Distribution of Units of a Cubic Field with Negative Discriminant

Yoshiyuki Kitaoka

Department of Mathematics, Meijo University, Tenpaku, Nagoya, 468-8502, Japan

Communicated by P. Roquette

Received September 25, 2000

Let \( F \) be a cubic number field with negative discriminant. Taking into account the extension degree of the ray class field modulo a prime ideal, we study the residual index \( I(p) \) of residue classes represented by units in the multiplicative group of the residue field modulo a prime ideal \( p \). The possible minimal value \( \ell(p) \) is given, and we give the density of prime ideals \( p \) with \( I(p) = \ell(p) \) if the degree of \( p \) is one, and a conjecture if the degree is 2 or 3.

Let \( F \) be an algebraic number field. We want to know how units of \( F \) distribute. As an approach to this purpose, we try a method by Hooley to Artin's conjecture on primitive roots.

Let \( f_1, \ldots, f_g \) be natural numbers such that \( f_1 \leq f_2 \leq \cdots \leq f_g \) and \( \sum_{i=1}^g f_i = [F : \mathbb{Q}] \) and set \( T = (f_1, \ldots, f_g) \). For a prime ideal \( p \) of \( F \), we denote by \( p_1 \) a prime number lying below \( p \). When \( p \) is a product of prime ideals \( p_1, \ldots, p_g \) with relative degree \( f_i \) in \( F \), we say that \( p \) is of type \( T \). We consider only unramified prime ideals. For a natural number \( f \) (one of \( f_i \)'s) we set

\[
\begin{align*}
P_{T,f}(x) &:= \{ p \mid p \text{ is of type } T, \text{ the degree of } p \text{ is } f \text{ and } p \leq x \} \\
E(p) &:= \{ u \mod p \in (O_F/p)^\times \mid u \equiv \text{unit mod } p \}, \\
I(p) &:= [(O_F/p)^\times : \bar{E}(p)],
\end{align*}
\]

where \( p \) stands for prime ideals of \( F \). Under the assumption on the existence of a good function \( \ell_{T,f} \) which satisfies the condition

\[(A) \quad \ell_{T,f}(p) \mid I(p) \text{ for } p \in P_{T,f}(\infty),\]

1The author is grateful to Professor Yuji Kida, who provided the test version of UBASIC ver.9 which was helpful to make examples.
we can embody a problem explicitly. Set
\[ P_{T,f}(x, n) := \# \{ p \in P_{T,f}(x) \mid n \mid (I(p)/\ell_{T,f}(p)) \}, \]
\[ N_{T,f}(x) := \# \{ p \in P_{T,f}(x) \mid I(p) = \ell_{T,f}(p) \}. \]

Now the problem is to study an asymptotic behavior of these with the determination of \( \ell_{T,f}(p) \). We gave a conjecture in [IK] for real quadratic fields, and we have affirmative answers [M, CKY, R] under the generalized Riemann Hypothesis (GRH). This is merely one possible view point to study the distribution of units. Following [Ho], we state a strategy to tackle it. Set
\[ N_{T,f}(x, g) := \# \{ p \in P_{T,f}(x) \mid q_{h}(I(p)/\ell_{T,f}(p)) = 1 \} \text{ for } -g < q \leq g, \]
\[ M_{T,f}(x, g_1, g_2) := \# \{ p \in P_{T,f}(x) \mid q_{g_1}(I(p)/\ell_{T,f}(p)) = 1 \} \text{ for } g_1 < q \leq g_2, \]
where \( q \) stands for prime numbers. Then the following obvious inequalities for \( t < x \) are fundamental:
\[ \left| N_{T,f}(x, t) - M_{T,f}(x, t, \infty) \right| \leq N_{T,f}(x, \infty) = N_{T,f}(x) \leq N_{T,f}(x, t). \]

We want to take \( \xi \) so that \( N_{T,f}(x, \xi) \) and \( M_{T,f}(x, \xi, \infty) \) are a main term and an error term of \( N_{T,f}(x) \), respectively. The treatment of \( N_{T,f}(x, \xi) \) is as follows: Set \( Q(\xi) := \prod_{q < \xi} q \), where \( q \) stands for prime numbers. Then we have
\[ N_{T,f}(x, \xi) = \# \{ p \in P_{T,f}(x) \mid (I(p)/\ell_{T,f}(p), Q(\xi)) = 1 \} \]
\[ = \sum_{p \in P_{T,f}(x)} 1 = \sum_{p \in P_{T,f}(x)} \sum_{n \mid (I(p)/\ell_{T,f}(p), Q(\xi))} \mu(n) \]
\[ = \sum_{n \mid Q(\xi)} \mu(n) \sum_{p \in P_{T,f}(x)} \sum_{n \mid (I(p)/\ell_{T,f}(p), Q(\xi))} 1 = \sum_{n \mid Q(\xi)} \mu(n) P_{T,f}(x, n). \]

If, hence we can separate \( N_{T,f}(x) \) into \( N_{T,f}(x, \xi) \) and \( M_{T,f}(x, \xi, \infty) \), and give an asymptotic formula for \( P_{T,f}(x, n) \), we can get an asymptotic formula for \( N_{T,f}(x) \). As stated above, everything goes well under the GRH when \( F \) is a real quadratic field.

