists and

$$\varphi_T(\psi_{c(x_3);d}(\mathfrak{G})) = \varphi_T(\psi_{c(x_1);d}(\mathfrak{G})) + \varphi_T(\psi_{c(x_2);d}(\mathfrak{G}))$$

for each $\emptyset \neq T \subseteq S$.

Proof. This is now an immediate consequence of Proposition 4.3. Indeed, it follows from Equation (3.1) that the system of maps

$$\{\varphi_T(\psi_{(\pi_i(c(x_1)))_{i\in S};d}(\mathfrak{G})) + \varphi_T(\psi_{(\pi_i(c(x_2)))_{i\in S};d}(\mathfrak{G}))\}_{\emptyset\neq T\subseteq S}$$

(together with $\varphi_\emptyset = \chi_d$) yields an expansion map from the group $\mathrm{Gal}(H_2^+(K(Y))/\mathbb{Q})$ to the group

$$\mathbb{F}_2[\mathbb{F}_2^{\{\chi_{\pi_i(c(x_3))} : i\in S\cup U \text{ and } \chi_{\pi_i(c(x_3))}\neq 0\}}] \rtimes \mathbb{F}_2^{\{\chi_{\pi_i(c(x_3))} : i\in S\cup U \text{ and } \chi_{\pi_i(c(x_3))}\neq 0\}}.$$

Furthermore, the vanishing at all elements of $\mathfrak{G}$ follows by construction. This gives the desired conclusion. □

Finally, in order to obtain Theorem 1.3, part (b), we recast here (a special case of) Rédei reciprocity, rewritten in the language of expansion maps. Suppose that (a_1, a_2, a_3) is a strongly quadratically consistent vector. Then there exists an expansion map $\psi_{a_1;a_2} : G_{\mathbb{Q}} \to \mathbb{F}_2[\mathbb{F}_2] \rtimes \mathbb{F}_2$. Indeed, such an expansion map exists if and only if there exists a continuous map $\varphi : G_{\mathbb{Q}} \to \mathbb{F}_2$ satisfying

$$\varphi(\sigma\tau) - \varphi(\sigma) - \varphi(\tau) = \chi_{a_1}(\sigma) \cdot \chi_{a_2}(\tau),$$

which is clearly equivalent to $\chi_{a_1} \cup \chi_{a_2}$ being trivial in $H^2(G_{\mathbb{Q}}, \mathbb{F}_2)$. This last condition is in turn equivalent to $\chi_{a_1} \cup \chi_{a_2}$ being locally trivial everywhere, which follows quickly from the assumption that (a_1, a_2, a_3) is strongly quadratically consistent.

Furthermore, every prime divisor p of a_3 splits completely in $\mathbb{Q}(\sqrt{a_1}, \sqrt{a_2})/\mathbb{Q}$. Hence $\mathrm{Frob}(p)$ lands in the central subgroup $\mathrm{Gal}(L(\psi_{a_1;a_2})/\mathbb{Q}(\sqrt{a_1}, \sqrt{a_2}))$, which can be canonically identified with $\mathbb{F}_2$: here we recall that $L(\psi_{a_1;a_2})$ denotes the field of definition of an expansion map. In what follows Frobenius symbols need to be interpreted as elements of $\mathbb{F}_2$.

Theorem 4.6. *Let (a_1, a_2, a_3) be a strongly quadratically consistent vector. Let $\psi_{a_1;a_2}$: $Gal(H_2^+(\mathbb{Q}(\sqrt{a_1}, \sqrt{a_2}))/\mathbb{Q}) \to \mathbb{F}_2[\mathbb{F}_2] \rtimes \mathbb{F}_2$ and $\psi_{a_1;a_3}$: $Gal(H_2^+(\mathbb{Q}(\sqrt{a_1}, \sqrt{a_3}))/\mathbb{Q}) \to \mathbb{F}_2[\mathbb{F}_2] \rtimes \mathbb{F}_2$ be expansion maps with supports, respectively, $\{\chi_{a_1}, \chi_{a_2}\}$ and $\{\chi_{a_1}, \chi_{a_3}\}$ and pointers, respectively, χ_{a_2} and χ_{a_3}. Then*

$$\sum_{p | a_3} Frob_{L(\psi_{a_1;a_2})/\mathbb{Q}}(p) = \sum_{p | a_2} Frob_{L(\psi_{a_1;a_3})/\mathbb{Q}}(p).$$

