J. Math. Soc. Japan
Vol. 58, No. 2, 2006

Distribution of units of a cubic abelian field modulo prime numbers

By Yoshiyuki KITAOKA

(Received May 16, 2005)

Abstract. We studied the distribution of units of an algebraic number field modulo prime ideals. Here we study the distribution of units of a cubic abelian field modulo rational prime numbers. For a decomposable prime number p, $2(p-1)^2$ is an upper bound of the order of the unit group modulo p, and we show that the conjectural density of primes which attain it is really positive.

Introduction.

We are interested in the distribution of units modulo ideals of an algebraic number field. Let F be an algebraic number field and $o_F, o_F^\times$ the maximal order of F and the group of units of F, respectively. For an integral ideal $\mathfrak{n}$ of F, we set

$$\begin{aligned} E(\mathfrak{n}) &= \left\{u \bmod \mathfrak{n} | u \in o_F^\times\right\} \ \left(\subset (o_F/\mathfrak{n})^\times\right), \\ I(\mathfrak{n}) &= \left[(o_F/\mathfrak{n})^\times : E(\mathfrak{n})\right]. \end{aligned}$$

We note that the extension degree of the ray class field $F(\mathfrak{n})$ of conductor $\mathfrak{n}$ of F over F is the product of $I(\mathfrak{n})$ and the class number of F by the class field theory.

We studied cases where $\mathfrak{n}$'s are prime ideals. Indeed, for the set of prime ideals $\mathfrak{p}$ for which the Frobenius automorphism is a prescribed one, we showed that there is a polynomial h with rational coefficients such that $I(\mathfrak{p})$ is divisible by $h(p)$ for a prime number p lying below $\mathfrak{p}$ and conjectured that prime ideals satisfying $h(p) = I(\mathfrak{p})$ has a positive (modified natural) density [**K2**]. The conjectural density is really positive, and the conjecture is true for several cases under G.R.H. [**CKY**], [**K1**], [**K2**], [**K4**], [**L**], [**M**], [**R**]. As a next step, we proceed to the case of ideals $\mathfrak{n} = po_F$ with a rational prime number. In this case, finding out the polynomial h above is difficult, because we have to manage the obstruction group

$$M(\mathfrak{n}) = \left\{(a_0, \cdots, a_m) \in \boldsymbol{Z}^{m+1} \middle| \zeta^{a_0}\epsilon_1^{a_1}\cdots\epsilon_m^{a_m} \equiv 1 \bmod \mathfrak{n}\right\}$$

where $\{\epsilon_1, \cdots, \epsilon_m\}$ is a set of fundamental units of F and ζ is a generator of the group of roots of unity in F. If $\mathfrak{n}$ is a prime ideal, then $(o_F/\mathfrak{n})^\times$ is cyclic, and if the rank of the unit group $o_F^\times$ is one, $E(\mathfrak{n})$ is almost cyclic. In such cases, we have only to consider the

2000 *Mathematics Subject Classification.* 11R27.
Key Words and Phrases. Distribution of units, cubic abelian field.
Partially supported by Grant-in-Aid for Scientific Research (C), Ministry of Education, Culture, Sports, Science and Technology of Japan.

order of each unit modulo $\mathfrak{n}$, and so such cases are relatively easy. The former case is in [**K2**]. In the latter case, we announced the polynomial h explicitly in some cases of the rank of $o_F^\times$ being one, and the positivity of the conjectural density [**K3**]. Contrary to it, in case of $m \geq 2$, we must study the obstruction group seriously.

As the simplest case, we take up a cubic abelian field F, whose rank of $o_F^\times$ is two. Let p be a prime number. The case where p runs over the set of rational primes which remain prime in F is contained in [**K2**]. The polynomial h, then is $(x-1)/2$ and we showed that the expected density is positive. We know that the ray class field of conductor being a prime number p contains the composite field of the Hilbert class field and $\boldsymbol{Q}(\zeta_p + \zeta_p^{-1})$ for a primitive pth root ζ_p of unity, and so, if the conjecture above is true, then they coincide for infinitely many primes.

In this paper, we confine ourselves to decomposable primes. Before explaining the content, we should remark: Let K be a Galois extension of the rational number field $\boldsymbol{Q}$, and let w, r be the order of the group of the roots of unity in K and the rank of the unit group. If a prime p decomposes fully in K, then $\#E((p))$ divides $w(p-1)^r/c_K$ with $c_K = 1$. $c_K > 1$ can happen, for example $c_K = 2$ holds for a real quadratic field with the norm of the fundamental unit being 1 [**K3**]. Note that $c_K > 1$ means that there are relations among units modulo p besides $\epsilon^{p-1} \equiv 1 \bmod (p)$.

Now, F denotes a cubic abelian field as before. In the first section, we evaluate the number of prime numbers p for which $\#E((p)) = 2(p-1)^2$ holds. We involve Frobenius automorphisms, and conjecture the density, taking account of Chebotarev's density theorem. The key is the proposition 2, which describes the obstruction group $\{\epsilon \in o_F^\times | \epsilon \equiv 1 \bmod (p)\}$ explicitly, and makes the evaluation of the number of primes with $\#E((p)) = 2(p-1)^2$ possible, using Frobenius automorphisms. We do not have any extension, i.e. any algebraic frame to express the condition $\#E((p)) = w(p-1)^r/c_K$ in terms of Frobenius automorphism for a general Galois extension yet.

In the second section, we write down the conjectural density explicitly. Making use of details on fields $F(\sqrt[m]{o_F^\times})$, we see that it is really positive, and so $c_F = 1$ is expected. The numerical data support the conjecture. Like Artin's conjecture on primitive roots, the proof of our conjecture shall involve the estimate of the infinitely many accumulation of error terms of analytic version of Chebotarev's density theorem.

Hereafter F is a cubic abelian field with Galois group $\langle \sigma \rangle$, and $E(\mathfrak{n}), I(\mathfrak{n})$ are those defined above. Here $\langle g_1, \cdots, g_n \rangle$ stands for the group generated by $g_1, \cdots, g_n$. d_F stands for the discriminant of F. Moreover the letter p denotes an odd prime number which decomposes in F, and ℓ denotes a prime number. Let m be a natural number. ζ_m denotes a primitive mth root of unity. F_m stands for $F(\sqrt[m]{o_F^\times})$, which is a finite Galois extension over $\boldsymbol{Q}$. For a prime ideal $\mathfrak{p}$ of F_m lying above p, $\sigma_{F_m/\boldsymbol{Q}}(\mathfrak{p})$ denotes the Frobenius automorphism corresponding to $\mathfrak{p}$, and $\sigma_{F_m/\boldsymbol{Q}}(p)$ denotes the conjugacy class of $\mathrm{Gal}(F_m/\boldsymbol{Q})$ containing $\sigma_{F_m/\boldsymbol{Q}}(\mathfrak{p})$.

§1.

In this section, we show that $\#E((p))$ divides $2(p-1)^2$ and describe the number of prime numbers p satisfying $p < x$ and $\#E((p)) = 2(p-1)^2$, i.e. $I((p)) = (p-1)/2$ in terms of Frobenius automorphisms.

Proposition 1. *We can choose a set $\{\epsilon_1, \epsilon_2\}$ of fundamental units of F such that*

$$\epsilon_1^\sigma = \epsilon_2,\ \epsilon_2^\sigma = (\epsilon_1\epsilon_2)^{-1},$$

and we have $\langle\epsilon_1, \epsilon_2\rangle = \{\epsilon \in o_F^\times | N_{F/\boldsymbol{Q}}(\epsilon) = 1\}$.

Proof. The unit group $o_F^\times$ is the direct product of $\{\pm 1\}$ and $\{\epsilon \in o_F^\times | N_{F/\boldsymbol{Q}}(\epsilon) = 1\}$. By considering $\{\epsilon \in o_F^\times | N_{F/\boldsymbol{Q}}(\epsilon) = 1\}$ as a free $\boldsymbol{Z}$-module of rank two and by applying the theory of integral representation of a cyclic group $\langle\sigma\rangle$ of order three operating on it [**CR**], there is a system $\{\epsilon_1, \epsilon_2\}$ of fundamental units such that

$$\epsilon_1^\sigma = \epsilon_2,\ \epsilon_2^\sigma = (\epsilon_1\epsilon_2)^{-1}.$$

This completes the proof. □

Hereafter ϵ_1, ϵ_2 are those in the proposition 1. By virtue of the proposition, $\epsilon \equiv -1 \bmod (p)$ does not happen for $\epsilon \in \langle\epsilon_1, \epsilon_2\rangle$, since it implies $1 = N_{F/\boldsymbol{Q}}(\epsilon) \equiv -1 \bmod (p)$ holds, which contradicts our assumption that p is odd. Hence we redefine the obstruction group $M = M_p$ by

$$M_p := \left\{(a_1, a_2) \in (\boldsymbol{Z}/(p-1)\boldsymbol{Z})^2 \middle| \epsilon_1^{a_1}\epsilon_2^{a_2} \equiv 1 \bmod (p)\right\},$$

which is different from the definition in the introduction. Here we note $\epsilon^{p-1} \equiv 1 \bmod (p)$ for every $\epsilon \in o_F^\times$ since p is supposed to decompose in F.

Proposition 2. *There are natural numbers $D_1 = D_1(p), D_2 = D_2(p), b = b(p)$ which satisfy*

(i) $D_1D_2 | p-1$,
(ii) $d_1 := (p-1)/D_1$ *is the order of* $\epsilon_i \bmod (p)$ $(i = 1, 2)$,
(iii) $M_p = \langle(d_1, 0), (0, d_1)\rangle + \langle(d_2, bd_2)\rangle$ *where* $d_2 = (p-1)/D_1D_2$.

Moreover, b satisfies $b^2 - b + 1 \equiv 0 \bmod D_2$ and it is uniquely determined modulo D_2.

Proof. By $\epsilon_2 = \epsilon_1^\sigma$, the order d_1 of $\epsilon_2 \bmod (p)$ is equal to that of $\epsilon_1 \bmod (p)$. Put $d_1 = (p-1)/D_1$; then M contains clearly

$$\begin{aligned} S :&= \left\{(a_1, a_2) \in (\boldsymbol{Z}/(p-1)\boldsymbol{Z})^2 \middle| \epsilon_i^{a_i} \equiv 1 \bmod (p) (i = 1, 2)\right\} \\ &= \langle(d_1, 0), (0, d_1)\rangle. \end{aligned}$$

If $M = S$ holds, then we have only to put $D_2 = 1$ and $b = 0$.

