Nagoya Math. J., **237** (2020), 166–187
DOI 10.1017/nmj.2018.16

DISTRIBUTION OF GALOIS GROUPS OF MAXIMAL UNRAMIFIED 2-EXTENSIONS OVER IMAGINARY QUADRATIC FIELDS

SOSUKE SASAKI

Abstract. Let k be an imaginary quadratic field with $\mathrm{Cl}_2(k) \simeq V_4$. It is known that the length of the Hilbert 2-class field tower is at least 2. Gerth (*On 2-class field towers for quadratic number fields with* 2*-class group of type* $(2, 2)$, Glasgow Math. J. **40**(1) (1998), 63–69) calculated the density of k where the length of the tower is 1; that is, the maximal unramified 2-extension is a V_4-extension. In this paper, we shall extend this result for generalized quaternion, dihedral, and semidihedral extensions of small degrees.

§1. Introduction

Let k be an imaginary quadratic field. We denote by $\mathrm{Cl}_2(k)$ the Sylow 2-subgroup of the class group of k, and by $G_2(k)$ the Galois group of the maximal unramified 2-extension of k.

Consider the 2-class field tower

$$k = k^0 \subseteq k^1 \subseteq k^2 \subseteq k^3 \subseteq \cdots$$

where k^{i+1} is the Hilbert 2-class field of k^i. It is easily seen that, for $i < j$, k^j/k^i is Galois and $\mathrm{Gal}(k^j/k^{i+1})$ is the derived subgroup of $\mathrm{Gal}(k^j/k^i)$.

We shall consider the case of $\mathrm{Cl}_2(k) \simeq \mathrm{Gal}(k^1/k) \simeq V_4$, the Klein four group. It is well-known [4, 17] in the group theory that all the finite 2-groups whose abelianization is isomorphic to V_4 are:

(i) V_4 itself;
(ii) Q_{2^n} $(n \geqslant 3)$, the (generalized) quaternion group of order 2^n;
(iii) D_{2^n} $(n \geqslant 3)$, the dihedral group of order 2^n;
(iv) SD_{2^n} $(n \geqslant 4)$, the semidihedral group of order 2^n.

Moreover, the derived subgroups of these groups are cyclic. Hence, we find that $\mathrm{Gal}(k^2/k)$ is isomorphic to one of these groups and $\mathrm{Gal}(k^2/k^1)$ is cyclic.

Received April 13, 2017. Revised April 24, 2018. Accepted April 24, 2018.
2010 Mathematics subject classification. 11R29, 11R32, 11R45.

In addition, it is known that a group with cyclic abelianization is itself cyclic, so that $k^2 = k^3 = \cdots$. This means $G_2(k) = \mathrm{Gal}(k^2/k)$, and it is isomorphic to V_4, Q_{2^n}, D_{2^n}, or SD_{2^n}.

We want to know the distribution of k with $G_2(k)$ isomorphic to each group.

DEFINITION. *Let A, B be subsets of $\mathbb{N}$. Here $0 \notin \mathbb{N}$. If the limit*

$$\lim_{x\to\infty} \frac{\#\{m \in A \mid m \leqslant x\}}{\#\{m \in B \mid m \leqslant x\}}$$

exists, we call it the relative density of A with respect to B, and denote it by $\delta(A/B)$.

Let

$$A(G) = \{m \in \mathbb{N} : \text{square-free} \mid G_2(\mathbb{Q}(\sqrt{-m})) \simeq G\}$$

and we consider the densities $\delta(A(G)/B)$ for $G = V_4, Q_{2^n}, D_{2^n}$, and SD_{2^n} with appropriate set B. Here we take

$$B(V_4) = \{m \in \mathbb{N} : \text{square-free} \mid \mathrm{Cl}_2(\mathbb{Q}(\sqrt{-m})) \simeq V_4\}\,.$$

The density of k such that the 2-class field tower terminates at k^1 is known by Gerth [6]:

THEOREM 1. (Gerth)

$$\delta(A(V_4)/B(V_4)) = \tfrac{1}{7}.$$

In Section 3, we shall extend this theorem for Q_{2^n}, D_{2^n}, and SD_{2^n}. For this purpose, we need to extend the Chebotarev density theorem for products of prime numbers. Accordingly, we shall produce a "multivariable" version of the Chebotarev density theorem as our main theorem. We shall prove this theorem by assuming the generalized Riemann hypothesis and using the effective version of the Chebotarev density theorem.

We shall use following notations:

(i) $\mathrm{Cl}_2(k)$ is the Sylow 2-subgroup of the class group of k, and $\mathrm{Cl}_2^+(k)$ is that of the narrow class group of k;
(ii) $h_2(k)$ and $h_2^+(k)$ are the orders of $\mathrm{Cl}_2(k)$ and $\mathrm{Cl}_2^+(k)$, respectively;
(iii) d_k is the discriminant of k;
(iv) $(\cdot/\cdot)$ is the Kronecker symbol, $(\cdot/\cdot)_4$ is the quartic residue symbol, and $(\cdot,\cdot/\cdot)$ is the Hilbert symbol.

https://doi.org/10.1017/nmj.2018.16 Published online by Cambridge University Press

§2. Conditions for $G_2(k) \simeq G$

At first we have to know when $G_2(k) \simeq Q_{2^n}$, D_{2^n}, or SD_{2^n}. Moreover, the conditions should be able to be written by splitting of primes in a number field because we use the Chebotarev density theorem. The conditions are known by several authors and gathered (together with other groups) in the table in [1]. In this section, we outline the conditions and prove them partially.

The 2-rank of the narrow class group of a quadratic field is obtained by the genus theory:

PROPOSITION 1. *Let F be a quadratic field and let t be the number of distinct prime divisors of d_F. Then the 2-rank $\dim_{\mathbb{F}_2} \mathrm{Cl}_2^+(F)$ of $\mathrm{Cl}_2^+(F)$ equals to $t-1$.*

The 4-rank can also be calculated by using the Rédei–Reichardt criterion [14]:

PROPOSITION 2. *Let F be a quadratic field and $l_1, \ldots, l_t$ be all the distinct prime divisors of d_F. We define the Rédei matrix:*

$$R_F = \left(\left[\frac{l_i, d_F}{l_j}\right]\right)_{\substack{1\leqslant i\leqslant t\\ 1\leqslant j\leqslant t-1}}$$

where $[l_i, d_F/l_j] \in \mathbb{F}_2$ is defined as

$$\left(\frac{l_i, d_F}{l_j}\right) = (-1)^{[l_i, d_F/l_j]}.$$

Then the 4-rank $\dim_{\mathbb{F}_2}(\mathrm{Cl}_2^+(F)^2/\mathrm{Cl}_2^+(F)^4)$ of $\mathrm{Cl}_2^+(F)$ equals to $t-1-\mathrm{rank}\, R_F$.

From Propositions 1 and 2, one can show

PROPOSITION 3. *Let k be an imaginary quadratic field with odd discriminant. Then, $\mathrm{Cl}_2(k) \simeq V_4$ if and only if $k = \mathbb{Q}(\sqrt{-pqr})$ for some distinct primes p, q, r such that:*

(i) $p \equiv q \equiv r \equiv -1\ (4)$ *and* $(p/q) = (q/r) = (r/p)$*; or*
(ii) $-p \equiv q \equiv r \equiv 1\ (4)$ *and at least two of* $(p/q), (p/r), (q/r)$ *equal to* -1.

https://doi.org/10.1017/nmj.2018.16 Published online by Cambridge University Press

The following conditions are shown by several authors, see [1]:

PROPOSITION 4.