Proof. This is a special case of [8, Theorem 3.3]. □

Remark 4.7. Theorem 4.6 has recently been generalized by the authors to more general expansion maps, see [8, Theorem *3.3*]. It is natural to wonder if this reciprocity law allows one to generalize the proof of Theorem 1.3 part (b) to $n > 3$. For every $(k_1, \dots, k_n)$ we have been able to construct vectors $(a_1, \dots, a_n)$ with $(\omega(a_1), \dots, \omega(a_n)) = (k_1, \dots, k_n)$ and $|\mathrm{Cl}^+(\mathbb{Q}(\sqrt{a_1}, \dots, \sqrt{a_n}))[2]|$ "large." However, already for $n = 4$, we have not been able to produce maximal vectors this way.

4.2 | Proof of Theorem 1.3

Let us start with a proposition that immediately yields part (b) and will be an important step for part (a).

Proposition 4.8. *Let N and m be positive integers. Then there exists a product space*

$$X := X_1 \times \cdots \times X_m,$$

where the X_i are disjoint sets of primes congruent to 1 modulo 4 with $|X_i| = N$ for each $i \in [m]$ such that

$$\prod_{i \in S} X_i$$

consists entirely of maximal vectors for every subset $S \subseteq [m]$ with $1 \leqslant |S| \leqslant 3$.

Proof. We proceed by induction on m. For $m = 1$ the statement is trivial. Now suppose that the statement is true for m, so that we have to prove it for $m + 1$. Pick a product set $X_1 \times \cdots \times X_m$ guaranteed by the inductive hypothesis. Choose inertia elements $\mathfrak{G}$ for the product set $X_1 \times \cdots \times X_m$, which is naturally a $((1, 2, 2, \dots, 2), N)$-space. Consider the set Z of primes that split completely in $H_2^+(K(X_1 \times \cdots \times X_m))\mathbb{Q}(\sqrt{-1})/\mathbb{Q}$. Thanks to the Chebotarev density theorem, we see that Z is an infinite set.

Pick any N-set X_{m+1} inside Z. Observe that X_{m+1} is disjoint from each of the X_i with $i \leqslant m$, since these are all primes ramifying in $H_2^+(K(X_1 \times \cdots \times X_m))/\mathbb{Q}$. Next, since X_{m+1} consists in particular of primes splitting in $K(X_1 \times \cdots \times X_m)/\mathbb{Q}$, we see that $X_{i_1} \times X_{i_2}$ consists entirely of maximal vectors for every distinct i_1 and i_2. Hence for each 2-set $\{i_1, i_2\}$ and every point $(p, q) \in X_{i_1} \times X_{i_2}$, we have an expansion map

$$\psi_{p;q}(\mathfrak{G}) : \mathrm{Gal}(H_2^+(\mathbb{Q}(\sqrt{p}, \sqrt{q}))/\mathbb{Q}) \to \mathbb{F}_2[\mathbb{F}_2] \rtimes \mathbb{F}_2$$

with support $\{\chi_p, \chi_q\}$ and pointer χ_q.

Thanks to our choice of X_{m+1}, we have that every x in X_{m+1} splits completely in $L(\psi_{p;q}(\mathfrak{G}))$ whenever $i_1, i_2 \leqslant m$ are distinct. But then Theorem 4.6 yields that p splits completely in $L(\psi_{q;x}(\mathfrak{G}))$ and q splits completely in $L(\psi_{p;x}(\mathfrak{G}))$. Therefore we deduce from Theorem 4.2 that for any 3-set $\{s_1, s_2, s_3\} \subseteq [m + 1]$ and any choice of $x_i \in X_{s_i}$, for $i \in \{1, 2, 3\}$, the map $\psi_{x_1,x_2;x_3}(\mathfrak{G})$ exists. Cycling the 3 variables s_1, s_2, s_3 and using Theorem 4.2, we conclude that (x_1, x_2, x_3) is maximal. □