Suppose $M \neq S$ and choose $(a_1, a_2) \in M \setminus S$ so that a_1 is the minimal natural number satisfying $(a_1, a_2) \in M \setminus S$. It is easy to see $0 < a_1 \leq d_1$. If $a_1 = d_1$, then we have $\epsilon_2^{a_2} \equiv 1 \bmod (p)$ and then $a_2 \equiv 0 \bmod d_1$. It contradicts $(a_1, a_2) \notin S$. Hence $a_1 \neq d_1$ holds. Thus we have $0 < a_1 < d_1$ and a_1 is minimal in the set of natural numbers a such that $(a, *) \in M$. Put

$$A_1 = \gcd(a_1, d_1)$$

and write $A_1 = xa_1+yd_1$ $(x, y \in \boldsymbol{Z})$. Then $M \ni x(a_1, a_2) = (A_1-yd_1, xa_2) = (A_1, xa_2)-(yd_1, 0)$ implies $(A_1, xa_2) \in M$. The inequality $0 < A_1 \le a_1$ and the minimality of a_1 yield $A_1 = a_1$. By virtue of $A_1|d_1$,

$$a_1 = A_1 = d_1/D_2$$

holds for some integer D_2, where $1 < D_2|d_1$. Let us see

$$M = S + \langle (a_1, a_2) \rangle.$$

Suppose $(c_1, c_2) \in M$ and $c_1 = qa_1+r$, $0 \le r < a_1$. By virtue of $M \ni (c_1, c_2)-q(a_1, a_2) = (r, c_2-qa_2)$ and $0 \le r < a_1$, we have $r = 0$ by the minimality of a_1, and then $(0, c_2-qa_2) \in M$ yields $c_2 - qa_2 \equiv 0 \bmod d_1$ and so $(c_1, c_2) - q(a_1, a_2) = (0, c_2 - qa_2) \in S$. Thus we have $M = S + \langle (a_1, a_2) \rangle$. By virtue of $(\epsilon_1^{a_1}\epsilon_2^{a_2})^\sigma = \epsilon_1^{-a_2}\epsilon_2^{a_1-a_2}$, $(-a_2, a_1 - a_2) \in M$ holds. Hence we have $(-a_2, a_1 - a_2) + b(a_1, a_2) \in S$ for some integer b and so $a_2 \equiv ba_1 \bmod d_1$ and hence $(a_1, ba_1) = (a_1, a_2) - (0, a_2 - ba_1) \in M$ and $(a_1, a_2) - (a_1, ba_1) \in S$ follow. Thus we may assume

$$a_2 = ba_1$$

without loss of generality. Then $M \ni (-a_2, a_1 - a_2) + b(a_1, a_2) = (0, a_1(1-b+b^2))$ holds and so we get $a_1(1 - b + b^2) \equiv 0 \bmod d_1$. Since we put $a_1 = d_1/D_2$, the desired equation $1 - b + b^2 \equiv 0 \bmod D_2$ follows.

To show the uniqueness of $b \bmod D_2$, suppose $(a_1, b_ia_1) \in M$ $(i = 1, 2)$; then $M \ni (a_1, b_2a_1)-(a_1, b_1a_1) = (0, (b_2-b_1)a_1)$ implies $(b_2-b_1)a_1 \equiv 0 \bmod d_1$, and hence $b_2-b_1 \equiv 0 \bmod D_2$. Thus we have completed the proof. $\square$

PROPOSITION 3. *$\#E((p))$ divides $2(p-1)^2$, and $I((p))$ is divisible by $(p-1)/2$.*

PROOF. The natural mapping φ from $\langle -1 \bmod (p) \rangle \times \langle \epsilon_1 \bmod (p) \rangle \times \langle \epsilon_2 \bmod (p) \rangle$ to $E((p))\,(= \{u \bmod (p) | u \in o_F^\times\})$ is surjective. Therefore $\#E((p)) = 2\#\langle \epsilon_1 \bmod (p) \rangle \dot{\#}\langle \epsilon_2 \bmod (p) \rangle / \# \ker \varphi$ holds. By assumption on p, (p) decomposes in F and so $\#\langle \epsilon_1 \bmod (p) \rangle = \#\langle \epsilon_2 \bmod (p) \rangle$ divides $(p-1)$. Thus $\#E((p))$ divides $2(p-1)^2$. Hence $I((p)) = [(o_F/(p))^\times : E((p))] = (p-1)^3/\#E((p))$ is divisible by $(p-1)/2$. $\square$

The following follows from the proposition 2, 3.

COROLLARY 1. *$I((p)) = (p-1)/2$ and hence $\#E((p)) = 2(p-1)^2$ holds if and only if M_p is trivial, i.e. $D_1(p) = D_2(p) = 1$ holds.*

REMARK. The proposition 2 and the proof of the proposition 3 imply $\#E((p)) = 2(p-1)^2/\#M_p = 2(p-1)^2/D_1^2D_2\,(\in \boldsymbol{Z})$, and hence $I((p)) = (p-1)/2 \cdot D_1^2D_2$. Moreover the equation $x^2 - x + 1 \equiv 0 \bmod D_2$ has to have a solution and so a prime divisor ℓ of D_2 is 3 or congruent to 1 modulo 3.

PROPOSITION 4. *Let ϵ be a unit of F and $r=(p-1)/D$ the order of ϵ mod (p), and let m be an integer relatively prime to p. Then m divides D if and only if $\zeta_m^{\rho-1} = \sqrt[m]{\epsilon}^{\rho-1}=1$ for every $\rho\in\sigma_{F_m/\boldsymbol{Q}}(p)$.*

PROOF. Since p is supposed to decompose in F, we have $\epsilon^{p-1}\equiv 1 \bmod (p)$. Therefore the order r of ϵ mod (p) divides $p-1$ and $D=(p-1)/r$ is an integer. Then

$$\begin{aligned} m|D=(p-1)/r &\Leftrightarrow m|p-1 \text{ and } r|(p-1)/m \\ &\Leftrightarrow m|p-1 \text{ and } \epsilon^{(p-1)/m}\equiv 1 \bmod (p) \\ &\Leftrightarrow m|p-1 \text{ and } \epsilon^{(p-1)/m}\equiv 1 \bmod \mathfrak{p} \text{ for } {}^{\forall}\mathfrak{p}|p \\ &\qquad \text{where } \mathfrak{p} \text{ is a prime ideal in } F_m \\ &\Leftrightarrow \zeta_m^{\rho-1}=1 \text{ and } \sqrt[m]{\epsilon}^{\rho-1}=1 \text{ for } \rho=\sigma_{F_m/\boldsymbol{Q}}(\mathfrak{p}), {}^{\forall}\mathfrak{p}|p. \end{aligned}$$

Let us explain the last equivalence. Since p decomposes in F, ρ is the identity on F and then $\sqrt[m]{\epsilon}^{\rho-1}$ is an mth root of unity. Suppose that ζ is an mth root of unity. We have only to show $\zeta\equiv 1 \bmod \mathfrak{p}$ implies $\zeta=1$. If $\zeta\neq 1$, then there is a prime $\ell\,(|m)$ such that $\zeta_\ell\equiv 1 \bmod \mathfrak{p}$. Therefore $p=\ell|m$ holds, which contradicts $(m,p)=1$. □

PROPOSITION 5. *Let $D_1(p), D_2(p), b(p)$ be those in the proposition 2, and suppose that a natural number n divides $(p-1)/D_1(p)$. Then $n|D_2(p)$ holds if and only if*

$$\sqrt[D_1(p)n]{\epsilon_1\epsilon_2^b}^{\rho-1}=1 \text{ for } {}^{\forall}\rho\in\sigma_{F_{D_1(p)n}/\boldsymbol{Q}}(p) \tag{1}$$

holds for some integer b. Then b is uniquely determined modulo n so that $b\equiv b(p)$ mod n.

PROOF. For simplicity, we write $D_i(p)=D_i$. If n divide D_2, then putting $D_2=nr$, we have

$$M_p\ni r\big((p-1)/D_1D_2, b(p)(p-1)/D_1D_2\big)=\big((p-1)/D_1n, b(p)(p-1)/D_1n\big),$$

and hence $\epsilon_1^{(p-1)/D_1n}\epsilon_2^{b(p)(p-1)/D_1n}\equiv 1 \bmod (p)$. Hence the order of $\epsilon=\epsilon_1\epsilon_2^{b(p)}$ mod (p) is $(p-1)/D_1na$ for a natural number a. Applying the previous proposition to $\epsilon, m=D_1n\,(\not\equiv 0 \bmod p)$, we have

$$\sqrt[D_1n]{\epsilon_1\epsilon_2^{b(p)}}^{\rho-1}=1 \text{ for } {}^{\forall}\rho\in\sigma_{F_{D_1n}/\boldsymbol{Q}}(p).$$

Conversely, the equation (1) yields $M_p\ni((p-1)/D_1n, b\cdot(p-1)/D_1n)$, and then $n|D_2$ by virtue of the proposition 2.

To show the uniqueness of b, suppose that $n|D_2$ and $\sqrt[D_1n]{\epsilon_1\epsilon_2^b}^{\rho-1}=1$ for ${}^{\forall}\rho\in\sigma_{F_{D_1n}/\boldsymbol{Q}}(p)$ holds for some integer b. Then we have both $M_p\ni((p-1)/D_1n, b\cdot(p-1)/D_1n)$ and $M_p\ni((p-1)/D_1n, b(p)(p-1)/D_1n)$, and so the difference $(0,(b-b(p))(p-1)/D_1n)\in M_p$. The proposition 2 implies $n|(b(p)-b)$, which completes the proof. □

Proposition 6. *For natural numbers b, n, suppose*

$$\zeta_n^{\rho-1} = \sqrt[n]{\epsilon_1\epsilon_2^b}^{\rho-1} = 1 \textit{ for } {}^\forall\rho \in \sigma_{F_n/\boldsymbol{Q}}(p).$$

Then $\sqrt[n]{\epsilon_2}^{(b^2-b+1)(\rho-1)} = 1$ *holds for* ${}^\forall\rho \in \sigma_{F_n/\boldsymbol{Q}}(p)$.

Proof. Take an automorphism $\eta \in \mathrm{Gal}(F_n/\boldsymbol{Q})$ satisfying $\eta = \sigma$ on F. For $\rho \in \sigma_{F_n/\boldsymbol{Q}}(p)$, $\eta\rho\eta^{-1} \in \sigma_{F_n/\boldsymbol{Q}}(p)$ implies $\sqrt[n]{\epsilon_1\epsilon_2^b}^{\eta\rho} = \sqrt[n]{\epsilon_1\epsilon_2^b}^{\eta}$ by the assumption. On the other hand, we have $(\epsilon_1\epsilon_2^b)^\eta = \epsilon_1^{-b}\epsilon_2^{1-b} = (\epsilon_1\epsilon_2^b)^{-b}\epsilon_2^{b^2-b+1}$, and then $\sqrt[n]{\epsilon_1\epsilon_2^b}^{\eta} = \zeta\sqrt[n]{\epsilon_1\epsilon_2^b}^{-b}\sqrt[n]{\epsilon_2}^{b^2-b+1}$ for an nth root ζ of unity. Thus $\sqrt[n]{\epsilon_1\epsilon_2^b}^{\eta\rho}$ is equal to $\zeta\sqrt[n]{\epsilon_1\epsilon_2^b}^{-b}\sqrt[n]{\epsilon_2}^{(b^2-b+1)\rho} = \sqrt[n]{\epsilon_1\epsilon_2^b}^{\eta}\sqrt[n]{\epsilon_2}^{(b^2-b+1)(\rho-1)}$. Comparing it with the above, we have $\sqrt[n]{\epsilon_2}^{(b^2-b+1)(\rho-1)} = 1$. $\square$

Proposition 7. *For natural numbers m, n, b, we set*

$$H(m,n;b) = \left\{\rho \in \mathrm{Gal}(F_{mn}/\boldsymbol{Q}) \,\middle|\, \begin{array}{l} \text{(i) } \zeta_m^{\rho-1} = \sqrt[m]{\epsilon_i}^{\rho-1} = 1 \textit{ for } i = 1,2, \\ \text{(ii) } \zeta_n^{\rho-1} = \sqrt[n]{\epsilon_1\epsilon_2^b}^{\rho-1} = \sqrt[n]{\epsilon_2}^{(b^2-b+1)(\rho-1)} = 1 \end{array}\right\}.$$

Then it is a union of conjugacy classes of $\mathrm{Gal}(F_{mn}/\boldsymbol{Q})$.