(1) *Let* $k=\mathbb{Q}(\sqrt{-pqr})$ *where* $p, q,$ *and* r *are distinct primes with* $p\equiv q\equiv r\equiv -1\ (4)$. *Then* $G_2(k)$ *is abelian.*
(2) *Let* $k=\mathbb{Q}(\sqrt{-pqr})$ *where* $p, q,$ *and* r *are distinct primes with* $-p\equiv q\equiv r\equiv 1\ (4)$. *Then:*

 (a) $G_2(k)\simeq Q_8$ *if and only if*

$$\left(\frac{p}{q}\right)=\left(\frac{p}{r}\right)=\left(\frac{q}{r}\right)=-1.$$

 (b) $G_2(k)\simeq Q_{2^n}$ $(n\geqslant 4)$ *if and only if*

$$\left(\frac{p}{q}\right)=\left(\frac{p}{r}\right)=-1,\qquad \left(\frac{q}{r}\right)=1,\qquad \mathbf{N}\varepsilon_{qr}=-1,\, 2^n=4h_2(qr).$$

 (c) $G_2(k)\simeq D_{2^n}$ $(n\geqslant 3)$ *if and only if*

$$\left(\frac{p}{q}\right)=\left(\frac{p}{r}\right)=-1,\qquad \left(\frac{q}{r}\right)=1,\qquad \mathbf{N}\varepsilon_{qr}=1,\, 2^n=4h_2(qr).$$

 (d) $G_2(k)\simeq SD_{2^n}$ $(n\geqslant 4)$ *if and only if, by swapping* q *and* r *if necessary,*

$$\left(\frac{p}{q}\right)=1,\qquad \left(\frac{p}{r}\right)=\left(\frac{q}{r}\right)=-1,\, 2^n=4h_2(-pq).$$

Here $\mathbf{N}$ *is the absolute norm and* $h_2(m)=h_2(\mathbb{Q}(\sqrt{m}))$ *for* $m\in\mathbb{Z}$.

This proposition is shown by Kisilevsky [8] except for the conditions $2^n=4h_2(qr)$ and $2^n=4h_2(-pq)$ in (2b), (2c), and (2d). We give a proof of the conditions $2^n=4h_2(qr)$ and $2^n=4h_2(-pq)$ in (2b), (2c), and (2d) because no proof is given in [1].

Let $k=\mathbb{Q}(\sqrt{-pqr})$ where p, q, r are distinct primes with $-p\equiv q\equiv r\equiv 1\ (4)$, and assume $h_2(k)=4$. Then the Hilbert 2-class field k^1 is $\mathbb{Q}(\sqrt{-p},\sqrt{q},\sqrt{r})$. Let K be the maximal real subfield of k^1, that is, $K=\mathbb{Q}(\sqrt{q},\sqrt{r})$.

LEMMA 1.

$$h_2(k^1)=\tfrac{1}{2}h_2(K)h_2(-pq)h_2(-pr),$$

where $h_2(m)=h_2(\mathbb{Q}(\sqrt{m}))$ *for* $m\in\mathbb{Z}$.

Proof. From the relative class number formula [18, Chapter 4], one has

$$h(k^1)/h(K) = wQ \prod_{\chi:\text{odd}} \left(-\frac{1}{2f_\chi} \sum_{a=1}^{f_\chi} \chi(a)a \right)$$

where the product runs over the odd Dirichlet characters of k^1 and

(i) h is the class number;
(ii) w is the number of the roots of unity in k^1;
(iii) $Q = [U : \mu U_K]$, where U and U_K are the unit groups of k^1 and K, respectively, and μ is the group of the roots of unity in k^1;
(iv) f_χ is the conductor of χ.

Note that one can easily show

$$\begin{aligned}&\{\text{the odd Dirichlet characters of } k^1\}\\ &\quad = \left\{ \left(\frac{-p}{\cdot}\right), \left(\frac{-pq}{\cdot}\right), \left(\frac{-pr}{\cdot}\right), \left(\frac{-pqr}{\cdot}\right) \right\}.\end{aligned}$$

Similarly we have

$$h(m) = w_m \left(-\frac{1}{2|d_m|} \sum_{a=1}^{|d_m|} \left(\frac{m}{a}\right) a \right)$$

for $m = -p, -pq, -pr, -pqr$, where $h(m) = h(\mathbb{Q}(\sqrt{m}))$, $w_m = w_{\mathbb{Q}(\sqrt{m})}$, and $d_m = d_{\mathbb{Q}(\sqrt{m})}$. Putting these formulas together we obtain

$$h(k^1)/h(K) = wQ \frac{h(-p)h(-pq)h(-pr)h(k)}{w_p w_{pq} w_{pr} w_k}.$$

Now $h(-p)$ is odd by Proposition 1 and $h_2(k) = 4$. Also we know that the 2-parts of w, w_p, w_{pq}, w_{pr}, and w_k are 2 since $k^1/\mathbb{Q}$ is unramified at 2.

Hence it suffices to show $Q = 1$. By [18, Theorem 4.12], $Q = 1$ if and only if $\varepsilon/\overline{\varepsilon} \in \mu^2$ for any $\varepsilon \in U$, where $\overline{\varepsilon}$ means the conjugate of ε over K. Suppose $\varepsilon/\overline{\varepsilon} \notin \mu^2$ for some $\varepsilon \in U$. It can be easily shown that $w = 2$ or 6. Hence, $\varepsilon/\overline{\varepsilon} = -1$ or $(1 \pm \sqrt{-3})/2$. We let

$$\alpha = \begin{cases} \varepsilon\sqrt{-p} & \text{if } \varepsilon/\overline{\varepsilon} = -1, \\ \varepsilon\left(\dfrac{3 \mp \sqrt{-3}}{2}\right) & \text{if } \varepsilon/\overline{\varepsilon} = \dfrac{1 \pm \sqrt{-3}}{2} \quad (p = 3). \end{cases}$$

We can check $\alpha = \overline{\alpha}$ so that $\alpha \in K$. Hence,

$$\alpha^2 = N_{k^1/K}(\alpha) = pN_{k^1/K}(\varepsilon).$$

Since $N_{k^1/K}(\varepsilon) \in U_K$, this implies that p ramifies in $K/\mathbb{Q}$, which is absurd. $\square$

LEMMA 2. *The Hilbert 2-class fields of K and of $\mathbb{Q}(\sqrt{qr})$ coincide.*

Proof. Let K^1 and $\mathbb{Q}(\sqrt{qr})^1$ be the Hilbert 2-class fields of K and $\mathbb{Q}(\sqrt{qr})$, respectively. It can be shown that $K^1/\mathbb{Q}(\sqrt{qr})$ is Galois and $K^1 \supseteq \mathbb{Q}(\sqrt{qr})^1$. Since $K/\mathbb{Q}(\sqrt{qr})$ is unramified, so is $K^1/\mathbb{Q}(\sqrt{qr})$. Hence $\mathbb{Q}(\sqrt{qr})^1$ is the maximal abelian subextension of $K^1/\mathbb{Q}(\sqrt{qr})$, and the abelianization of $\mathrm{Gal}(K^1/\mathbb{Q}(\sqrt{qr}))$ is $\mathrm{Cl}_2(\mathbb{Q}(\sqrt{qr}))$. On the other hand, $\mathrm{Cl}_2^+(\mathbb{Q}(\sqrt{qr}))$ is cyclic by Proposition 1; therefore $\mathrm{Cl}_2(\mathbb{Q}(\sqrt{qr}))$ is also cyclic. Hence, $\mathrm{Gal}(K^1/\mathbb{Q}(\sqrt{qr}))$ is cyclic and $K^1 = \mathbb{Q}(\sqrt{qr})^1$. $\square$

Proof of Proposition 4. Now we determine n. We know that

$$2^n = \#G_2(k) = [k^2 : k] = h_2(k)h_2(k^1) = 4h_2(k^1).$$

From Lemma 2 we have $h_2(qr) = 2h_2(K)$. Hence from Lemma 1,

$$h_2(k^1) = \tfrac{1}{4}h_2(qr)h_2(-pq)h_2(-pr).$$

(2b), (2c)

Since $(p/q) = (p/r) = -1$, we get $h_2(-pq) = h_2(-pr) = 2$ from Proposition 1 (see Proposition 5 below). Hence $2^n = 4h_2(k^1) = 4h_2(qr)$.