Proof of Theorem 1.3 part (b). By taking $m = 3$ and N arbitrary large, we see that Proposition 4.8 immediately implies part (b) of Theorem 1.3 for $(k_1, k_2, k_3) = (1, 1, 1)$. The general case then follows from Proposition 4.5. Indeed, applying repeatedly Proposition 4.5 to the expansion maps $\psi_{x_1,x_2;x_3}(\mathfrak{G})$ constructed at the end of the proof of Proposition 4.8, we see that if a_1, a_2, a_3 are products of primes in, respectively, $X_{s_1}, X_{s_2}, X_{s_3}$, then the map $\psi_{a_1,a_2;q_3}(\mathfrak{G})$ exists for each prime divisor q_3 of a_3. We can now apply this three times, cycling the three variables s_1, s_2, s_3. Hence Theorem 4.2 shows that (a_1, a_2, a_3) is maximal, as desired. □

Proof of Theorem 1.3 part (a). Take $n \in \mathbb{Z}_{\geqslant 4}$ and $(k_1, \dots, k_n) \in \mathbb{Z}_{\geqslant 1} \times (2\mathbb{Z}_{\geqslant 1})^{n-1}$. Fix furthermore an auxiliary parameter $M \in \mathbb{Z}_{\geqslant 1}$. It follows from Proposition 4.5 and Proposition 4.8 that we can construct a $((k_1, \dots, k_n), M)$-space

$$Y := Y_1 \times \cdots \times Y_n,$$

equipped with a choice of inertia $\mathfrak{G}$ such that for any 3-set $\{i_1, i_2, i_3\} \subseteq [n]$, any triple $(y_{i_1}, y_{i_2}, y_{i_3}) \in Y_{i_1} \times Y_{i_2} \times Y_{i_3}$ and any prime divisor $p \mid y_{i_3}$ we have that the map

$$\psi_{y_{i_1},y_{i_2};p}(\mathfrak{G})$$

exists. Fix such a $((k_1, \dots, k_n), M)$-space Y. Also fix a point $y_1 \in Y_1$ and put

$$\widetilde{Y} := \{y_1\} \times Y_2 \times \dots \times Y_n.$$

We are going to construct an additive system on $\widetilde{Y}$ for the subsets S of $[n] - \{1\}$. We start by defining subsets

$$C_S \subseteq \prod_{i \in S} Y_i^2 \times \prod_{j \in [n]-S} Y_j$$

for every $S \subseteq [n] - \{1\}$. Let us first consider the case that $|S| \leqslant n-2$. We define C_S by the property that $a \in C_S$ if and only if for each 2-set $\{i, j\} \subseteq [n] - S$ and for every prime divisor $p \mid \pi_j(a)$, we have that

$$\psi_{\pi_{S\cup\{i\}}(c(a));p}(\mathfrak{G})$$

exists. We next put $C_{[n]-\{1\}}$ to be the set of a in $\{y_1\} \times \prod_{2\leqslant h\leqslant n} Y_h^2$ such that for any $j \in [n] - \{1\}$ and any prime divisor p of $\pi_j(c(a))$ we have that

$$\psi_{\pi_{[n]-\{j\}}(c(a));p}(\mathfrak{G})$$

exists and furthermore

$$\psi_{\pi_{[n]-\{1,j\}}(c(a)),\mathrm{pr}_k(\pi_j(a));p}(\mathfrak{G})$$

exists for all $j \in [n] - \{1\}$, $k \in [2]$ and p dividing y_1.

We now define the spaces A_S. Assume first that $|S| \leqslant n-3$. We put A_S to be the space of formal $\mathbb{F}_2$-linear combinations of 5-tuples

$$(x_1, x_2, x_3, x_4, x_5),$$

where $x_1, x_2, x_3 \in [n] - S$ are pairwise distinct and $x_4 \in [k_{x_2}], x_5 \in [k_{x_3}]$. Instead for $|S| \in \{n-2, n-1\}$, we set $A_S = \{0\}$.