Proof. Let $\rho \in H(m,n;b)$ and $\eta \in \mathrm{Gal}(F_{mn}/\boldsymbol{Q})$. It is clear that we have only to see $\sqrt[m]{\epsilon_i}^{\eta\rho\eta^{-1}-1} = \sqrt[n]{\epsilon_1\epsilon_2^b}^{\eta\rho\eta^{-1}-1} = \sqrt[n]{\epsilon_2}^{(b^2-b+1)(\eta\rho\eta^{-1}-1)} = 1$.

(i) In case of $\eta = \mathrm{id}$ on F.

Since $\sqrt[m]{\epsilon_i}^{\eta} = \zeta\sqrt[m]{\epsilon_i}$ for an mth root ζ of unity, it is easy to see $\sqrt[m]{\epsilon_i}^{\eta\rho} = \sqrt[m]{\epsilon_i}^{\eta}$ and so $\sqrt[m]{\epsilon_i}^{\eta\rho\eta^{-1}-1} = 1$. The others are similar.

(ii) In case of $\eta = \sigma$ on F.

$\epsilon_1^\eta = \epsilon_2$ and $\epsilon_2^\eta = (\epsilon_1\epsilon_2)^{-1}$ imply $\sqrt[m]{\epsilon_1}^{\eta} = \alpha_1\sqrt[m]{\epsilon_2}$, $\sqrt[m]{\epsilon_2}^{\eta} = \alpha_2\sqrt[m]{\epsilon_1\epsilon_2}^{-1}$ for mth roots α_1, α_2 of unity and hence $\sqrt[m]{\epsilon_i}^{\eta\rho} = \sqrt[m]{\epsilon_i}^{\eta}$ for $i = 1, 2$. Because of $(\epsilon_1\epsilon_2^b)^\eta = (\epsilon_1\epsilon_2^b)^{-b}\epsilon_2^{b^2-b+1}$, we have $\sqrt[n]{\epsilon_1\epsilon_2^b}^{\eta} = \alpha_3\sqrt[n]{\epsilon_1\epsilon_2^b}^{-b}\sqrt[n]{\epsilon_2}^{b^2-b+1}$ for an nth root α_3 of unity and then $\sqrt[n]{\epsilon_1\epsilon_2^b}^{\eta\rho} = \sqrt[n]{\epsilon_1\epsilon_2^b}^{\eta}$. By virtue of $\epsilon_2^\eta = (\epsilon_1\epsilon_2^b)^{-1}\epsilon_2^{b-1}$, we obtain $\sqrt[n]{\epsilon_2}^{\eta} = \alpha_4\sqrt[n]{\epsilon_1\epsilon_2^b}^{-1}\sqrt[n]{\epsilon_2}^{b-1}$ for an nth root of α_4 of unity and so $\sqrt[n]{\epsilon_2}^{(b^2-b+1)\eta\rho} = \sqrt[n]{\epsilon_2}^{(b^2-b+1)\eta}$.

(iii) In case of $\eta = \sigma^2$ on F.

$\epsilon_1^\eta = (\epsilon_1\epsilon_2)^{-1}$ and $\epsilon_2^\eta = \epsilon_1$ yield $\sqrt[m]{\epsilon_i}^{\eta\rho} = \sqrt[m]{\epsilon_i}^{\eta}$ for $i = 1, 2$. $(\epsilon_1\epsilon_2^b)^\eta = (\epsilon_1\epsilon_2^b)^{b-1}\epsilon_2^{-(b^2-b+1)}$ implies $\sqrt[n]{\epsilon_1\epsilon_2^b}^{\eta\rho} = \sqrt[n]{\epsilon_1\epsilon_2^b}^{\eta}$, and $\epsilon_2^\eta = (\epsilon_1\epsilon_2^b)\epsilon_2^{-b}$ implies $\sqrt[n]{\epsilon_2}^{(b^2-b+1)\eta\rho} = \sqrt[n]{\epsilon_2}^{(b^2-b+1)\eta}$. $\square$

For a positive number x, we put

$$S_x = \{p \le x | p \text{ is an odd prime number which decomposes in } F\}$$

$$T_x = \{p \in S_x | I((p)) = (p-1)/2\} = \{p \in S_x | \#E((p)) = 2(p-1)^2\}.$$

Let us express the number $\#T_x$ in terms of Frobenius automorphisms. Since $\#E((p)) = 2(p-1)^2$ is equivalent to $D_1(p) = D_2(p) = 1$, we have

$$
\begin{aligned}
\#T_x &= \sum_{\substack{p\in S_x\\ D_1(p)=D_2(p)=1}} 1\\
&= \sum_{\substack{p\in S_x\\ D_1(p)=1}} \sum_{n|D_2(p)} \mu(n) \quad (\mu \text{ is the Möbius function})\\
&= \sum_n \mu(n) \sum_{\substack{p\in S_x\\ D_1(p)=1,\, n|D_2(p)}} 1\\
&= \sum_n \mu(n) \sum_{b \bmod n} \sum_{\substack{p\in S_x\\ D_1(p)=1,\, n|p-1,\\ \sqrt[n]{\epsilon_1\epsilon_2^b}^{\rho-1}=1 \text{ for } ^\forall\rho\in\sigma_{F_n/\boldsymbol{Q}}(p)}} 1
\end{aligned}
$$

(by the proposition 5, since $n|D_2(p)$ implies $n|p-1$)

$$
\begin{aligned}
&= \sum_n \mu(n) \sum_{b \bmod n} \sum_{\substack{p\in S_x\\ n|p-1,\\ \sqrt[n]{\epsilon_1\epsilon_2^b}^{\rho-1}=1 \text{ for } ^\forall\rho\in\sigma_{F_n/\boldsymbol{Q}}(p)}} \sum_{m|D_1(p)} \mu(m)\\
&= \sum_{n,m} \mu(n)\mu(m) \sum_{b \bmod n} \#\left\{ p\in S_x \,\middle|\, \begin{array}{l} \text{(i)}\ \ m|D_1(p)\\ \text{(ii)}\ p\equiv 1 \bmod n,\ \sqrt[n]{\epsilon_1\epsilon_2^b}^{\rho-1}=1\\ \qquad \text{for } ^\forall\rho\in\sigma_{F_n/\boldsymbol{Q}}(p)\end{array}\right\}\\
&= \sum_{n,m} \mu(n)\mu(m) \sum_{b \bmod n} \#\left\{ p\in S_x \,\middle|\, \begin{array}{l} \text{(0)}\ \ p\nmid mn\\ \text{(i)}\ \ \zeta_m^{\rho-1} = \sqrt[m]{\epsilon_1}^{\rho-1} = \sqrt[m]{\epsilon_2}^{\rho-1} = 1\\ \qquad \text{for } ^\forall\rho\in\sigma_{F_m/\boldsymbol{Q}}(p)\\ \text{(ii)}\ \zeta_n^{\rho-1}=1,\ \sqrt[n]{\epsilon_1\epsilon_2^b}^{\rho-1}=1\\ \qquad \text{for } ^\forall\rho\in\sigma_{F_n/\boldsymbol{Q}}(p),\end{array}\right\}
\end{aligned}
$$

(by the proposition 4)

$$
= \sum_{n,m} \mu(n)\mu(m) \sum_{b \bmod n} \#\{p\in S_x | p\nmid mn, \sigma_{F_{mn}/\boldsymbol{Q}}(p)\subset H(m,n;b)\}
$$

(by the proposition 6).

Thus we have shown

THEOREM 1. *The number $\#T_x$ is equal to*

$$
\sum_{n,m\geq 1} \mu(n)\mu(m) \sum_{b \bmod n} \#\{p\in S_x | p\nmid mn, \sigma_{F_{mn}/\boldsymbol{Q}}(p)\subset H(m,n;b)\}.
$$

Taking account of Chebotarev's density theorem, we propose

CONJECTURE.

$$
\lim_{x\to\infty} \#T_x/\mathrm{Li}(x) = \sum_{n,m} \mu(n)\mu(m) \sum_{b \bmod n} \frac{\#H(m,n;b)}{[F_{mn}:\boldsymbol{Q}]} = \kappa \quad \text{(say)}
$$

In the next section, we will show the expected density κ above is really positive.

§2.

Let us show that the infinite series κ in the conjecture is absolutely convergent to a positive number. The aim in this section is the following

Theorem 2. *We have*

$$\kappa = \frac{1}{4}\prod_{\ell\nmid 2d_F}\left(1+\frac{1}{\ell^2}-\frac{\alpha(\ell)}{(\ell-1)\ell^2}\right)\begin{cases}\prod_{\ell|d_F}\left(1+\dfrac{1}{\ell^2}-\dfrac{\alpha(\ell)}{(\ell-1)\ell^2}\right) & \text{if } 3|d_F,\\ \prod_{\ell|d_F}\left(1+\dfrac{1-2\ell}{(\ell-1)\ell^2}\right)+2\displaystyle\prod_{\ell|d_F}\frac{1-2\ell}{(\ell-1)\ell^2} & \text{if } 3\nmid d_F,\end{cases}$$

where ℓ denotes prime numbers and

$$\alpha(\ell)=\begin{cases}\ell & \text{if } \ell\equiv 2 \bmod 3,\\ 3\ell-2 & \text{if } \ell\equiv 1 \bmod 3,\\ \ell+2 & \text{if } \ell=3,\end{cases}$$

and $\kappa\neq 0$.

Before the proof, let us give numerical examples. Set $x=10^8$ and $\pi(x)$ is the number of primes not exceeding x. κ' denotes the partial product of κ for $\ell<450000$.
In case of $F\subset \boldsymbol{Q}(\zeta_7):\ \kappa'=0.17400\cdots$ and $\#T_x/\pi(x)=0.17410\cdots$,
In case of $F\subset \boldsymbol{Q}(\zeta_9):\ \kappa'=0.19175\cdots$ and $\#T_x/\pi(x)=0.19181\cdots$.