(2d)

Similarly, we get $h_2(-pr) = 2$. Since $(q/r) = -1$, we get $h_2^+(qr) = 2$ from Proposition 1. Since $h_2(qr) = 2h_2(K)$ is even, we have $h_2(qr) = 2$. Hence $2^n = 4h_2(k^1) = 4h_2(-pq)$. $\square$

Also the following conditions are known, see [19]:

PROPOSITION 5. *Let p, q, and r be distinct primes with $-p \equiv q \equiv r \equiv 1\ (4)$. Then:*

(1) *$h_2(qr) = 2$ and $\mathbf{N}\varepsilon_{qr} = -1$ if and only if $(q/r) = -1$;*
(2) *$h_2(qr) = 2$ and $\mathbf{N}\varepsilon_{qr} = 1$ if and only if $(q/r) = 1$ and $(q/r)_4(r/q)_4 = -1$;*
(3) *$h_2(qr) = 4$ and $\mathbf{N}\varepsilon_{qr} = -1$ if and only if $(q/r) = 1$ and $(q/r)_4 = (r/q)_4 = -1$;*
(4) *$h_2(-pq) = 2$ if and only if $(p/q) = -1$;*
(5) *$h_2(-pq) = 4$ if and only if $(p/q) = 1$ and $(-p/q)_4 = -1$.*

§3. Densities for Q_8, Q_{16}, D_8, and SD_{16}

We want to find the densities of quadratic fields which have maximal unramified 2-extensions with Galois groups isomorphic to Q_{2^n}, D_{2^n}, or SD_{2^n}. In other words, we want to calculate the densities, $\delta(A(G)/B(V_4))$ for $G = Q_{2^n}, D_{2^n}, SD_{2^n}$. For this purpose, we produce a multivariable version of the Chebotarev density theorem.

For an integer $n \geqslant 0$, we let

$$P_n = \{p_1 \cdots p_n \mid p_1, \ldots, p_n : \text{distinct primes}\};$$
$$P_n(x) = \{m \in P_n \mid m \leqslant x\}.$$

At first we calculate $\delta(A(G)/P_3)$. Note that in our definition of $\delta(A/B)$, we do not assume $A \subseteq B$. It is known [7, Theorem 437] that for $n \geqslant 1$

$$\#P_n(x) \sim \frac{x(\log\log x)^{n-1}}{(n-1)!\log x}. \tag{1}$$

Suppose that F_a and $\mathcal{C}_a$ are given for each square-free positive integer a, where F_a is a number field which is Galois over $\mathbb{Q}$, and $\mathcal{C}_a$ is a conjugacy class in $\mathcal{G}_a = \mathrm{Gal}(F_a/\mathbb{Q})$. For a prime number p, we let $\varphi_a(p) = 1$ when p does not ramify in F_a and

$$\left(\frac{F_a/\mathbb{Q}}{p}\right) = \mathcal{C}_a,$$

and $\varphi_a(p) = 0$ otherwise. We denote for $n \geqslant 0$,

$$S_n = \left\{ p_1 \cdots p_n \in P_n \,\middle|\, p_1 < \cdots < p_n, \prod_{k=1}^{n} \varphi_{p_1 \cdots p_{k-1}}(p_k) = 1 \right\};$$
$$S_n(x) = \{m \in S_n \mid m \leqslant x\}.$$

Note that the empty product means 1 and $P_0 = S_0 = \{1\}$.

Now we state our main theorem:

Theorem 2. *Let n be a positive integer. Assume that:*

(i) *the Generalized Riemann Hypothesis (GRH) holds for the Dedekind zeta function of F_a for all $a \in S_0 \cup \cdots \cup S_{n-1}$;*

(ii) *there are positive constants c_0 and ε depending only on n, such that for $1 \leqslant k \leqslant n-1$ and $a = p_1 \cdots p_k \in S_k$ $(p_1 < \cdots < p_k)$,*

$$\log|d_{F_a}| \leqslant \frac{c_0\sqrt{p_k}}{(\log p_k)^{1+\varepsilon}} \qquad \text{and} \qquad [F_a : \mathbb{Q}] \leqslant \frac{c_0\sqrt{p_k}}{(\log p_k)^{2+\varepsilon}};$$

(iii) *for* $1 \leqslant k \leqslant n$, *there is a rational number* δ_k *such that for any* $a \in S_{k-1}$,

$$\frac{\#\mathcal{C}_a}{\#\mathcal{G}_a} = \delta_k.$$

Then

$$\delta(S_n/P_n) = \delta_1 \cdots \delta_n.$$

The proof of this theorem is given in the next section.

Now we shall calculate $\delta(A(G)/B(V_4))$ by using the theorem. Here we only calculate $\delta(A(D_8)/B(V_4))$. From Propositions 4 and 5, we know that $\mathbb{Q}(\sqrt{-m})$ has odd discriminant and $m \in A(D_8)$, if and only if, $m = pqr$ such that p, q, and r are distinct primes with $-p \equiv q \equiv r \equiv 1$ (4) and

$$\left(\frac{p}{q}\right) = \left(\frac{p}{r}\right) = -1, \qquad \left(\frac{q}{r}\right) = 1, \qquad \left(\frac{q}{r}\right)_4 \left(\frac{r}{q}\right)_4 = -1.$$

Let

$$\begin{aligned}
A_1 &= \{pqr \in A(D_8) \cap P_3 \mid p < q < r,\ -p \equiv q \equiv r \equiv 1\ (4)\};\\
A_2 &= \{pqr \in A(D_8) \cap P_3 \mid q < p < r,\ -p \equiv q \equiv r \equiv 1\ (4)\};\\
A_3 &= \{pqr \in A(D_8) \cap P_3 \mid q < r < p,\ -p \equiv q \equiv r \equiv 1\ (4)\};\\
A_4 &= \{m \in A(D_8) \mid m \not\equiv -1\ (4)\}\,.
\end{aligned}$$

Then clearly these are disjoint, and we know

$$A_1 \cup A_2 \cup A_3 \cup A_4 = A(D_8)$$

from Propositions 1 and 4. Note that if $m \in A_4$ then $\mathbb{Q}(\sqrt{-m})$ has even discriminant; therefore from Proposition 1, we can easily show that $m \in P_2$ or $m/2 \in P_2$. But we know $\delta(P_2/P_3) = 0$ from (1), which yields $\delta(A_4/P_3) = 0$. Hence,

$$\delta(A(D_8)/P_3) = \delta(A_1/P_3) + \delta(A_2/P_3) + \delta(A_3/P_3).$$

Now we see $\delta(A_1/P_3)$. We put:

(i) $F_1 = \mathbb{Q}(\sqrt{-1}), \mathcal{C}_1 = \{j\}, \delta_1 = \frac{1}{2}$ where $\langle j \rangle$ corresponds to $\mathbb{Q}$;
(ii) $F_p = \mathbb{Q}(\sqrt{-1}, \sqrt{p}), \mathcal{C}_p = \{\sigma\}, \delta_2 = \frac{1}{4}$ for primes $p \equiv -1$ (4), where $\langle \sigma \rangle$ corresponds to $\mathbb{Q}(\sqrt{-1})$;

(iii) $F_{pq} = \mathbb{Q}(\sqrt{-1}, \sqrt{p}, \sqrt{q}, \sqrt{\varepsilon_q}), \mathcal{C}_{pq} = \{\tau\}, \delta_3 = \frac{1}{16}$ for primes $p < q$, $-p \equiv q \equiv 1$ (4), where ε_q is the fundamental unit of $\mathbb{Q}(\sqrt{q})$, and $\langle\tau\rangle$ corresponds to $\mathbb{Q}(\sqrt{-1}, \sqrt{q}, \sqrt{p\varepsilon_q})$.