Let us now define $F_S : C_S \to A_S$. In case $|S| > n-3$, we set F_S to be the trivial map. Henceforth we assume that $|S| \leqslant n-3$. Let $(x_1, x_2, x_3, x_4, x_5)$ be a 5-tuple as above and $a \in C_S$. Let $p_{x_4}(a)$ be the x_4th prime divisor of $\pi_{x_2}(c(a))$, by the natural ordering, and let $p_{x_5}(a)$ be the x_5th prime divisor of $\pi_{x_3}(c(a))$. We have that the Frobenius of $p_{x_5}(a)$ lands in the center of

$$\mathrm{Gal}(L(\psi_{\pi_{S\cup\{x_1\}}(c(a));p_{x_4}(a)}(\mathfrak{G}))/\mathbb{Q})$$

thanks to Theorem 4.4 and the definition of C_S. Observe that the center of

$$\mathbb{F}_2[t_1, \dots, t_n]/(t_1^2, \dots, t_n^2) \rtimes \mathbb{F}_2^n$$

is cyclic of order 2 and generated by $t_1 \cdot \dots \cdot t_n$. Hence to decide whether an element of the center is trivial or not one may simply apply the 1-cochain $\varphi_{S\cup\{x_1\}}(\psi_{\pi_{S\cup\{x_1\}};p_{x_4}(a)}(\mathfrak{G}))$ to the central element. In other words the value

$$\varphi_{S\cup\{x_1\}}(\psi_{\pi_{S\cup\{x_1\}}(c(a));p_{x_4}(a)}(\mathfrak{G}))(\mathrm{Frob}(p_{x_5}(a)))$$

is well defined and equals 0 if and only if $p_{x_5}(a)$ splits completely in the field of definition of $\psi_{\pi_{S\cup\{x_1\}}(c(a));p_{x_4}(a)}(\mathfrak{G})$. With this preliminary in mind, we define $F_S(a)$ to be the vector of A_S whose $(x_1, x_2, x_3, x_4, x_5)$-coordinate equals

$$\varphi_{S\cup\{x_1\}}(\psi_{\pi_{S\cup\{x_1\}}(c(a));p_{x_4}(a)}(\mathfrak{G}))(\mathrm{Frob}(p_{x_5}(a)))$$

for each 5-tuple $(x_1, x_2, x_3, x_4, x_5)$ as described above. Finally, for each $S \subseteq [n] - \{1\}$, we put

$$C_S^{\mathrm{acc}} := F_S^{-1}(0).$$

We now establish the following crucial fact.

Proposition 4.9. *The 4-tuple* $\{(C_S, C_S^{\mathrm{acc}}, F_S, A_S)\}_{S \subseteq [n]-\{1\}}$ *defined above is an additive system on* $\widetilde{Y}$*. Furthermore,*

$$|A_S| \leqslant 2^{n \cdot (\sum_{i=1}^{n} k_i)^2}$$

for each $S \subseteq [n] - \{1\}$*.*

Finally, for all $a \in C_{[n]-\{1\}}$ *we have that the vector* $(\pi_i(c(a)))_{i \in [n] : \chi_{\pi_i(c(a))} \neq 0}$ *is a maximal vector of dimension* $|\{i \in [n] : \chi_{\pi_i(c(a))} \neq 0\}|$*.*

Proof. Equation (2.1) is satisfied thanks to Proposition 4.5. The bound on $|A_S|$ follows from straightforward counting. The maximality claim is a consequence of Theorem 4.2 and Theorem 4.4. □