Since we have

$$\begin{aligned}\#H(m,n;b)/[F_{mn}:\boldsymbol{Q}] &= \left[\boldsymbol{Q}\left(\zeta_m,\ \sqrt[m]{\epsilon_1},\ \sqrt[m]{\epsilon_2},\zeta_n,\ \sqrt[n]{\epsilon_1\epsilon_2^b},\ \sqrt[n]{\epsilon_2}^{\,b^2-b+1}\right):\boldsymbol{Q}\right]^{-1}\\ &= 3^{-1}\left[F\left(\zeta_m,\ \sqrt[m]{\epsilon_1},\ \sqrt[m]{\epsilon_2},\zeta_n,\ \sqrt[n]{\epsilon_1\epsilon_2^b},\ \sqrt[n]{\epsilon_2}^{\,b^2-b+1}\right):F\right]^{-1},\end{aligned}$$

we set

$$k(m,n;b)=\left[F\left(\zeta_m,\ \sqrt[m]{\epsilon_1},\ \sqrt[m]{\epsilon_2},\zeta_n,\ \sqrt[n]{\epsilon_1\epsilon_2^b},\ \sqrt[n]{\epsilon_2}^{\,b^2-b+1}\right):F\right]$$

for simplicity, and then

$$\kappa=\frac{1}{3}\sum_{n,m\geq 1}\mu(n)\mu(m)\sum_{b \bmod n}1/k(m,n;b).$$

Put $m=m_1d, n=n_1d$ for $d=(m,n)$. Since we may assume that m,n are square-free, m_1n_1d is supposed to be square-free. So we have, replacing m_1,n_1 by m,n

$$\begin{aligned}
3\kappa &= \sum_{\substack{n,m,d\geq 1\\ mnd:\text{square-free}}} \mu(m)\mu(n) \sum_{b \bmod nd} 1/k(md,nd;b)\\
&= \sum_{\substack{n,m,d\geq 1\\ mnd:\text{square-free}}} \mu(m)\mu(n) \sum_{b \bmod nd} 1/k(md,n;b)\\
&\quad \text{(because of } k(md,nd;b)=k(md,n;b))\\
&= \sum_{\substack{n,m,d\geq 1\\ mnd:\text{square-free}}} \mu(m)\mu(n)d \sum_{b \bmod n} 1/k(md,n;b)\\
&\quad \text{(since } k(md,n;b) \text{ is determined by } b \bmod n, \text{ and putting } M=md)\\
&= \sum_{\substack{M,n\geq 1\\ Mn:\text{square-free}}} \mu(M)\mu(n)\Big(\sum_{d|M}\mu(d)d\Big) \sum_{b \bmod n} 1/k(M,n;b)\\
&= \sum_{\substack{m,n\geq 1\\ mn:\text{square-free}}} \mu(n)\varphi(m) \sum_{b \bmod n} 1/k(m,n;b)
\end{aligned}$$

since $\sum_{d|M}\mu(d)d=\prod_{\ell|M}(1-\ell)=\mu(M)\varphi(M)$, where ℓ stands for primes and φ is the Euler function.

Set

$$A=\prod_{\ell|2d_F}\ell.$$

We note that A is even and square-free. For natural numbers a,b with $a|A^\infty,(b,A)=1$, we know [**K2**]

$$[F_{ab}:F]=[F_a:F][F_b:F]=b^2\varphi(b)[F_a:F] \text{ and } F_a\cap F_b=F.$$

In particular, $(b_1,b_2)=1$ and $(b_1b_2,A)=1$ imply that F_{b_1} and F_{b_2} are linearly disjoint over F by $[F_{b_1b_2}:F]=(b_1b_2)^2\varphi(b_1b_2)$ and $[F_{b_i}:F]=b_i^2\varphi(b_i)$ for $i=1,2$.

Suppose that mn is square-free, and write $m=m_1m_2, n=n_1n_2$ so that $(m_1n_1,A)=1$ and $m_2n_2|A^\infty$. Then we have, noting that mn is square-free

$$\begin{aligned}
k(m,n;b) &= k(m_1m_2,n_1n_2;b)\\
&= \Big[F\Big(\zeta_{m_1},\ \sqrt[m_1]{\epsilon_1},\ \sqrt[m_1]{\epsilon_2},\ \zeta_{m_2},\ \sqrt[m_2]{\epsilon_1},\ \sqrt[m_2]{\epsilon_2},\\
&\qquad \zeta_{n_1},\ \sqrt[n_1]{\epsilon_1\epsilon_2^b},\ \sqrt[n_1]{\epsilon_2}^{\,b^2-b+1},\ \zeta_{n_2},\ \sqrt[n_2]{\epsilon_1\epsilon_2^b},\ \sqrt[n_2]{\epsilon_2}^{\,b^2-b+1}\Big):F\Big]\\
&= \Big[F\Big(\zeta_{m_1n_1},\ \sqrt[m_1]{\epsilon_1},\ \sqrt[m_1]{\epsilon_2},\ \sqrt[n_1]{\epsilon_1\epsilon_2^b},\ \sqrt[n_1]{\epsilon_2}^{\,b^2-b+1}\Big):F\Big]\\
&\quad \times\Big[F\Big(\zeta_{m_2n_2},\ \sqrt[m_2]{\epsilon_1},\ \sqrt[m_2]{\epsilon_2},\ \sqrt[n_2]{\epsilon_1\epsilon_2^b},\ \sqrt[n_2]{\epsilon_2}^{\,b^2-b+1}\Big):F\Big]\\
&\quad \text{(by } F_{m_1n_1} \text{ and } F_{m_2n_2} \text{ being linearly disjoint over } F)\\
&= k(m_1,n_1;b)k(m_2,n_2;b).
\end{aligned}$$

Since mn is square-free, $(m,n)=1$ holds and $(m_1n_1,2)=1$, we have

$$\begin{aligned}k(m_1,n_1;b) &= \Big[F\Big(\zeta_{m_1n_1},\ \sqrt[m_1]{\epsilon_1},\ \sqrt[m_1]{\epsilon_2},\ \sqrt[n_1]{\epsilon_1\epsilon_2^b},\ \sqrt[n_1]{\epsilon_2}^{\,b^2-b+1}\Big):F\Big]\\ &= [F_{m_1}:F]\Big[F\Big(\zeta_{n_1},\ \sqrt[n_1]{\epsilon_1\epsilon_2^b},\ \sqrt[n_1]{\epsilon_2}^{\,b^2-b+1}\Big):F\Big]\\ &= \varphi(m_1)m_1^2\prod_{\ell|n_1}\Big[F\Big(\zeta_\ell,\sqrt[\ell]{\epsilon_1\epsilon_2^b},\sqrt[\ell]{\epsilon_2}^{\,b^2-b+1}\Big):F\Big].\end{aligned}$$

By virtue of $[F_\ell:F]=\varphi(\ell)\ell^2$ for $\ell|n_1$, we see

$$\begin{aligned}\Big[F\Big(\zeta_\ell,\sqrt[\ell]{\epsilon_1\epsilon_2^b},\sqrt[\ell]{\epsilon_2}^{\,b^2-b+1}\Big):F\Big] &= \begin{cases}\varphi(\ell)\ell & \text{if } b^2-b+1\equiv 0 \bmod \ell,\\ \varphi(\ell)\ell^2 & \text{if } b^2-b+1\not\equiv 0 \bmod \ell\end{cases}\\ &= \varphi(\ell)\ell^{2-\alpha(b,\ell)},\end{aligned}$$

where we put

$$\alpha(b,\ell)=\begin{cases}1 & \text{if } b^2-b+1\equiv 0 \bmod \ell,\\ 0 & \text{if } b^2-b+1\not\equiv 0 \bmod \ell.\end{cases}$$

Therefore we have

$$k(m_1,n_1;b)=\varphi(m_1)m_1^2\varphi(n_1)n_1^2\prod_{\ell|n_1}\ell^{-\alpha(b,\ell)},$$

and 3κ is equal to

$$\sum_{\substack{m_1,m_2,n_1,n_2\geq 1,\\ m_1m_2n_1n_2:\text{square-free}\\ (m_1n_1,A)=1,m_2n_2|A}}\mu(n_1n_2)\varphi(m_1m_2)\sum_{b \bmod n_1n_2}\frac{\prod_{\ell|n_1}\ell^{\alpha(b,\ell)}}{\varphi(m_1)m_1^2\varphi(n_1)n_1^2}\cdot\frac{1}{k(m_2,n_2;b)}.$$

Writing $b=b_1n_2+b_2n_1$, we see easily

$$\alpha(b,\ell)=\alpha(b_1n_2,\ell) \text{ for } \ell|n_1 \text{ and } k(m_2,n_2;b)=k(m_2,n_2;b_2n_1),$$

and then, replacing b_1n_2, b_2n_1 by b_1,b_2 respectively

$$\begin{aligned}3\kappa = &\sum_{\substack{m_1,n_1\geq 1,\\ m_1n_1:\text{square-free}\\ (m_1n_1,A)=1}}\ \sum_{b_1 \bmod n_1}\frac{\mu(n_1)\prod_{\ell|n_1}\ell^{\alpha(b_1,\ell)}}{m_1^2\varphi(n_1)n_1^2}\\ &\times\sum_{\substack{m_2,n_2\geq 1,\\ m_2n_2|A}}\mu(n_2)\varphi(m_2)\sum_{b_2 \bmod n_2}1/k(m_2,n_2;b_2)\\ = &\ E_I\times E_{II}\quad \text{(say)}.\end{aligned}$$

We see

$$
\begin{aligned}
E_I &= \sum_{\substack{m,n\geq 1,\\ mn:\text{square-free}\\ (mn,A)=1}} \sum_{b \bmod n} \frac{\mu(n)\prod_{\ell|n}\ell^{\alpha(b,\ell)}}{m^2\varphi(n)n^2} \\
&= \sum_{n\geq 1,(n,A)=1} \frac{\mu(n)}{\varphi(n)n^2} \sum_{b \bmod n} \prod_{\ell|n} \ell^{\alpha(b,\ell)} \sum_{\substack{m\geq 1,(m,nA)=1,\\ m:\text{square-free}}} \frac{1}{m^2} \\
&= \sum_{n\geq 1,(n,A)=1} \frac{\mu(n)}{\varphi(n)n^2} \sum_{b \bmod n} \prod_{\ell|n} \ell^{\alpha(b,\ell)} \prod_{\ell\nmid nA}\left(1+\frac{1}{\ell^2}\right) \\
&= \prod_{\ell\nmid A}\left(1+\frac{1}{\ell^2}\right) \sum_{n\geq 1,(n,A)=1} \frac{\mu(n)}{\varphi(n)n^2}\left(\sum_{b \bmod n}\prod_{\ell|n}\ell^{\alpha(b,\ell)}\right)\prod_{\ell|n}\left(1+\frac{1}{\ell^2}\right)^{-1}.
\end{aligned}
$$