Assume that GRH holds for these fields. F_a and $\mathcal{C}_a$ are unused for the other integers a, so we may let them be anything.

Then we show $S_3 = A_1$. As is well-known that

$$\varphi_1(p) = 1 \iff p \equiv 3\ (4) \quad (\forall p : \text{prime});$$
$$\varphi_p(q) = 1 \iff q \equiv 1\ (4) \text{ and } (p/q) = -1 \quad (\forall p, q : \text{primes}, p \equiv 3\ (4)).$$

Now we consider F_{pq}. Assume $p < q$ and $-p \equiv q \equiv 1$ (4). By Scholz's reciprocity law [12, Proposition 5.8], if $q \equiv r \equiv 1$ (4) and $(q/r) = 1$,

$$\left(\frac{q}{r}\right)_4 \left(\frac{r}{q}\right)_4 = \left(\frac{\varepsilon_q}{r}\right).$$

We know that

$$(p/r) = -1 \iff r \text{ is inert in } \mathbb{Q}(\sqrt{p})/\mathbb{Q};$$
$$(q/r) = +1 \iff r \text{ splits in } \mathbb{Q}(\sqrt{q})/\mathbb{Q};$$
$$(\varepsilon_q/r) = -1 \iff \text{the primes above } r \text{ are inert in } \mathbb{Q}(\sqrt{q}, \sqrt{\varepsilon_q})/\mathbb{Q}(\sqrt{q}).$$

F_{pq} includes these fields. It is straightforward to show that $-(p/r) = (q/r) = -(\varepsilon_q/r) = 1$ if and only if the decomposition group of any prime ideal of F_{pq} above r is $\mathbb{Q}(\sqrt{-1}, \sqrt{q}, \sqrt{p\varepsilon_q})$. Hence, we have

$$\varphi_{pq}(r) = 1 \iff r \equiv 1\ (4) \text{ and } -(p/r) = (q/r) = -(q/r)_4(r/q)_4 = 1.$$
$$(\forall p, q, r : \text{primes}, p < q, -p \equiv q \equiv 1\ (4))$$

Therefore, for any primes $p < q < r$ we get

$$\varphi_1(p)\varphi_p(q)\varphi_{pq}(r) = 1 \iff -p \equiv q \equiv r \equiv 1\ (4) \text{ and } pqr \in A(D_8).$$

This means $S_3 = A_1$ by definition.

Finally, we estimate the discriminant of F_a. Clearly $|d_{F_1}| = 4$. Now $\mathbb{Q}(\sqrt{-1})$ and $\mathbb{Q}(\sqrt{-p})$ are linearly disjoint over $\mathbb{Q}$, and their discriminants are coprime. This yields [11, Chapter III, Proposition 17]

$$d_{F_p} = d^2_{\mathbb{Q}(\sqrt{-1})} d^2_{\mathbb{Q}(\sqrt{-p})} = 16p^2.$$

For F_{pq}, we first let $L = \mathbb{Q}(\sqrt{-1}, \sqrt{-p}, \sqrt{q})$ and we deduce as above

$$d_L = d^4_{\mathbb{Q}(\sqrt{-1})} d^4_{\mathbb{Q}(\sqrt{-p})} d^4_{\mathbb{Q}(\sqrt{q})} = 2^8 p^4 q^4.$$

Then we use the formula:

$$d_{F_{pq}}\mathbb{Z} = N_{L/\mathbb{Q}}(\mathfrak{d}_{F_{pq}/L}) \cdot d_L^{[F_{pq}:L]}\mathbb{Z}$$

where $\mathfrak{d}_{F_{pq}/L}$ is the relative discriminant. Also we use the fact that $\mathfrak{d}_{F_{pq}/L}$ divides the discriminant of the minimal polynomial of $\sqrt{\varepsilon_q}$ over L in $\mathcal{O}_L$, the ring of integers in L. Hence, we have

$$\mathfrak{d}_{F_{pq}/L} \mid 4\varepsilon_q \mathcal{O}_L = 4\mathcal{O}_L;$$
$$\therefore\ N_{L/\mathbb{Q}}(\mathfrak{d}_{F_{pq}/L}) \mid 4^8\mathbb{Z};$$
$$\therefore\ d_{F_{pq}} \mid 4^8 \cdot (2^8 p^4 q^4)^2 = 2^{32} p^8 q^8.$$

In any cases, F_a satisfies the discriminant condition of Theorem 2. For the facts about discriminants used above, see [3, Section III.2].

At this time we can apply Theorem 2, which yields

$$\delta(A_1/P_3) = \delta(S_3/P_3) = \delta_1\delta_2\delta_3 = \tfrac{1}{128}.$$

Similarly as above, we can also deduce $\delta(A_2/P_3) = 1/128$ by using

$$F_1 = \mathbb{Q}(\sqrt{-1}), \qquad F_q = \mathbb{Q}(\sqrt{-1}, \sqrt{q}), \qquad F_{qp} = \mathbb{Q}(\sqrt{-1}, \sqrt{p}, \sqrt{q}, \sqrt{\varepsilon_q}),$$

and $\delta(A_3/P_3) = 1/128$ by using

$$F_1 = \mathbb{Q}(\sqrt{-1}), \qquad F_q = \mathbb{Q}(\sqrt{-1}, \sqrt{q}, \sqrt{\varepsilon_q}), \qquad F_{qr} = \mathbb{Q}(\sqrt{-1}, \sqrt{q}, \sqrt{r}).$$

Therefore, we have

$$\delta(A(D_8)/P_3) = \tfrac{3}{128}.$$

It is known in [6] that $\delta(B(V_4)/P_3) = 7/32$; hence, we conclude

$$\delta(A(D_8)/B(V_4)) = \tfrac{3}{28}.$$

Also we can calculate densities for Q_8, Q_{16}, and SD_{16} in the same way. One can easily find the appropriate F_a and $\mathcal{C}_a$ by using the following fact: If q, r are odd primes with $r \equiv 1\ (4)$ and $(q/r) = 1$ then

$$(q/r)_4 = -1 \iff \text{the primes above } q \text{ are inert in } \mathbb{Q}(\zeta_r)_4/\mathbb{Q}(\sqrt{r});$$
$$(q/r)_4 = -1 \iff \text{the primes above } r \text{ are inert in } \mathbb{Q}(\sqrt[4]{q})/\mathbb{Q}(\sqrt{q}),$$

where $\mathbb{Q}(\zeta_r)_4$ is the quartic subfield of the rth cyclotomic field.

Table 1.
Densities.

A	$A(V_4)$	$A(Q_8)$	$A(Q_{16})$	$A(D_8)$	$A(SD_{16})$	$\bigcup_{n\geqslant 4} A(SD_{2^n})$
$\delta(A/B(V_4))$	$\frac{1}{7}$	$\frac{3}{14}$	$\frac{3}{56}$ (GRH)	$\frac{3}{28}$ (GRH)	$\frac{3}{14}$ (GRH)	$\frac{3}{7}$

THEOREM 3. *The results in Table 1 hold.*

Note that if the condition for $m \in A(G)$ can be written by using only quadratic residue symbols, we do not need GRH since we can use the same way as Gerth.

§4. Proof of Theorem 2

The following argument is basically from Gerth [5]. However, we cannot use the same way to estimate error terms because the quartic residue symbol $(p/\cdot)_4$ cannot be considered as Dirichlet characters. Hence, we shall use the effective Chebotarev density theorem.