We now finish the proof of Theorem 1.3, part (a). Write $\mathfrak{A}$ for the additive system on $\widetilde{Y}$ guaranteed by Proposition 4.9. We apply Proposition 2.2 to the product space $\widetilde{Y}$ and the additive system $\mathfrak{A}$ to deduce that there exists a positive number $c_{(k_1,\ldots,k_n)}$, depending only on the vector $(k_1, \ldots, k_n)$, such that there are at least

$$c_{(k_1,\ldots,k_n)} \cdot M^{2n-2}$$

vectors $a \in \{y_1\} \times \prod_{2 \leqslant i \leqslant n} Y_i^2$ in $C_{[n]-\{1\}}$ (and therefore, by the last part of Proposition 4.9, with $(\pi_i(c(a)))_{i \in [n] : \chi_{\pi_i(c(a))} \neq 0}$ maximal). On the other hand, no more than $(n-1) \cdot M^{2n-3}$ vectors a in $\{y_1\} \times \prod_{2 \leqslant i \leqslant n} Y_i^2$ are such that $\mathrm{pr}_1(\pi_i(a)) = \mathrm{pr}_2(\pi_i(a))$ for some i. It follows that there are at least

$$c_{(k_1,\ldots,k_n)} \cdot M^{2n-2} - (n-1) \cdot M^{2n-3}$$

vectors in $C_{[n]-\{1\}}$ with distinct coordinates. By the last part of Proposition 4.9, each of them gives a maximal vector $c(a)$ such that

$$\omega(\pi_i(c(a))) = k_i$$

for each $i \in [n]$. Precisely 2^{n-1} choices of a will give rise to the same vector when passing to $c(a)$. All in all, we have obtained at least

$$\frac{c_{(k_1,\ldots,k_n)} \cdot M^{2n-2} - (n-1) \cdot M^{2n-3}}{2^{n-1}}$$

distinct multiquadratic fields $\mathbb{Q}(\sqrt{a_1}, \ldots, \sqrt{a_n})$ with $(a_1, \ldots, a_n)$ a maximal vector and with $\omega(a_i) = k_i$ for each $i \in [n]$. For M going to infinity this quantity goes to infinity, which gives us the desired conclusion. □

5 PROOF OF THEOREM 1.4 AND COROLLARY 1.5

In this section we give a proof of Theorem 1.4 and Corollary 1.5. We start by demonstrating that Corollary 1.5 is a simple consequence of Theorem 1.4. Denote by $K := \mathbb{Q}(\sqrt{a_1}, \ldots, \sqrt{a_n})$ a field satisfying the conclusion of Theorem 1.4. Recall that we have an exact sequence

$$0 \to \frac{(\mathcal{O}_K/c)^*}{\mathcal{O}_K^*} \to \mathrm{Cl}(K, c) \to \mathrm{Cl}(K) \to 0.$$

To ease the notation, let us denote by A the group $\frac{(\mathcal{O}_K/c)^*}{\mathcal{O}_K^*}$. This gives the inequality

$$\begin{aligned}\dim_{\mathbb{F}_2} \mathrm{Cl}(K, c)[2] &\leqslant \dim_{\mathbb{F}_2} \mathrm{Cl}(K)[2] + \dim_{\mathbb{F}_2} A[2] \\ &\leqslant \omega(a_1 \cdot \ldots \cdot a_n) \cdot 2^{n-1} - 2^n + 1 + 2^n \cdot \omega(c).\end{aligned}$$

The second inequality can be an equality only if

$$\dim_{\mathbb{F}_2} \mathrm{Cl}(K)[2] = \omega(a_1 \cdot \ldots \cdot a_n) \cdot 2^{n-1} - 2^n + 1,$$

and

$$\dim_{\mathbb{F}_2} A[2] = 2^n \cdot \omega(c),$$

thanks to Theorem 1.1 (for the first equation) and simple counting (for the second equation). Therefore we deduce from

$$\dim_{\mathbb{F}_2} \mathrm{Cl}(K, c)[2] = \omega(a_1 \cdot \ldots \cdot a_n) \cdot 2^{n-1} - 2^n + 1 + 2^n \cdot \omega(c)$$

that

$$\dim_{\mathbb{F}_2} \mathrm{Cl}(K)[2] = \omega(a_1 \cdot \ldots \cdot a_n) \cdot 2^{n-1} - 2^n + 1$$

and

$$\dim_{\mathbb{F}_2} A[2] = 2^n \cdot \omega(c). \tag{5.1}$$

Observe that we have a surjection

$$\varphi : \frac{(\mathcal{O}_K/c)^*}{(\mathcal{O}_K/c)^{*2}} \to \frac{A}{2A}.$$