Writing $n = n_1n_2$ and $b = b_1n_2 + b_2n_1$, we see

$$
\begin{aligned}
\sum_{b \bmod n}\prod_{\ell|n}\ell^{\alpha(b,\ell)} &= \sum_{\substack{b_1 \bmod n_1\\ b_2 \bmod n_2}} \prod_{\ell|n_1}\ell^{\alpha(b_1n_2,\ell)}\prod_{\ell|n_2}\ell^{\alpha(b_2n_1,\ell)} \\
&= \left(\sum_{b_1 \bmod n_1}\prod_{\ell|n_1}\ell^{\alpha(b_1,\ell)}\right)\left(\sum_{b_2 \bmod n_2}\prod_{\ell|n_2}\ell^{\alpha(b_2,\ell)}\right),
\end{aligned}
$$

and hence inductively

$$
\sum_{b \bmod n}\prod_{\ell|n}\ell^{\alpha(b,\ell)} = \prod_{\ell|n}\left(\sum_{b \bmod \ell}\ell^{\alpha(b,\ell)}\right).
$$

Therefore E_I turns out to be

$$
\begin{aligned}
&\prod_{\ell\nmid A}\left(1+\frac{1}{\ell^2}\right)\cdot\prod_{\ell\nmid A}\left(1-\frac{1}{\varphi(\ell)\ell^2}\sum_{b \bmod \ell}\ell^{\alpha(b,\ell)}\times\left(1+\frac{1}{\ell^2}\right)^{-1}\right) \\
&\quad= \prod_{\ell\nmid A}\left(1+\frac{1}{\ell^2}-\frac{1}{(\ell-1)\ell^2}\sum_{b \bmod \ell}\ell^{\alpha(b,\ell)}\right).
\end{aligned}
$$

It is easy to see

$$
\alpha(\ell) := \sum_{b \bmod \ell}\ell^{\alpha(b,\ell)} = \begin{cases} \ell & \text{if } \ell\equiv 2 \bmod 3, \\ 3\ell-2 & \text{if } \ell\equiv 1 \bmod 3, \\ \ell+2 & \text{if } \ell = 3. \end{cases}
$$

Finally we have

$$E_I = \prod_{\ell \nmid A} \left(1 + \frac{1}{\ell^2} - \frac{\alpha(\ell)}{(\ell-1)\ell^2}\right).$$

Because of $\alpha(\ell) \le 3\ell - 2 = 2(\ell-1) + \ell$, we have

$$\frac{\alpha(\ell)}{(\ell-1)\ell^2} \le \frac{2}{\ell^2} + \frac{1}{(\ell-1)\ell} = \frac{1}{\ell^2} + \left(\frac{1}{\ell^2} + \frac{1}{(\ell-1)\ell}\right) < \frac{1}{\ell^2} + 1$$

by $\ell \ge 2$, and hence we have $E_I \ne 0$.

To study the term E_{II}, we need several algebraic preparations.

Let f be the conductor of F, that is, f is the minimal natural number such that $F \subset \boldsymbol{Q}(\zeta_f)$. By virtue of $[F : \boldsymbol{Q}] = 3$, we see that f or $f/9$ is a product of prime numbers which are congruent to one modulo 3.

Lemma 1. *Let m, n be natural numbers such that $(m,n) = 1$, $F \not\subset \boldsymbol{Q}(\zeta_m)$ and $F \not\subset \boldsymbol{Q}(\zeta_n)$. Then we have*

$$[F(\zeta_m) \cap F(\zeta_n) : F] = \begin{cases} 1 & \text{if } F \not\subset \boldsymbol{Q}(\zeta_{mn}), \\ 3 & \text{if } F \subset \boldsymbol{Q}(\zeta_{mn}). \end{cases}$$

Proof. The assumption implies $[F(\zeta_m) : F] = [\boldsymbol{Q}(\zeta_m) : \boldsymbol{Q}] = \varphi(m)$ and $[F(\zeta_n) : F] = \varphi(n)$. Then the assertion follows from

$$\begin{aligned} [F(\zeta_m) \cap F(\zeta_n) : F] &= \frac{[F(\zeta_m) : F]}{[F(\zeta_m) : F(\zeta_m) \cap F(\zeta_n)]} \\ &= \frac{\varphi(m)[F(\zeta_n) : F]}{[F(\zeta_{mn}) : F]} \quad (\text{by } F(\zeta_m)(\zeta_n) = F(\zeta_{mn})) \\ &= \frac{\varphi(m)\varphi(n)}{[\boldsymbol{Q}(\zeta_{mn}) : \boldsymbol{Q}(\zeta_{mn}) \cap F]}. \end{aligned}$$

□

Lemma 2. *If $(n,m) = 1$, then $F_m \cap F_n \subset F(\zeta_{mn})$ holds.*

Proof. The extension degree of $F_m(\zeta_{mn}) = F(\zeta_{mn})(\sqrt[m]{o_F^\times})$ over $F(\zeta_{mn})$ divides m^∞ by theory of Kummer extension. Similarly that of $F_n(\zeta_{mn})$ divides n^∞, and then $F(\zeta_{mn})(\sqrt[m]{o_F^\times}) \cap F(\zeta_{mn})(\sqrt[n]{o_F^\times}) = F(\zeta_{mn})$. Thus we have $F_m \cap F_n \subset F_m(\zeta_{mn}) \cap F_n(\zeta_{mn}) = F(\zeta_{mn})$. □

Lemma 3. *If m is square-free and $F \not\subset \boldsymbol{Q}(\zeta_m)$, then $x^m - \epsilon$ is irreducible over $F(\zeta_m)$, where $\pm\epsilon \in o_F^\times$ are supposed not to be a power of a unit in F.*

Proof. Since m is square-free, we have only to show $\epsilon \notin F(\zeta_m)^\ell$ for any prime $\ell | m$. Suppose $\epsilon \in F(\zeta_m)^\ell$ for a prime divisor ℓ of m. By virtue of $F \subset F(\sqrt[\ell]{\epsilon}) \subset F(\zeta_m)$, $F(\sqrt[\ell]{\epsilon})/F$ is a Galois extension, and then the assumption $\sqrt[\ell]{\epsilon} \notin F$ implies $F(\sqrt[\ell]{\epsilon}) \ne F$ and then $\zeta_\ell \sqrt[\ell]{\epsilon} \in F(\sqrt[\ell]{\epsilon})$, and so $\zeta_\ell \in F(\sqrt[\ell]{\epsilon})$. If $F \cap \boldsymbol{Q}(\zeta_\ell) \ne \boldsymbol{Q}$, then $F \subset \boldsymbol{Q}(\zeta_\ell)$ holds because of $[F:\boldsymbol{Q}]=3$. This contradicts $F\not\subset\boldsymbol{Q}(\zeta_m)$. Thus we have $F\cap\boldsymbol{Q}(\zeta_\ell)=\boldsymbol{Q}$ and hence $[F(\zeta_\ell):F]=[\boldsymbol{Q}(\zeta_\ell):\boldsymbol{Q}]=\ell-1$. Suppose $\ell\neq 2$; then $\ell\geq[F(\sqrt[\ell]{\epsilon}):F]=[F(\sqrt[\ell]{\epsilon}):F(\zeta_\ell)](\ell-1)$ holds. Thus $\ell>2$ implies $[F(\sqrt[\ell]{\epsilon}):F(\zeta_\ell)]=1$, i.e. $F(\sqrt[\ell]{\epsilon})=F(\zeta_\ell)$. This is a contradiction since $F(\sqrt[\ell]{\epsilon})$ has a real conjugate field and $F(\zeta_\ell)$ is totally imaginary. Next, suppose $\ell=2$; then we have $F\subsetneq F(\sqrt{\epsilon})\subset F(\zeta_m)$. Therefore there is a quadratic field $\boldsymbol{Q}(\sqrt{D})$ in $\boldsymbol{Q}(\zeta_m)$ satisfying $F(\sqrt{\epsilon})=F(\sqrt{D})$ by virtue of $F\cap\boldsymbol{Q}(\zeta_m)=\boldsymbol{Q}$, where D is a square-free integer. It implies $\sqrt{\epsilon}/\sqrt{D}\in F$ and then $\epsilon=Da^2$ for some $a\in F$. If $D\neq-1$, then prime divisors q of D have an even ramification index at F. It contradicts $[F:\boldsymbol{Q}]=3$. Thus we have $\epsilon=-a^2$, which also contradicts the assumption. □

Lemma 4. *If m is odd and square-free, and if $F\not\subset\boldsymbol{Q}(\zeta_m)$, then we have $[F_m:F(\zeta_m)]=m^2$ and $[F_m:F]=m^2\varphi(m)$.*

Proof. Since m is odd, we obtain $F_m=F(\zeta_m,\ \sqrt[m]{\epsilon_1},\ \sqrt[m]{\epsilon_2})$ and

$$\begin{aligned}[F_m:F(\zeta_m)]&=[F(\zeta_m,\ \sqrt[m]{\epsilon_1},\ \sqrt[m]{\epsilon_2}):F(\zeta_m)]\\&=[F(\zeta_m,\ \sqrt[m]{\epsilon_1},\ \sqrt[m]{\epsilon_2}):F(\zeta_m,\ \sqrt[m]{\epsilon_1})][F(\zeta_m,\ \sqrt[m]{\epsilon_1}):F(\zeta_m)]\\&=m[F(\zeta_m,\ \sqrt[m]{\epsilon_1},\ \sqrt[m]{\epsilon_2}):F(\zeta_m,\ \sqrt[m]{\epsilon_1})]\end{aligned}$$

by the lemma 3.

Suppose $[F_m:F(\zeta_m)]<m^2$; then $x^m-\epsilon_2$ is reducible over $F(\zeta_m,\ \sqrt[m]{\epsilon_1})$ by the above. Hence there is a prime $\ell|m$ such that $\sqrt[\ell]{\epsilon_2}\in F(\zeta_m,\ \sqrt[m]{\epsilon_1})$. Let us consider the sequence

$$F(\zeta_m)\subset F(\zeta_m,\sqrt[\ell]{\epsilon_1})\subset F(\zeta_m,\sqrt[\ell]{\epsilon_1},\sqrt[\ell]{\epsilon_2})\subset F(\zeta_m,\ \sqrt[m]{\epsilon_1}).$$

Since $[F(\zeta_m,\sqrt[\ell]{\epsilon_1}):F(\zeta_m)]=\ell$ holds by the lemma 3, we see that $[F(\zeta_m,\ \sqrt[m]{\epsilon_1}):F(\zeta_m,\sqrt[\ell]{\epsilon_1})]=m/\ell$ is relatively prime to ℓ. Since $F(\zeta_m,\sqrt[\ell]{\epsilon_1})\ni\zeta_\ell$ by $\ell|m$, $[F(\zeta_m,\sqrt[\ell]{\epsilon_1},\sqrt[\ell]{\epsilon_2}):F(\zeta_m,\sqrt[\ell]{\epsilon_1})]=1$ or ℓ holds, and then it yields $F(\zeta_m,\sqrt[\ell]{\epsilon_1})=F(\zeta_m,\sqrt[\ell]{\epsilon_1},\sqrt[\ell]{\epsilon_2})$ and so $\sqrt[\ell]{\epsilon_2}\in F(\zeta_m,\sqrt[\ell]{\epsilon_1})$. Then there is a natural number r such that $\sqrt[\ell]{\epsilon_1}/\sqrt[\ell]{\epsilon_2}^{\,r}\in F(\zeta_m)$. It is a contradiction, applying the lemma 3 for $\epsilon=\epsilon_1\epsilon_2^{-r}$. Thus we have proved $[F_m:F(\zeta_m)]=m^2$ and then the second equation follows easily from $F\cap\boldsymbol{Q}(\zeta_m)=\boldsymbol{Q}$. □

The isomorphism in the following lemma is a special case of the theorem 2.1 in [**K4**] or a refinement of the lemma 4.