In what follows, we use the following notations:

(i) $\sum_{a<p\leqslant b}$ means a single summation on p only over primes.
(ii) For a multivariable function f, $O(f)$ means a term whose absolute value is always at most $c|f|$ for some constant c depending only on n and ε.

We shall use the following formulas [9, Section 27.1], [7, Chapter XXII]:

$$\sum_{p\leqslant y} 1 = \frac{y}{\log y} + O\left(\frac{y}{(\log y)^2}\right); \tag{2}$$

$$\sum_{p\leqslant y} \frac{1}{p} = \log\log y + O(1); \tag{3}$$

$$\sum_{p\leqslant y} \frac{\log p}{p} = \log y + O(1). \tag{4}$$

https://doi.org/10.1017/nmj.2018.16 Published online by Cambridge University Press

We may assume $n \geqslant 2$. It suffices to show

$$\#S_n(x) = \delta_1 \cdots \delta_n \# P_n(x) + o(\# P_n(x)).$$

As in [5], we write

$$\begin{aligned}\#S_n(x) = \sum_{1<p_1\leqslant x^{1/n}} \varphi_1(p_1) \sum_{p_1<p_2\leqslant (x/p_1)^{1/(n-1)}} \varphi_{p_1}(p_2) \cdots \\ \sum_{p_{n-2}<p_{n-1}\leqslant (x/(p_1\cdots p_{n-2}))^{1/2}} \varphi_{p_1\cdots p_{n-2}}(p_{n-1}) \\ \times \sum_{p_{n-1}<p_n\leqslant x/(p_1\cdots p_{n-1})} \varphi_{p_1\cdots p_{n-1}}(p_n).\end{aligned}$$

Note that if $p_1, \ldots, p_k$ are in each interval, one has

$$x^{1/n} \leqslant \left(\frac{x}{p_1 \cdots p_k}\right)^{1/(n-k)}.$$

In particular,

$$\frac{1}{\log(x/p_1 \cdots p_k)} = O\left(\frac{1}{\log x}\right). \tag{5}$$

An elementary calculation shows

$$\begin{aligned}\#S_n(x) &= \sum_{p_1} \varphi_1(p_1) \sum_{p_2} \varphi_{p_1}(p_2) \cdots \sum_{p_n} \varphi_{p_1\cdots p_{n-1}}(p_n) \\ &= \sum_{p_1} \delta_1 \sum_{p_2} \delta_2 \cdots \sum_{p_n} \delta_n \\ &\quad + \sum_{p_1} (\varphi_1(p_1) - \delta_1) \sum_{p_2} \delta_2 \cdots \sum_{p_n} \delta_n \\ &\quad + \sum_{p_1} \varphi_1(p_1) \sum_{p_2} (\varphi_{p_1}(p_2) - \delta_2) \cdots \sum_{p_n} \delta_n \\ &\quad + \cdots \\ &\quad + \sum_{p_1} \varphi_1(p_1) \sum_{p_2} \varphi_{p_1}(p_2) \cdots \sum_{p_n} (\varphi_{p_1\cdots p_{n-1}}(p_n) - \delta_n).\end{aligned} \tag{6}$$

The first term in the right-hand side of (6) equals to $\delta_1 \cdots \delta_n \# P_n(x)$. So we have to estimate the remaining terms.

We need the following estimation:

LEMMA 3. *Let* $1 \leqslant k \leqslant n$ *and* $a = p_1 \cdots p_{k-1} \in P_{k-1}$ $(p_1 < \cdots < p_{k-1})$. *Then for* $y \geqslant p_{k-1}$,

$$\left|\sum_{p \leqslant y} (\varphi_a(p) - \delta_k)\right| = O\left(\frac{y}{(\log y)^{1+\varepsilon}}\right).$$

Proof. From the definition of φ_a, we know

$$\begin{aligned}\sum_{p \leqslant y} \varphi_a(p) &= \pi_{\mathcal{C}_a}(y, F_a/\mathbb{Q}) \\ &= \#\left\{p : \text{prime} \,\middle|\, p \leqslant x, p \text{ does not ramify in } F_a, \left(\frac{F_a/\mathbb{Q}}{p}\right) = \mathcal{C}_a\right\}.\end{aligned}$$

Also we note that $\pi(y) = \sum_{p \leqslant y} 1$ is the usual prime-counting function and $\delta_k = \#\mathcal{C}_a / \#\mathcal{G}_a$.

From the effective version of the Chebotarev density theorem [10, 15], we have

$$\begin{aligned}\pi_{\mathcal{C}_a}(y, F_a/\mathbb{Q}) &= \frac{\#\mathcal{C}_a}{\#\mathcal{G}_a}(\mathrm{Li}(y) + O(\sqrt{y}([F_a : \mathbb{Q}] \log y + \log|d_{F_a}|))); \\ \pi(y) &= \mathrm{Li}(y) + O(\sqrt{y} \log y),\end{aligned}$$

where

$$\mathrm{Li}(y) = \int_2^y \frac{dt}{\log t}.$$

Note that GRH for the Dedekind zeta function of F_a implies the usual Riemann hypothesis. Our claim follows from these equations and our assumptions for $|d_{F_a}|$ and $[F_a : \mathbb{Q}]$. $\square$

We consider the last term of (6). Since $x/p_1 \cdots p_{n-1} \geqslant p_{n-1}$, we get

$$\begin{aligned}&\left|\sum_{p_1} \varphi_1(p_1) \sum_{p_2} \varphi_{p_1}(p_2) \cdots \sum_{p_n} (\varphi_{p_1 \cdots p_{n-1}}(p_n) - \delta_n)\right| \\ &\leqslant \sum_{p_1} \sum_{p_2} \cdots \sum_{p_{n-1}} \left| \sum_{1 < p_n \leqslant x/(p_1 \cdots p_{n-1})} (\varphi_{p_1 \cdots p_{n-1}}(p_n) - \delta_n) \right. \\ &\qquad \left. - \sum_{1 < p_n \leqslant p_{n-1}} (\varphi_{p_1 \cdots p_{n-1}}(p_n) - \delta_n) \right|\end{aligned}$$

$$
\begin{aligned}
&= \sum_{p_1} \sum_{p_2} \cdots \sum_{p_{n-1}} O\biggl(\frac{x}{p_1 \cdots p_{n-1}(\log (x/(p_1 \cdots p_{n-1})))^{1+\varepsilon}} \\
&\quad + \frac{p_{n-1}}{(\log p_{n-1})^{1+\varepsilon}}\biggr) \\
&= O\biggl(\frac{x}{(\log x)^{1+\varepsilon}}\biggr) \sum_{p_1 \leqslant x} \frac{1}{p_1} \sum_{p_2 \leqslant x} \frac{1}{p_2} \cdots \sum_{p_{n-1} \leqslant x} \frac{1}{p_{n-1}} \\
&= O\biggl(\frac{x(\log \log x)^{n-1}}{(\log x)^{1+\varepsilon}}\biggr) = o(\# P_n(x))
\end{aligned}
$$

from Lemmas 3 and (5).