Therefore we deduce from Equation (5.1) that

$$\dim_{\mathbb{F}_2} \frac{(\mathcal{O}_K/c)^*}{(\mathcal{O}_K/c)^{*2}} \geqslant \dim_{\mathbb{F}_2} \frac{A}{2A} = \dim_{\mathbb{F}_2} A[2] = 2^n \cdot \omega(c). \tag{5.2}$$

However, since all prime divisors of c are odd, direct counting gives the upper bound

$$\dim_{\mathbb{F}_2} \frac{(\mathcal{O}_K/c)^*}{(\mathcal{O}_K/c)^{*2}} \leqslant 2^n \cdot \omega(c) \tag{5.3}$$

with equality if and only if all the primes dividing c split completely in K. It follows from Equations (5.1)–(5.3) that

$$\dim_{\mathbb{F}_2} \frac{(\mathcal{O}_K/c)^*}{(\mathcal{O}_K/c)^{*2}} = 2^n \cdot \omega(c) = \dim_{\mathbb{F}_2} A[2] = \dim_{\mathbb{F}_2} \frac{A}{2A},$$

whence φ is an isomorphism. Furthermore, all primes dividing c split completely in K.

On the other hand,

$$\ker(\varphi) = \mathrm{im}\left(\mathrm{red}_c(K) : \frac{\mathcal{O}_K^*}{\mathcal{O}_K^{*2}} \to \frac{(\mathcal{O}_K/c)^*}{(\mathcal{O}_K/c)^{*2}}\right),$$

where $\mathrm{red}_c(K)$ is the natural reduction map modulo c. We conclude that the map $\mathrm{red}_c(K)$ is trivial as desired.

It remains to prove Theorem 1.4. To this end we switch to the setup of the proof of Theorem 1.3 and indicate the necessary modifications. First of all, we recall that the choice of y_1 was arbitrary, so we are allowed to take $y_1 := c$. Now suppose that $(c, a_1, \dots, a_n)$ is a maximal vector such that all expansion maps have totally real field of definition. Then we claim that

$$\dim_{\mathbb{F}_2} \mathrm{Cl}(\mathbb{Q}(\sqrt{a_1}, \dots, \sqrt{a_n}), c)[2] = \omega(a_1 \cdot \dots \cdot a_n) \cdot 2^{n-1} - 2^n + 1 + 2^n \cdot \omega(c).$$

Surely we have that

$$\dim_{\mathbb{F}_2} \mathrm{Cl}(\mathbb{Q}(\sqrt{a_1}, \dots, \sqrt{a_n}))[2] = \omega(a_1 \cdot \dots \cdot a_n) \cdot 2^{n-1} - 2^n + 1.$$

But now observe that the collection of characters

$$\{\varphi_T(\psi_{a_1,\dots,a_n;l}(\mathfrak{G}))\}_{l|c \text{ prime}, \, T \subseteq [n]}$$

is linearly independent and generates a subspace of

$$\mathrm{Cl}(\mathbb{Q}(\sqrt{a_1}, \dots, \sqrt{a_n}), c)^\vee[2]$$

linearly disjoint from

$$\mathrm{Cl}(\mathbb{Q}(\sqrt{a_1}, \dots, \sqrt{a_n}))^\vee[2]$$

by ramification considerations. This gives precisely the $2^n \cdot \omega(c)$ additional characters in $\mathrm{Cl}(\mathbb{Q}(\sqrt{a_1}, \dots, \sqrt{a_n}), c)^\vee[2]$ and therefore yields

$$\dim_{\mathbb{F}_2} \mathrm{Cl}(\mathbb{Q}(\sqrt{a_1}, \dots, \sqrt{a_n}), c)[2] = \omega(a_1 \cdot \dots \cdot a_n) \cdot 2^{n-1} - 2^n + 1 + 2^n \cdot \omega(c)$$

as desired.