Lemma 5. *Let q be an odd prime number. Then we have*

$$\mathrm{Gal}\Big(F\Big(\sqrt[q]{o_F^\times}\Big)/F(\zeta_q)\Big)\cong(\boldsymbol{Z}/q\boldsymbol{Z})^2,$$

$$\Big[F\Big(\zeta_q,\ \sqrt[q]{\epsilon_1\epsilon_2^b},\ \sqrt[q]{\epsilon_2}^{\,b^2-b+1}\Big):F\Big]=(q-1)q^{2-\alpha(b,q)}/[F\cap\boldsymbol{Q}(\zeta_q):\boldsymbol{Q}].$$

Proof. The second follows from the first and the definition of α. □

Lemma 6. *Let m be odd and square-free, and assume $F\not\subset\boldsymbol{Q}(\zeta_m)$. Then an abelian subfield K of F_m is contained in $F(\zeta_m)$.*

Proof. Let K be an abelian subfield of F_m and suppose $K \not\subset F(\zeta_m)$. Since $F_m = F(\zeta_m)(\sqrt[m]{\epsilon_1}, \sqrt[m]{\epsilon_2})$ is a Kummer extension of $F(\zeta_m)$, and $F_m \supset K \cdot F(\zeta_m) \supsetneq F(\zeta_m)$, there are integers a, b, m' such that $K \cdot F(\zeta_m) \ni \sqrt[m']{\epsilon_1^a \epsilon_2^b}$ with $(a,b) = 1$, $1 \neq m' | m$. Set $\epsilon = \epsilon_1^a \epsilon_2^b$ and take $\eta \in \mathrm{Gal}(F_m/\boldsymbol{Q})$ so that $\eta = \mathrm{id}$ on $F(\zeta_m)$ and $\sqrt[m']{\epsilon}^{\eta} = \zeta_{m'} \sqrt[m']{\epsilon}$, using the lemma 4. Let $\rho_0 \in \mathrm{Gal}(F(\zeta_{m'})/\boldsymbol{Q})$ such that $\rho_0 = \mathrm{id}$ on F and $\zeta_{m'}^{\rho_0} \neq \zeta_{m'}$. This is possible since m' is odd. We extend ρ_0 to an element of $\mathrm{Gal}(F(\zeta_m)/\boldsymbol{Q})$. By virtue of the lemma 4, we can extend ρ_0 to $\rho \in \mathrm{Gal}(F_m/\boldsymbol{Q})$ so that $\sqrt[m']{\epsilon}^{\rho} = \sqrt[m']{\epsilon}$ holds by multiplying an element of $\mathrm{Gal}(F_m/F(\zeta_m))$, if necessary. Then we have

$$\sqrt[m']{\epsilon}^{\eta\rho} = \left(\zeta_{m'} \sqrt[m']{\epsilon}\right)^{\rho} = \zeta_{m'}^{\rho_0} \sqrt[m']{\epsilon},$$
$$\sqrt[m']{\epsilon}^{\rho\eta} = \sqrt[m']{\epsilon}^{\eta} = \zeta_{m'} \sqrt[m']{\epsilon} \neq \zeta_{m'}^{\rho_0} \sqrt[m']{\epsilon}.$$

Hence $\sqrt[m']{\epsilon}$ is not abelian over $\boldsymbol{Q}$. However the assumption implies that $K \cdot F(\zeta_m)$ $(\ni \sqrt[m']{\epsilon})$ is abelian over $\boldsymbol{Q}$. This is a contradiction. □

Lemma 7. *Suppose that m, n are relatively prime square-free odd integers and suppose $F \not\subset \boldsymbol{Q}(\zeta_m)$ and $F \not\subset \boldsymbol{Q}(\zeta_n)$. Then $F_m \cap F_n = F(\zeta_m) \cap F(\zeta_n)$ holds and we have*

$$[F_m \cap F_n : F] = \begin{cases} 1 & \text{if } F \not\subset \boldsymbol{Q}(\zeta_{mn}), \\ 3 & \text{if } F \subset \boldsymbol{Q}(\zeta_{mn}). \end{cases}$$

Proof. Put $K = F_m \cap F_n$ $(\supset F(\zeta_m) \cap F(\zeta_n))$; then $K \subset F(\zeta_{mn})$ holds by the lemma 2, and hence K is abelian over $\boldsymbol{Q}$. Then the lemma 6 implies $K \subset F(\zeta_m) \cap F(\zeta_n)$ and hence $K = F(\zeta_m) \cap F(\zeta_n)$, and then the lemma 1 implies the desired equation. □

Lemma 8. $[F_2 : F] = 8$ *and the maximal abelian subfield of F_2 is $F(\sqrt{-1})$.*

Proof. $F_2 = F(\sqrt{-1}, \sqrt{\epsilon_1}, \sqrt{\epsilon_2})$ and $F_(\sqrt{-1}) \neq F$ are clear. If we have $F(\sqrt{-1}, \sqrt{\epsilon_1}) = F(\sqrt{-1})$, then $\sqrt{\epsilon_1} \in F(\sqrt{-1})$ and so $\sqrt{\epsilon_1}/\sqrt{-1} \in F$ hold. It implies a contradiction $\epsilon_1 = -a^2$ for an element $a \in F$. Therefore we have $F(\sqrt{-1}, \sqrt{\epsilon_1}) \neq F(\sqrt{-1})$. Next, suppose $F(\sqrt{-1}, \sqrt{\epsilon_1}, \sqrt{\epsilon_2}) = F(\sqrt{-1}, \sqrt{\epsilon_1})$; then $\sqrt{\epsilon_2} \in F(\sqrt{-1}, \sqrt{\epsilon_1})$ and so $\sqrt{\epsilon_2}/\sqrt{-1}, \sqrt{\epsilon_2}/\sqrt{\epsilon_1}$ or $\sqrt{\epsilon_2}/\sqrt{-\epsilon_1} \in F$ holds since quadratic subfields over F in $F(\sqrt{-1}, \sqrt{\epsilon_1})$ are $F(\sqrt{-1}), F(\sqrt{\epsilon_1})$ or $F(\sqrt{-\epsilon_1})$. They are contradictions similarly to the above. Thus we obtain $[F_2 : F] = 8$. The maximal abelian subfield K of F_2 contains $F(\sqrt{-1})$ clearly. Suppose $K \neq F(\sqrt{-1})$; then K must contain $F(\sqrt{-1})(\sqrt{\epsilon_1}), F(\sqrt{-1})(\sqrt{\epsilon_2})$ or $F(\sqrt{-1})(\sqrt{\epsilon_1\epsilon_2})$. Therefore one of the three fields is abelian. However they are conjugate by virtue of $\epsilon_1^{\sigma} = \epsilon_2, \epsilon_2^{\sigma} = (\epsilon_1\epsilon_2)^{-1}$, and so they coincide. This is a contradiction. □

Lemma 9. *For an odd square-free integer m, $F_2 \cap F_m = F$ holds.*

Proof. It is easy to see that $[F_2(\zeta_{4m}) : F(\zeta_{4m})] = [F(\zeta_{4m})(\sqrt{\epsilon_1}, \sqrt{\epsilon_2}) : F(\zeta_{4m})]$ divides 4, and $[F_m(\zeta_{4m}) : F(\zeta_{4m})] = [F(\zeta_{4m})(\sqrt[m]{\epsilon_1}, \sqrt[m]{\epsilon_2}) : F(\zeta_{4m})]$ is odd. Therefore we have $F(\zeta_{4m}) = F_2(\zeta_{4m}) \cap F_m(\zeta_{4m}) \supset F_2 \cap F_m$, and then $K := F_2 \cap F_m$ is an abelian subfield of F_2. By the previous lemma, K is equal to F or $F(\sqrt{-1})$. Suppose $K = F(\sqrt{-1})$. Since $[F_m : F] = [F_m : F(\zeta_m)][F(\zeta_m) : F]$ and $[F_m : F(\zeta_m)]$ is odd, we see that $\sqrt{-1}\,(\in K \subset F_m)$ is contained in $F(\zeta_m)$, i.e. $\sqrt{-1} \in F(\zeta_m)$.

On the other hand, d_F and m are odd and hence the discriminant of $F(\zeta_m)$ is odd. Thus the prime 2 is unramified, which contradicts $\sqrt{-1} \in F(\zeta_m)$. □

Under preparations above, let us evaluate the term

$$E_{II} = \sum_{\substack{m,n\geq 1\\ mn|A}} \varphi(m)\mu(n) \sum_{b \bmod n} 1/k(m,n;b).$$

Dividing terms according to parities of m, n, we have

$$\begin{aligned} E_{II} = &\sum_{mn|A/2} \varphi(m)\mu(n) \sum_{b \bmod n} 1/k(m,n;b) + \sum_{mn|A/2} \varphi(m)\mu(n) \sum_{b \bmod n} 1/k(2m,n;b) \\ &- \sum_{mn|A/2} \varphi(m)\mu(n) \sum_{b \bmod 2n} 1/k(m,2n;b), \end{aligned}$$

recalling A is even and square-free. By virtue of the lemma 9, we see, for $mn|A/2$

$$\begin{aligned} k(2m,n;b) &= \left[F\left(\zeta_{2m},\ \sqrt[2m]{\epsilon_1},\ \sqrt[2m]{\epsilon_2},\ \zeta_n,\ \sqrt[n]{\epsilon_1\epsilon_2^b},\ \sqrt[n]{\epsilon_2}^{b^2-b+1}\right) : F\right] \\ &= [F(\sqrt{\epsilon_1}, \sqrt{\epsilon_2}) : F]\left[F\left(\zeta_m,\ \sqrt[m]{\epsilon_1},\ \sqrt[m]{\epsilon_2},\ \zeta_n,\ \sqrt[n]{\epsilon_1\epsilon_2^b},\ \sqrt[n]{\epsilon_2}^{b^2-b+1}\right) : F\right] \\ &= 4k(m,n;b). \end{aligned}$$