Next we see the middle terms in the right-hand side of (6). We first claim

$$
\sum_{p_{n-1} < p_n \leqslant x/(p_1 \cdots p_{n-1})} 1 = \frac{x}{p_1 \cdots p_{n-1} \log x} + O\biggl(\frac{x \log p_{n-1}}{p_1 \cdots p_{n-1} (\log x)^2}\biggr). \tag{7}
$$

In fact, from (2) we have

$$
\begin{aligned}
\sum_{1 < p_n \leqslant (x/(p_1 \cdots p_{n-1}))} 1 &= \frac{x}{p_1 \cdots p_{n-1} \log (x/(p_1 \cdots p_{n-1}))} \\
&\quad + O\biggl(\frac{x}{p_1 \cdots p_{n-1} (\log (x/(p_1 \cdots p_{n-1})))^2}\biggr) \\
&= \frac{x}{p_1 \cdots p_{n-1} \log x} + \frac{x \log (p_1 \cdots p_{n-1})}{p_1 \cdots p_{n-1} \log (x/(p_1 \cdots p_{n-1})) \log x} \\
&\quad + O\biggl(\frac{x}{p_1 \cdots p_{n-1} (\log x)^2}\biggr) \\
&= \frac{x}{p_1 \cdots p_{n-1} \log x} + O\biggl(\frac{x \log p_{n-1}}{p_1 \cdots p_{n-1} (\log x)^2}\biggr),
\end{aligned}
$$

and from

$$
O\biggl(\frac{p_{n-1}}{(\log p_{n-1})^2}\biggr) = O\biggl(\frac{x/(p_1 \cdots p_{n-1})}{(\log (x/(p_1 \cdots p_{n-1})))^2}\biggr) = O\biggl(\frac{x}{p_1 \cdots p_{n-1} (\log x)^2}\biggr)
$$

we have

$$
\sum_{1 < p_n \leqslant p_{n-1}} 1 = O\biggl(\frac{p_{n-1}}{\log p_{n-1}}\biggr) = O\biggl(\frac{x \log p_{n-1}}{p_1 \cdots p_{n-1} (\log x)^2}\biggr).
$$

https://doi.org/10.1017/nmj.2018.16 Published online by Cambridge University Press

Hence, (7) follows. Then we can ignore the error term of (7) since

$$\sum_{p_1}\sum_{p_2}\cdots\sum_{p_{n-1}} O\biggl(\frac{x\log p_{n-1}}{p_1\cdots p_{n-1}(\log x)^2}\biggr)$$
$$= O\biggl(\frac{x}{(\log x)^2}\biggr)\sum_{p_1\leqslant x}\frac{1}{p_1}\sum_{p_2\leqslant x}\frac{1}{p_2}\cdots\sum_{p_{n-1}\leqslant x}\frac{\log p_{n-1}}{p_{n-1}}$$
$$= O\biggl(\frac{x(\log\log x)^{n-2}}{\log x}\biggr) = o(\#P_n(x))$$

from (3) and (4). Thus, we have to estimate

$$\sum_{p_1}\varphi_1(p_1)\cdots\sum_{p_k}(\varphi_{p_1\cdots p_{k-1}}(p_k)-\delta_k)\sum_{p_{k+1}}\delta_{k+1}\cdots$$
$$\sum_{p_{n-1}}\delta_{n-1}\frac{\delta_n x}{p_1\cdots p_{n-1}\log x}$$
$$= O\biggl(\frac{x}{\log x}\biggr)\sum_{p_1}\frac{1}{p_1}\cdots\sum_{p_{k_1}}\frac{1}{p_{k-1}}$$

$$\biggl|\sum_{p_k}\frac{\varphi_{p_1\cdots p_{k-1}}(p_k)-\delta_k}{p_k}\sum_{p_{k+1}}\frac{1}{p_{k+1}}\cdots\sum_{p_{n-1}}\frac{1}{p_{n-1}}\biggr| \tag{8}$$

for $1\leqslant k\leqslant n-1$.We write

$$s_k = \sum_{p_k<p_{k+1}\leqslant(x/(p_1\cdots p_k))^{1/(n-k)}}\frac{1}{p_{k+1}}\cdots\sum_{p_{n-2}<p_{n-1}\leqslant(x/(p_1\cdots p_{n-2}))^{1/2}}\frac{1}{p_{n-1}}$$

for $1\leqslant k\leqslant n-2$ and $s_{n-1}=1$. Then we prove

$$s_k = \frac{(\log\log x-\log\log p_k)^{n-k-1}}{(n-k-1)!}+O((\log\log x)^{n-k-2}) \tag{9}$$

for $1\leqslant k\leqslant n-1$. If $k=n-1$ it is obvious, and if $k=n-2$ it follows from (3) and (5). Suppose $2\leqslant k\leqslant n-2$. Put

$$f_1(t) = \frac{(\log\log x-\log\log t)^{n-k-1}}{(n-k-1)!}.$$

Suppose now $s_k = f_1(p_k)+O((\log\log x)^{n-k-2})$. Let

$$y = \biggl(\frac{x}{p_1\cdots p_{k-1}}\biggr)^{1/(n-k+1)}$$

then from (5),

$$\log\log y = \log\log x + O(1), \qquad f_1(y) = O(1).$$

Let $C_1(t) = \sum_{p\leqslant t} 1/p$. Then from (3)

$$C_1(t) = \log\log t + O(1).$$

Next we quote Abel's summation formula [7, Theorem 421]:

PROPOSITION 6. *Let $\{c_m\}_{m\in\mathbb{N}}$ be a sequence of numbers. Put*

$$C(t) = \sum_{m\leqslant t} c_m.$$

Let $f(t)$ be a function which is continuously differentiable for $t \geqslant 1$. Then

$$\sum_{x<m\leqslant y} c_m f(m) = C(y)f(y) - C(x)f(x) - \int_x^y C(t)f'(t)\,dt.$$

Using this proposition we have

$$\begin{aligned}
s_{k-1} &= \sum_{p_{k-1}<p_k\leqslant y} \frac{s_k}{p_k} \\
&= \sum_{p_{k-1}<p_k\leqslant y} \frac{1}{p_k} f_1(p_k) + O((\log\log x)^{n-k-2}) \sum_{p_{k-1}<p_k\leqslant y} \frac{1}{p_k} \\
&= C_1(y)f_1(y) - C_1(p_{k-1})f_1(p_{k-1}) \\
&\quad - \int_{p_{k-1}}^y C_1(t)f_1'(t)\,dt + O((\log\log x)^{n-k-1}) \\
&= (\log\log x + O(1))O(1) - (\log\log p_{k-1} + O(1))f_1(p_{k-1}) \\
&\quad + \int_{p_{k-1}}^y (\log\log t + O(1))|f_1'(t)|\,dt + O((\log\log x)^{n-k-1}) \\
&= -f_1(p_{k-1})\log\log p_{k-1} + (\log\log x + O(1)) \int_{p_{k-1}}^y |f_1'(t)|\,dt \\
&\quad - \int_{p_{k-1}}^y (\log\log x - \log\log t)|f_1'(t)|\,dt + O((\log\log x)^{n-k-1}) \\
&= -f_1(p_{k-1})\log\log p_{k-1} - (\log\log x + O(1)) \int_{p_{k-1}}^y f_1'(t)\,dt
\end{aligned}$$

$$
\begin{aligned}
&- \int_{p_{k-1}}^{y} \frac{(\log\log x - \log\log t)^{n-k-1}}{(n-k-2)!\, t\log t}\, dt + O((\log\log x)^{n-k-1}) \\
&= -f_1(p_{k-1})\log\log p_{k-1} - (\log\log x + O(1))[f_1(t)]_{p_{k-1}}^{y} \\
&\quad - \left[-\frac{(\log\log x - \log\log t)^{n-k}}{(n-k-2)!(n-k)}\right]_{p_{k-1}}^{y} + O((\log\log x)^{n-k-1}) \\
&= -f_1(p_{k-1})\log\log p_{k-1} + f_1(p_{k-1})\log\log x \\
&\quad - \frac{(\log\log x - \log\log p_{k-1})^{n-k}}{(n-k-2)!(n-k)} + O((\log\log x)^{n-k-1}) \\
&= \frac{(\log\log x - \log\log p_{k-1})^{n-k}}{(n-k-2)!}\left(\frac{1}{n-k-1} - \frac{1}{n-k}\right) \\
&\quad + O((\log\log x)^{n-k-1}) \\
&= \frac{(\log\log x - \log\log p_{k-1})^{n-k}}{(n-k)!} + O((\log\log x)^{n-k-1}).
\end{aligned}
$$

Hence we have proved (9) by induction.