We still need to explain how one ensures that all expansion maps are totally real. First of all, we indicate how Proposition 4.8 can be modified to ensure that all the maps $\psi_{y_1;y_2}(\mathfrak{G})$ are totally real. In this case we use a more general version [13] of Rédei reciprocity, which includes -1 (taking the role of the infinite place). Next one enlarges A_S to encode the splitting condition at infinity, and the maps F_S are also extended accordingly. With these modifications in mind, one proceeds exactly with the same argument as in Theorem 1.3.

ACKNOWLEDGEMENTS

We thank Alexander Smith for several clarifying emails and conversations about his work. We are grateful to the anonymous referee of [7] for having encouraged us to write down a self-contained proof of Theorem 1.3 in the form of this independent work. The authors wish to thank the Max Planck Institute for Mathematics in Bonn for its financial support, great work conditions, and an inspiring atmosphere.

JOURNAL INFORMATION

Mathematika is owned by University College London and published by the London Mathematical Society. All surplus income from the publication of *Mathematika* is returned to mathematicians and mathematics research via the Society's research grants, conference grants, prizes, initiatives for early career researchers and the promotion of mathematics.

REFERENCES

1. M. Bhargava, A. Shankar, T. Taniguchi, F. Thorne, J. Tsimerman, and Y. Zhao, *Bounds on 2-torsion in class groups of number fields and integral points on elliptic curves*, J. Amer. Math. Soc. **33** (2020), no. 4, 1087–1099.
2. J. Ellenberg, L. B. Pierce, and M. M. Wood, *On l-torsion in class groups of number fields*, Algebra Number Theory **11** (2017), no. 8, 1739–1778.
3. C. Frei and M. Widmer, *Averages and higher moments for the ℓ-torsion in class groups*, Math. Ann. **379** (2021), no. 3–4, 1205–1229.
4. C. F. Gauss, *Disquisitiones arithmeticae*, in commissis apud Gerh. Fleischer, Lipsiae, 1801.
5. H. Helfgott and A. Venkatesh, *Integral points on elliptic curves and 3-torsion in class groups*, J. Amer. Math. Soc. **19** (2006), no. 3, 527–550.
6. J. Klüners and J. Wang, *ℓ-torsion bounds for the class group of number fields with an ℓ-group as Galois group*, arXiv:2003.12161, 2020. https://www.cambridge.org/core/journals/mathematical-proceedings-of-the-cambridgephilosophical-society/article/redei-reciprocity-governing-fields-and-negative-pell/128E98F4B96AB15B77CDF63E6E27D447.
7. P. Koymans and C. Pagano, *Higher genus theory*, Int. Math. Res. Not. **2022** (2022), no. 4, 2772–2823.
8. P. Koymans and C. Pagano, *Higher Rédei reciprocity and integral points on conics*, arXiv:2005.14157, 2020.
9. L. B. Pierce, *The 3-part of class numbers of quadratic fields*, J. Lond. Math. Soc. (2) **71** (2005), no. 3, 579–598.
10. L. B. Pierce, *A bound for the 3-part of class numbers of quadratic fields by means of the square sieve*, Forum Math. **18** (2006), no. 4, 677–698.
11. L. B. Pierce, C. Turnage-Butterbaugh, and M. M. Wood, *An effective Chebotarev Density Theorem for families of number fields, with an application to l-torsion in class groups*, Invent. Math. **219** (2020), no. 2, 701–778.
12. A. Smith, 2^∞*-Selmer groups*, 2^∞*-class groups, and Goldfeld's conjecture*, arXiv:1702.02325v2, 2017.
13. P. Stevenhagen, *Redei reciprocity, governing fields, and negative Pell*, Proc. Amer. Math. Soc., arXiv:1806.06250v2, 2020.
14. J. Wang, *Pointwise bound for ℓ-torsion in class groups: elementary abelian extensions*, J. reine angew. Math., to appear. https://doi.org/10.1515/crelle-2020-0034.
15. J. Wang, *Pointwise Bound for ℓ-torsion in Class Groups II: nilpotent extensions*, arXiv:2006.10295, 2020.