Writing $b = 2b_1 + b_2 n$ ($n:$ odd), we have

$$\begin{aligned} k(m,2n;b) &= \left[F\left(\zeta_m,\ \sqrt[m]{\epsilon_1},\ \sqrt[m]{\epsilon_2},\ \zeta_n, \sqrt{\epsilon_1\epsilon_2^{b_2 n}},\ \sqrt[n]{\epsilon_1\epsilon_2^{2b_1}},\right.\right. \\ &\qquad\qquad \left.\left.\sqrt{\epsilon_2}^{(b_2n)^2-b_2n+1},\ \sqrt[n]{\epsilon_2}^{(2b_1)^2-2b_1+1}\right) : F\right] \\ &= \left[F\left(\sqrt{\epsilon_1\epsilon_2^{b_2n}}, \sqrt{\epsilon_2}^{(b_2n)^2-b_2n+1}\right) : F\right] k(m,n;2b_1) \\ &= 4k(m,n;2b_1), \end{aligned}$$

by virtue of $(b_2n)^2 - b_2n + 1 \equiv 1 \bmod 2$. Therefore E_{II} is equal to

$$\begin{aligned} &\sum_{mn|A/2} \varphi(m)\mu(n) \sum_{b \bmod n} 1/k(m,n;b) + \frac{1}{4} \sum_{mn|A/2} \varphi(m)\mu(n) \sum_{b \bmod n} 1/k(m,n;b) \\ &\quad - \sum_{mn|A/2} \varphi(m)\mu(n) \sum_{\substack{b_1 \bmod n\\ b_2 \bmod 2}} 1/(4k(m,n;2b_1)) \\ &= \frac{3}{4} \sum_{mn|A/2} \varphi(m)\mu(n) \sum_{b \bmod n} 1/k(m,n;b). \end{aligned}$$

Set, for an integer a,

$$V(a) = \sum_{mn|a} \varphi(m)\mu(n) \sum_{b \bmod n} 1/k(m,n;b).$$

Then $E_{II} = \frac{3}{4}V(A/2)$ has been shown above.

PROPOSITION 8. *Let q be a prime number such that $q = 3$ or $q \equiv 1 \bmod 3$. We have*

$$V(q) = \begin{cases} \dfrac{5}{6} & \text{if } q = 3, \\ 1 + \dfrac{1-2q}{q^2(q-1)} & \text{if } q \neq 3 \text{ and } F \not\subset \boldsymbol{Q}(\zeta_q), \\ 1 + \dfrac{3(1-2q)}{q^2(q-1)} & \text{if } F \subset \boldsymbol{Q}(\zeta_q). \end{cases}$$

PROOF. It is easy to see

$$V(q) = 1 + \varphi(q)/k(q,1;0) - \sum_{b \bmod q} 1/k(1,q;b),$$

noting $k(1,1;0) = 1$. The lemma 5 implies

$$k(q,1;0) = [F(\zeta_q, \sqrt[q]{\epsilon_1}, \sqrt[q]{\epsilon_2}) : F] = q^2[F(\zeta_q) : F]$$

and

$$\begin{aligned} k(1,q;b) &= \left[F\left(\zeta_q, \sqrt[q]{\epsilon_1\epsilon_2^b}, \sqrt[q]{\epsilon_2}^{b^2-b+1}\right) : F\right] \\ &= \begin{cases} [F(\zeta_q, \sqrt[q]{\epsilon_1\epsilon_2^b}) : F] & \text{if } b^2-b+1 \equiv 0 \bmod q, \\ [F(\zeta_q, \sqrt[q]{\epsilon_1}, \sqrt[q]{\epsilon_2}) : F] & \text{if } b^2-b+1 \not\equiv 0 \bmod q \end{cases} \\ &= \begin{cases} q[F(\zeta_q) : F] & \text{if } b^2-b+1 \equiv 0 \bmod q, \\ q^2[F(\zeta_q) : F] & \text{if } b^2-b+1 \not\equiv 0 \bmod q. \end{cases} \end{aligned}$$

Therefore we have

$$V(q) = 1 + \frac{\varphi(q)}{q^2[F(\zeta_q):F]} - \sum_{\substack{b \bmod q \\ b^2-b+1\equiv 0 \bmod q}} \frac{1}{q[F(\zeta_q):F]} - \sum_{\substack{b \bmod q \\ b^2-b+1\not\equiv 0 \bmod q}} \frac{1}{q^2[F(\zeta_q):F]}.$$

$V(3) = 5/6$ is easy. If $q \neq 3$, then we have

$$V(q) = 1 + \frac{1-2q}{q^2[F(\zeta_q):F]},$$

which gives the assertion. $V(q) \neq 0$ is easy to see. □

Suppose that $q = A/2$ is a prime number.
If $F \subset \boldsymbol{Q}(\zeta_9)$, then $E_{II} = \frac{3}{4}V(3) = \frac{15}{24}$ and then

$$\kappa = \frac{5}{24}E_I\,(\neq 0),$$

which completes the proof of the theorem 2 when $F \subset \boldsymbol{Q}(\zeta_9)$.
If $F \subset \boldsymbol{Q}(\zeta_q)$, then we have $E_{II} = \frac{3}{4}V(q) = \frac{3}{4}(1 + \frac{3(1-2q)}{q^2(q-1)})$ and so

$$\kappa = \frac{1}{4}\left(1 + \frac{3(1-2q)}{q^2(q-1)}\right)E_I\,(\neq 0),$$

which completes the proof of the theorem 2 when $F \subset \boldsymbol{Q}(\zeta_q)$. Thus we have completed the proof of the case where $A/2$ is prime.

Lemma 10. *Let m, n be odd natural numbers and q an odd prime number. Suppose that mnq is square-free, $F \not\subset \boldsymbol{Q}(\zeta_q)$ and $F \not\subset \boldsymbol{Q}(\zeta_{mn})$. Then we have*

$$k(mq, n; b) = q^2(q-1)k(m,n;b)\begin{cases} 1 & \text{if } F \not\subset \boldsymbol{Q}(\zeta_{mnq}), \\ 1/3 & \text{if } F \subset \boldsymbol{Q}(\zeta_{mnq}), \end{cases}$$

$$\sum_{b \bmod nq} 1/k(m, nq; b) = \frac{\alpha(q)}{q^2(q-1)} \sum_{b \bmod n} 1/k(m,n;b)\begin{cases} 1 & \text{if } F \not\subset \boldsymbol{Q}(\zeta_{mnq}), \\ 3 & \text{if } F \subset \boldsymbol{Q}(\zeta_{mnq}). \end{cases}$$

Proof. By definition, it is easy to see

$$\begin{aligned}
k(mq, n; b) &= \left[F\left(\sqrt[mq]{o_F^\times},\ \zeta_n,\ \sqrt[n]{\epsilon_1\epsilon_2^b},\ \sqrt[n]{\epsilon_2}^{\,b^2-b+1}\right) : F\right] \\
&= \left[F_q \cdot F\left(\sqrt[m]{o_F^\times},\ \zeta_n,\ \sqrt[n]{\epsilon_1\epsilon_2^b},\ \sqrt[n]{\epsilon_2}^{\,b^2-b+1}\right) : F\right] \\
&= \frac{[F_q : F]\left[F\left(\sqrt[m]{o_F^\times},\ \zeta_n,\ \sqrt[n]{\epsilon_1\epsilon_2^b},\ \sqrt[n]{\epsilon_2}^{\,b^2-b+1}\right) : F\right]}{\left[F_q \cap F\left(\sqrt[m]{o_F^\times},\ \zeta_n,\ \sqrt[n]{\epsilon_1\epsilon_2^b},\ \sqrt[n]{\epsilon_2}^{\,b^2-b+1}\right) : F\right]}.
\end{aligned}$$

We have $[F_q : F] = [F(\zeta_q, \sqrt[q]{\epsilon_1}, \sqrt[q]{\epsilon_2}) : F(\zeta_q)][F(\zeta_q) : F] = q^2(q-1)$ by the lemma 5 and $F \not\subset \boldsymbol{Q}(\zeta_q)$, and then the numerator is $q^2(q-1)k(m,n;b)$. By the lemma 7, we see

$$\begin{aligned}
F_q \cap F_{mn} = F(\zeta_q) \cap F(\zeta_{mn}) &\subset F_q \cap F\left(\sqrt[m]{o_F^\times},\ \zeta_n,\ \sqrt[n]{\epsilon_1\epsilon_2^b},\ \sqrt[n]{\epsilon_2}^{\,b^2-b+1}\right) \\
&\subset F_q \cap F_{mn}
\end{aligned}$$

and hence $F_q \cap F(\sqrt[m]{o_F^\times},\ \zeta_n,\ \sqrt[n]{\epsilon_1\epsilon_2^b},\ \sqrt[n]{\epsilon_2}^{b^2-b+1}) = F_q \cap F_{mn}$. Then the lemma 7 gives the first equation.

For the second, we set $\mathfrak{s} = \{\zeta_q,\ \sqrt[q]{\epsilon_1\epsilon_2^{b_2 n}},\ \sqrt[q]{\epsilon_2}^{(b_2 n)^2 - b_2 n+1}\}$ for simplicity, and then we have

$$\begin{aligned}
&k(m, nq; b_1 q + b_2 n)\\
&\quad = \left[F\left(\sqrt[m]{o_F^\times},\ \zeta_n,\ \sqrt[n]{\epsilon_1\epsilon_2^{b_1 q}},\ \sqrt[n]{\epsilon_2}^{(b_1 q)^2 - b_1 q + 1}, \mathfrak{s}\right) : F\right]\\
&\quad = k(m, n; b_1 q)[F(\mathfrak{s}) : F] \Big/ \left[F\left(\sqrt[m]{o_F^\times},\ \zeta_n,\ \sqrt[n]{\epsilon_1\epsilon_2^{b_1 q}},\ \sqrt[n]{\epsilon_2}^{(b_1 q)^2 - b_1 q+1}\right) \cap F(\mathfrak{s}) : F\right].
\end{aligned}$$

Here $[F(\mathfrak{s}) : F]$ is equal to $\varphi(q) q^{2-\alpha(b_2 n, q)}$ by the lemma 5 and

$$\begin{aligned}
F(\zeta_{mn}) \cap F(\zeta_q) &\subset F\left(\sqrt[m]{o_F^\times},\ \zeta_n,\ \sqrt[n]{\epsilon_1\epsilon_2^{b_1 q}},\ \sqrt[n]{\epsilon_2}^{(b_1 q)^2 - b_1 q + 1}\right) \cap F(\mathfrak{s})\\
&\subset F_{mn} \cap F_q = F(\zeta_{mn}) \cap F(\zeta_q)
\end{aligned}$$

by the lemma 7, and so the denominator is equal to $[F(\zeta_{mn}) \cap F(\zeta_q) : F]$ and then

$$k(m, nq; b_1 q + b_2 n) = k(m, n; b_1 q)(q-1) q^{2-\alpha(b_2 n, q)} \begin{cases} 1 & \text{if } F \not\subset \boldsymbol{Q}(\zeta_{mnq}), \\ 1/3 & \text{if } F \subset \boldsymbol{Q}(\zeta_{mnq}). \end{cases}$$