Next we claim

(10)
$$
\sum_{p_{k-1}<p_k\leqslant(x/(p_1\cdots p_{k-1}))^{1/(n-k+1)}} \frac{\varphi_{p_1\cdots p_{k-1}}(p_k)-\delta_k}{p_k} s_k = O((\log\log x)^{n-k-1})
$$

for $1\leqslant k\leqslant n-1$. In fact, let

$$
\begin{aligned}
y &= \left(\frac{x}{p_1\cdots p_{k-1}}\right)^{1/(n-k+1)}; \\
f_2(t) &= \frac{(\log\log x - \log\log t)^{n-k-1}}{(n-k-1)!\, t}; \\
C_2(t) &= \sum_{p\leqslant t}(\varphi_{p_1\cdots p_{k-1}}(p) - \delta_k).
\end{aligned}
$$

Then from (9) we have

$$
\frac{s_k}{p_k} = f_2(p_k) + O\biggl(\frac{(\log\log x)^{n-k-2}}{p_k}\biggr),
$$

and from Lemma 3,

$$
C_2(t) = O\biggl(\frac{t}{(\log t)^{1+\varepsilon}}\biggr)
$$

https://doi.org/10.1017/nmj.2018.16 Published online by Cambridge University Press

for $t \geqslant p_{k-1}$. Similarly as before, by Proposition 6,

$$\begin{aligned}
&\sum_{p_{k-1}<p_k\leqslant y} \frac{\varphi_{p_1\cdots p_{k-1}}(p_k)-\delta_k}{p_k} s_k \\
&= \sum_{p_{k-1}<p_k\leqslant y} (\varphi_{p_1\cdots p_{k-1}}(p_k)-\delta_k) f_2(p_k) + O((\log\log x)^{n-k-2}) \\
&\quad \times \sum_{p_{k-1}<p_k\leqslant y} \frac{1}{p_k} = C_2(y)f_2(y) - C_2(p_{k-1})f_2(p_{k-1}) \\
&\quad - \int_{p_{k-1}}^{y} C_2(t)f_2'(t)\,dt + O((\log\log x)^{n-k-1}) \\
&= O\left(\frac{y}{(\log y)^{1+\varepsilon}}\right)O\left(\frac{1}{y}\right) + O\left(\frac{p_{k-1}}{(\log p_{k-1})^{1+\varepsilon}}\right)O\left(\frac{(\log\log x)^{n-k-1}}{p_{k-1}}\right) \\
&\quad + \int_{p_{k-1}}^{y} O\left(\frac{t}{(\log t)^{1+\varepsilon}}\right)|f_2'(t)|\,dt + O((\log\log x)^{n-k-1}) \\
&= \int_{p_{k-1}}^{y} O\left(\frac{t}{(\log t)^{1+\varepsilon}}\right)O\left(\frac{(\log\log x)^{n-k-1}}{t^2}\right)dt + O((\log\log x)^{n-k-1}) \\
&= O((\log\log x)^{n-k-1})\int_{p_{k-1}}^{y} \frac{1}{t(\log t)^{1+\varepsilon}}\,dt + O((\log\log x)^{n-k-1}) \\
&= O((\log\log x)^{n-k-1})\left[-\frac{1}{(\log t)^{\varepsilon}}\right]_{p_{k-1}}^{y} + O((\log\log x)^{n-k-1}) \\
&= O((\log\log x)^{n-k-1}).
\end{aligned}$$

Thus (10) follows.

Therefore, (8) becomes

$$\begin{aligned}
&O\left(\frac{x}{\log x}\right)\sum_{p_1}\frac{1}{p_1}\cdots\sum_{p_{k-1}}\frac{1}{p_{k-1}}O((\log\log x)^{n-k-1}) \\
&\quad = O\left(\frac{x(\log\log x)^{n-2}}{\log x}\right) = o(\#P_n(x)).
\end{aligned}$$

Hence we have completed the proof.

§5. Densities for the remaining groups

We cannot get the densities for the remaining groups because we do not know any conditions for them in which Theorem 2 can be applied. We want to know about the conditions $h_2(-pq)=2^n$, $h_2(qr)=2^n$ or $\mathbf{N}\varepsilon_{qr}=1$ in detail.

Cohn and Lagarias [2] considered $\mathrm{Cl}_2(\mathbb{Q}(\sqrt{dp}))$ as p varies where $d\not\equiv 2\ (4)$ is an integer. They conjectured that the splitting of primes in a number field determines the structure of $\mathrm{Cl}_2(\mathbb{Q}(\sqrt{dp}))$, and they also considered numerically. Here we consider $h_2(dp)$ and $h_2^+(dp)$ where d is an odd prime discriminant.

We suggest the following conjecture:

CONJECTURE 1.

(1) *For a prime $p\equiv -1\ (4)$ and an integer $n\geqslant 1$, there are $F_p^{(n)}$ and $\mathcal{C}_p^{(n)}$ as in Section 3 such that for a prime $q\equiv 1\ (4)$ which does not ramify in $F_p^{(n)}$,*

$$\left(\frac{F_p^{(n)}/\mathbb{Q}}{q}\right)=\mathcal{C}_p^{(n)} \iff h_2(-pq)=2^n.$$

In addition, $\#\mathcal{C}_p^{(n)}/[F_p^{(n)}:\mathbb{Q}]=1/2^n$. And the similar one holds for $p\equiv 1\ (4)$ and $q\equiv -1\ (4)$.

(2) *For a prime $p\equiv 1\ (4)$ and integers m,n with $1\leqslant m\leqslant n\leqslant m+1$, there are $F_p^{(m,n)}$ and $\mathcal{C}_p^{(m,n)}$ as in Section 3 such that for a prime $q\equiv 1\ (4)$ which does not ramify in $F_p^{(m,n)}$,*

$$\left(\frac{F_p^{(m,n)}/\mathbb{Q}}{q}\right)=\mathcal{C}_p^{(m,n)} \iff \begin{cases} h_2(pq)=2^m,\\ h_2^+(pq)=2^n.\end{cases}$$

In addition, $\#\mathcal{C}_p^{(m,n)}/[F_p^{(m,n)}:\mathbb{Q}]=1/2^{m+n-1}$.

Note that $h_2(pq)=h_2^+(pq)$ if and only if $\mathbf{N}\varepsilon_{pq}=-1$.

Stevenhagen [16] showed that the narrow 8-ranks of quadratic fields are determined by number fields. Hence the cases $n\leqslant 2$ in both 1 and 2 of Conjecture 1 are known to be true. Unfortunately however, Milovic [13] gives some evidence against Conjecture 1 for $n\geqslant 3$.

We calculated the numbers of $pq<10^7$ ($p,q:$ primes) with $-p\equiv q\equiv 1\ (4)$, $h_2(-pq)=2^n$; and also with $p\equiv q\equiv 1\ (4)$ and $h_2(pq)h_2^+(pq)/2=2^n$ for each $n\in\mathbb{N}$ (using SageMath 6.10); see Table 2. Note that both p and q vary.

Table 2.
Numbers of $pq < 10^7$ with $h_2(-pq) = 2^n$ and with $h_2(pq)h_2^+(pq)/2 = 2^n$.

n	Imaginary	Real
1	390350	163903
2	194214	81354
3	96712	40265
4	48489	20217
5	24276	9872
6	12145	5071
7	5999	2463
8	3137	1251
9	1523	597
10	622	288
11	171	121
12	18	60
13	0	20
14	0	9
15	0	4
Total	777656	325495

Table 3.
Conjectured densities.

A	$A(Q_{2^n})$	$\bigcup_{n\geqslant 3} A(Q_{2^n})$	$A(D_{2^n})$	$\bigcup_{n\geqslant 3} A(D_{2^n})$	$A(SD_{2^n})$
$\delta(A/B(V_4))$	$\dfrac{3}{2^{2n-5}\cdot 7}$	$\dfrac{2}{7}$	$\dfrac{3}{2^{2n-4}\cdot 7}$	$\dfrac{1}{7}$	$\dfrac{3}{2^{n-3}\cdot 7}$

This conjecture yields the densities for the remaining groups:

THEOREM 4. *Assume that Conjecture 1 holds. In addition, we assume that each F_p in Conjecture 1 satisfies*

$$\log|d_{F_p}| = O\left(\frac{\sqrt{p}}{(\log p)^{1+\varepsilon}}\right), \qquad [F_p:\mathbb{Q}] = O\left(\frac{\sqrt{p}}{(\log p)^{2+\varepsilon}}\right).$$

Moreover we assume GRH.

Then the results in Table 3 hold.

Proof. From our assumptions, we can apply Theorem 2. We omit the details.

https://doi.org/10.1017/nmj.2018.16 Published online by Cambridge University Press

Note that $\delta(\cdot/B(V_4))$ is not countably additive in general. In this case, however, we can calculate the densities of $A_Q = \bigcup_{n=3}^{\infty} A(Q_{2^n})$ and $A_D = \bigcup_{n=3}^{\infty} A(D_{2^n})$. In fact, for $N, x \in \mathbb{N}$

$$\sum_{n=3}^{N} \#A(Q_{2^n})(x) = \# \bigcup_{n=3}^{N} A(Q_{2^n})(x) \leqslant \#A_Q(x)$$

where $A(x) = \{\, m \in A \mid m \leqslant x \,\}$ for $A \subseteq \mathbb{N}$. Hence,

$$\sum_{n=3}^{N} \delta(A(Q_{2^n})/B(V_4)) = \sum_{n=3}^{N} \lim_{x\to\infty} \frac{\#A(Q_{2^n})(x)}{\#B(V_4)(x)} \leqslant \liminf_{x\to\infty} \frac{\#A_Q(x)}{\#B(V_4)(x)}$$

for $N \in \mathbb{N}$. Hence,

$$\frac{2}{7} = \sum_{n=3}^{\infty} \delta(A(Q_{2^n})/B(V_4)) \leqslant \liminf_{x\to\infty} \frac{\#A_Q(x)}{\#B(V_4)(x)}.$$

Similarly,

$$\frac{1}{7} \leqslant \liminf_{x\to\infty} \frac{\#A_D(x)}{\#B(V_4)(x)}.$$

On the other hand, since

$$\delta(A_Q \cup A_D/B(V_4)) = 1 - \delta(A(V_4)/B(V_4)) - \delta\left(\bigcup_{n\geqslant 4} A(SD_{2^n})/B(V_4)\right) = \frac{3}{7},$$

we have

$$\begin{aligned} \limsup_{x\to\infty} \frac{\#A_Q(x)}{\#B(V_4)(x)} &= \limsup_{x\to\infty} \left(\frac{\#(A_Q(x) \cup A_D(x))}{\#B(V_4)(x)} - \frac{\#A_D(x)}{\#B(V_4)(x)} \right) \\ &= \lim_{x\to\infty} \frac{\#(A_Q(x) \cup A_D(x))}{\#B(V_4)(x)} - \liminf_{x\to\infty} \frac{\#A_D(x)}{\#B(V_4)(x)} \leqslant \frac{2}{7}. \end{aligned}$$

Putting these together, we obtain that all these inequalities are equalities and lim inf = lim sup. It is similar for A_D. □

References

[1] E. Benjamin, F. Lemmermeyer and C. Snyder, *Imaginary quadratic fields k with cyclic* $\mathrm{Cl}_2(k^1)$, J. Number Theory **67**(2) (1997), 229–245.

[2] H. Cohn and J. C. Lagarias, *On the existence of fields governing the 2-invariants of the classgroup of* $\mathbf{Q}(\sqrt{dp})$ *as p varies*, Math. Comp. **41**(164) (1983), 711–730.

https://doi.org/10.1017/nmj.2018.16 Published online by Cambridge University Press

[3] A. Fröhlich and M. J. Taylor, *Algebra Number Theory*, Cambridge Studies in Advanced Mathematics **27**, Cambridge University Press, Cambridge, 1993.
[4] P. Furtwängler, *Über das Verhalten der Ideale des Grundkörpers im Klassenkörper*, Monatsh. Math. **27** (1916), 1–15.
[5] F. Gerth III, *Counting certain number fields with prescribed l-class numbers*, J. Reine Angew. Math. **337** (1982), 195–207.
[6] F. Gerth III, *On* 2*-class field towers for quadratic number fields with* 2*-class group of type* $(2, 2)$, Glasgow Math. J. **40**(1) (1998), 63–69.
[7] G. H. Hardy and E. M. Wright, *An Introduction to the Theory of Numbers*, 4th ed. The Clarendon Press, Oxford, 1965.
[8] H. Kisilevsky, *Number fields with class number congruent to* $4 \bmod 8$ *and Hilbert's theorem* 94, J. Number Theory **8**(3) (1976), 271–279.
[9] Helmut Koch., *Introduction to Classical Mathematics. I*, Mathematics and its Applications **70**, Kluwer Academic Publishers Group, Dordrecht, 1991, From the quadratic reciprocity law to the uniformization theorem, Translated and revised from the 1986 German original, Translated by John Stillwell.
[10] J. C. Lagarias and A. M. Odlyzko, "*Effective versions of the Chebotarev density theorem*", in *Algebraic number fields: L-functions and Galois properties (Proc. Sympos., Univ. Durham, Durham, 1975)*, Academic Press, London, 1977, 409–464.
[11] S. Lang, *Algebraic Number Theory*, 2nd ed., Graduate Texts in Mathematics **110**, Springer, New York, 1994.
[12] F. Lemmermeyer, *Reciprocity Laws*, Springer Monographs in Mathematics, Springer, Berlin, 2000. From Euler to Eisenstein.
[13] D. Milovic, *On the 16-rank of class groups of* $\mathbb{Q}(\sqrt{-8p})$ *for* $p \equiv -1 \bmod 4$, Geom. Funct. Anal. **27**(4) (2017), 973–1016.
[14] L. Rédei and H. Reichardt, *Die Anzahl der durch vier teilbaren Invarianten der Klassengruppe eines beliebigen quadratischen Zahlkörpers*, J. Reine Angew. Math. **170** (1934), 69–74.
[15] J.-P. Serre, *Quelques applications du théorème de densité de Chebotarev*, Publ. Math. Inst. Hautes Études Sci. **54** (1981), 323–401.
[16] P. Stevenhagen, "*Ray class groups and governing fields*", in *Théorie des nombres*, Publ. Math. Fac. Sci. Besançon, Univ. Franche-Comté, Besançon, 1989, 93.
[17] O. Taussky, *A Remark on the Class Field Tower*, J. Lond. Math. Soc. (2) **s1-12**(2) (1937), 82–85.
[18] L. C. Washington, *Introduction to Cyclotomic Fields*, 2nd ed., Graduate Texts in Mathematics **83**, Springer, New York, 1997.
[19] Y. Yamamoto, *Divisibility by* 16 *of class number of quadratic fields whose* 2*-class groups are cyclic*, Osaka J. Math. **21**(1) (1984), 1–22.

Department of Pure and Applied Mathematics
Graduate School of Fundamental Science and Engineering
Waseda University
3-4-1 Okubo
Shinjuku-ku
Tokyo
Japan
sosuke_s5@asagi.waseda.jp