Thus we have

$$\begin{aligned}
&\sum_{b \bmod nq} 1/k(m, nq; b)\\
&\quad = \sum_{b_1 \bmod n} 1/k(m, n; b_1 q) \sum_{b_2 \bmod q} (q-1)^{-1} q^{-2+\alpha(b_2 n, q)} \begin{cases} 1 & \text{if } F \not\subset \boldsymbol{Q}(\zeta_{mnq}), \\ 3 & \text{if } F \subset \boldsymbol{Q}(\zeta_{mnq}) \end{cases}\\
&\quad = \alpha(q)(q-1)^{-1} q^{-2} \sum_{b \bmod n} 1/k(m, n; b) \begin{cases} 1 & \text{if } F \not\subset \boldsymbol{Q}(\zeta_{mnq}), \\ 3 & \text{if } F \subset \boldsymbol{Q}(\zeta_{mnq}), \end{cases}
\end{aligned}$$

where $\sum_{b \bmod q} q^{\alpha(b,q)}$ is $\alpha(q)$ by definition as before. □

Proposition 9. *Suppose that $r | A/2$ and $F \not\subset \boldsymbol{Q}(\zeta_r)$; then we have*

$$V(r) = \prod_{\ell | r} \left(1 + \ell^{-2} - \frac{\alpha(\ell)}{\ell^2(\ell - 1)}\right).$$

Proof. If r is a prime, then $r \not\equiv 2 \bmod 3$ holds and so the assertion follows from the proposition 8. Suppose $r = aq$, where q is a prime number and $a > 1$. It is easy to see

$$V(aq) = \sum_{mn|a} \varphi(m)\mu(n) \sum_{b \bmod n} 1/k(m,n;b) + \sum_{mn|a} \varphi(mq)\mu(n) \sum_{b \bmod n} 1/k(mq,n;b)$$
$$- \sum_{mn|a} \varphi(m)\mu(n) \sum_{b \bmod nq} 1/k(m,nq;b).$$

The first partial sum is equal to $V(a)$. The lemma 10 yields $k(mq,n;b) = q^2(q-1)k(m,n;b)$ by the assumption $F \not\subset \boldsymbol{Q}(\zeta_{aq})$ if $mn|a$. Therefore the second partial sum is equal to $q^{-2}V(a)$. Similarly, the third partial sum is equal to

$$\frac{\alpha(q)}{q^2(q-1)} V(a).$$

Therefore we have

$$V(aq) = \left(1 + q^{-2} - \frac{\alpha(q)}{q^2(q-1)}\right) V(a),$$

and inductively

$$V(r) = \prod_{\ell|r} \left(1 + \ell^{-2} - \frac{\alpha(\ell)}{\ell^2(\ell-1)}\right). \qquad \square$$

Now suppose $3|d_F$; then $F \not\subset \boldsymbol{Q}(\zeta_A)$ holds since the conductor of F is divisible by 9 and A is square-free. Thus in case of $3|d_F$ we have by the proposition 9

$$V(A/2) = \prod_{q|A/2} \left(1 + q^{-2} - \frac{\alpha(q)}{q^2(q-1)}\right) \neq 0,$$

which completes the proof in case of $3|d_F$.

Lastly, we assume $3 \nmid d_F$. It implies that any prime divisor of $A/2$ is congruent to 1 modulo 3. Put $A/2 = aq$, where $a > 1$ and q is prime. Similarly as above, we have

$$V(A/2) = V(a) + \sum_{mn|a} \varphi(mq)\mu(n) \sum_{b \bmod n} 1/k(mq,n;b)$$
$$- \sum_{mn|a} \varphi(m)\mu(n) \sum_{b \bmod nq} 1/k(m,nq;b).$$

Here we see, by the lemma 10

$$k(mq,n;b) = q^2(q-1)k(m,n;b) \begin{cases} 1 & \text{if } mn < a, \\ 1/3 & \text{if } mn = a. \end{cases}$$

Therefore the second partial sum is equal to

$$q^{-2}\sum_{\substack{mn|a\\ mn\neq a}}\varphi(m)\mu(n)\sum_{b \bmod n}1/k(m,n;b)+3q^{-2}\sum_{mn=a}\varphi(m)\mu(n)\sum_{b \bmod n}1/k(m,n;b)$$
$$=q^{-2}V(a)+2q^{-2}\sum_{mn=a}\varphi(m)\mu(n)\sum_{b \bmod n}1/k(m,n;b).$$

Similarly, the third sum is equal to

$$\sum_{\substack{mn|a\\ mn\neq a}}\varphi(m)\mu(n)\sum_{b \bmod n}1/k(m,n;b)\cdot\frac{\alpha(q)}{(q-1)q^2}$$
$$+\sum_{mn=a}\varphi(m)\mu(n)\sum_{b \bmod n}1/k(m,n;b)\cdot\frac{3\alpha(q)}{(q-1)q^2}$$
$$=\frac{\alpha(q)}{(q-1)q^2}V(a)+\frac{2\alpha(q)}{(q-1)q^2}\sum_{mn=a}\varphi(m)\mu(n)\sum_{b \bmod n}1/k(m,n;b).$$

Here we note $\alpha(q)=3q-2$ by virtue of $q\equiv 1 \bmod 3$. Thus we obtain

$$V(A/2)=\left(1+\frac{1-2q}{(q-1)q^2}\right)V(a)+\frac{2(1-2q)}{(q-1)q^2}\sum_{mn=a}\varphi(m)\mu(n)\sum_{b \bmod n}1/k(m,n;b).$$

By the proposition 9, $V(a)=\prod_{q|a}(1+q^{-2}-\frac{\alpha(q)}{(q-1)q^2})=\prod_{q|a}(1+\frac{1-2q}{(q-1)q^2})$ holds because of $F\not\subset \boldsymbol{Q}(\zeta_a)$. If $mn=a\,(<A/2)$, then the lemma 7 yields that F_m and F_n are linearly disjoint over F and then we have

$$k(m,n;b)=[F_m:F]\Big[F\Big(\zeta_n,\sqrt[n]{\epsilon_1\epsilon_2^b},\sqrt[n]{\epsilon_2}^{\,b^2-b+1}\Big):F\Big]$$
$$=[F_m:F]\prod_{\ell|n}\Big[F\Big(\zeta_\ell,\sqrt[\ell]{\epsilon_1\epsilon_2^b},\sqrt[\ell]{\epsilon_2}^{\,b^2-b+1}\Big):F\Big]$$
$$=[F_m:F]\prod_{\ell|n}(\ell-1)\ell^{2-\alpha(b,\ell)},$$

and then by the lemma 4

$$\sum_{b \bmod n}1/k(m,n;b)=\frac{1}{[F_m:F]}\sum_{b \bmod n}\left(\prod_{\ell|n}(\ell-1)\ell^{2-\alpha(b,\ell)}\right)^{-1}$$
$$=\frac{1}{\varphi(m)m^2}\cdot\frac{\prod_{\ell|n}\alpha(\ell)}{\varphi(n)n^2}.$$

Thus we have

$$V(A/2) = \prod_{\ell|A/2}\left(1+\frac{1-2\ell}{(\ell-1)\ell^2}\right)+\frac{2(1-2q)}{(q-1)q^2}\sum_{mn=a}\varphi(m)\mu(n)\frac{\prod_{\ell|n}\alpha(\ell)}{\varphi(m)m^2\varphi(n)n^2}$$

$$= \prod_{\ell|A/2}\left(1+\frac{1-2\ell}{(\ell-1)\ell^2}\right)+\frac{2(1-2q)}{(q-1)q^2a^2}\sum_{mn=a}\mu(n)\frac{\prod_{\ell|n}(3\ell-2)}{\varphi(n)}$$

$$= \prod_{\ell|A/2}\left(1+\frac{1-2\ell}{(\ell-1)\ell^2}\right)+\frac{2}{(A/2)^2}\prod_{\ell|A/2}\frac{1-2\ell}{\ell-1},$$

which gives the formula in the theorem in case of $3\nmid d_F$.

To see $V(A/2)>0$, we have only to show

$$1+\frac{1-2\ell}{(\ell-1)\ell^2}\geq\frac{2(2\ell-1)}{(\ell-1)\ell^2},$$

which is equivalent to $(\ell-1)\ell^2\geq 3(2\ell-1)$, which follows from $3(2\ell-1)=6(\ell-1)+3\leq 9(\ell-1)\leq \ell^2(\ell-1)$ by $\ell\equiv 1 \bmod 3$. Thus we have completed the positivity of the expected density and so the proof of the theorem 2.

Remark. Let p be an odd prime and F an abelian extension of $\boldsymbol{Q}$ with $[F:\boldsymbol{Q}]=p$ and Galois group $\langle\sigma\rangle$. Then the rank of $o_F^\times$ is $p-1$ and σ operates on $o_F{}_+^\times=\{\epsilon\in o_F^\times | N_{F/\boldsymbol{Q}}(\epsilon)=1\}$. Hence it is isomorphic to an ideal of $\boldsymbol{Q}(\zeta_p)$ [**CR**]. If the ideal is principal, there are units $\epsilon_1,\cdots,\epsilon_{p-1}$ such that $\epsilon_k^\sigma=\epsilon_{k+1}$ for $1\leq k\leq p-2$ and $\epsilon_{p-1}^\sigma=(\epsilon_1\ldots\epsilon_{p-2})^{-1}$ and they are basis of $o_F{}_+^\times$, and then our argument may be generalized to it.

References

[CKY] Y-M. J. Chen, Y. Kitaoka and J. Yu, Distribution of units of real quadratic number fields, Nagoya Math. J., **158** (2000), 167–184.

[CR] C. W. Curtis and I. Reiner, Representation theory of finite groups and associative algebras, Interscience, 1962.

[IK] M. Ishikawa and Y. Kitaoka, On the distribution of units modulo prime ideals in real quadratic fields, J. Reine Angew. Math., **494** (1998), 65–72.

[K1] Y. Kitaoka, Distribution of units of a cubic field with negative discriminant, J. Number Theory, **91** (2001), 318–355.

[K2] Y. Kitaoka, Distribution of units of an algebraic number field, In: Galois Theory and Modular Forms, Dev. Math., Kluwer Academic Publishers, 2003, 287–303.

[K3] Y. Kitaoka, Distribution of units of an algebraic number fields with only one fundamental unit, Proc. Japan Acad., **80A** (2004), 86–89.

[K4] Y. Kitaoka, Distribution of units of an algebraic number field II, submitted.

[L] H. W. Lenstra, Jr., On Artin's conjecture and Euclid' algorithm in global fields, Invent. Math., **42** (1977), 201–224.

[M] K. Masima, On the distribution of units in the residue class field of real quadratic fields and Artin's conjecture, RIMS Kokyuroku, **1026** (1998), 156–166.

[R] H. Roskam, A quadratic analogue of Artin's conjecture on primitive roots, J. Number Theory, **81** (2000), 93–109.

Yoshiyuki Kitaoka
Department of Mathematics
Meijo University
Tenpaku, Nagoya, 468-8502
Japan
E-mail: kitaoka@ccmfs.meijo-u.ac.jp