In this paper, we are concerned in a real cubic field \( F \) with negative discriminant. In Section 1, we give algebraic prerequisites and in Section 2 asymptotic formulas of \( N_{T,f}(x) \) for \( T = (1, 1, 1) \) or \( (1, 2) \), \( f = 1 \) with \( \ell_{T,f}(p) = 1 \) are given. In Section 3, we treat the case \( T = (1, 2) \), \( f = 2 \). Suppose that a prime number \( p \) is \( p_1, p_2 \) in \( F \) where the degree of prime ideal \( p_1 \) is \( i \). Then we can find that \( \ell_{T,f}(p_2) := \delta_f I(p_2) \) satisfies the condition (A),
where $\delta_F = 3$ if $F$ is pure cubic and $F(\sqrt[3]{e})$ for a fundamental unit $e$ of $F$ is a Galois extension over $\mathbb{Q}$, and $\delta_F = 1$ otherwise. We can give an expected positive main term but can not handle the error term even if we assume the GRH. By the class field theory, we find that the extension degree of the ray class field mod $p$ over $F$ is divisible by $\delta_F I(p)$. How can one construct the subfield which corresponds to it? In Section 4, we treat the case $T = (3), f = 3$, i.e., the remaining primes. We see $\ell_T, f(p) = \delta_F(p−1)/2$, but can not handle the error term in this case, either. The subextension in the ray class field mod $p$ corresponding to $(p−1)/2$ can be explained by the composite of $F$ and $\mathbb{Q}(\zeta_p + \zeta_p^{-1})$ where $\zeta_p$ is a primitive $p$th root of unity. How can one construct the additional extension of degree 3 when $\delta_F = 3$?

Notation. $\mathbb{Q}, \mathbb{R}$ denote the field of rational numbers and real numbers, respectively. $\mathbb{Q}^{ab}$ stands for the maximal abelian extension of $\mathbb{Q}$. Through this paper, $F$ is a real cubic field with negative discriminant $d$ and a unique fundamental unit $e(>1)$. $\tilde{d}$ is the discriminant of $\mathbb{Q}(\sqrt[d]{d})$. $F_0 := F(\sqrt[3]{d})$ is a Galois closure of $F$ over $\mathbb{Q}$. $e, e', e'' \in F_0$ are conjugates of $e$ over $\mathbb{Q}$. $O_F$ is the maximal order of $F$ and for a prime ideal $p$ of $F$, we set

$$E(p) := \{ u \mod p \in (O_F/p)^\times | u \equiv \text{unit mod } p \},$$

$$I(p) := [(O_F/p)^\times : E(p)].$$

For a natural number $m$, we set

$$K(m) := F_0(\zeta_{2m}, \sqrt[m]{e}, \sqrt[m]{e'}, \sqrt[m]{e''}) = F_0(\zeta_{2m}, \sqrt[m]{e/\sqrt[m]{e'}}, \sqrt[m]{e''}).$$

where $\zeta_n$ denotes a primitive $n$th root of unity. We set

$$\delta_F := \begin{cases} 3 & \text{if } F \text{ is pure cubic and } F_0(\sqrt[3]{e})/\mathbb{Q} \text{ is a Galois extension,} \\ 1 & \text{otherwise.} \end{cases}$$

For a Galois extension $E/K$ and a union of conjugacy classes $C$ of $Gal(E/K)$, we denote by $\pi_C(x, E/K)$ the number of prime ideals $p$ of $K$ such that $p$ is unramified in $E$ with $N_{K/\mathbb{Q}}(p) \leq x$ and the Frobenius automorphism $(E/K)_p \in C$ for a prime ideal $\mathfrak{p}$ of $E$ lying above $p$.

We will use these without reference in the text.

1. PREREQUISITE

In this section, we give lemmas which are necessary to more detailed discussions later.
LEMMA 1.1. Let $p$ be a prime number unramified in $F$. $p$ remains prime in $Q(\sqrt{d})$ if and only if $(p) = \mathfrak{p}_1\mathfrak{p}_2$ in $F$ where $\mathfrak{p}_i$ is a prime ideal of degree $i$.

Proof. Suppose that $(p) = \mathfrak{p}_1\mathfrak{p}_2$ in $F$ for prime ideals $\mathfrak{p}_i$ of degree $i$. We assume that $p$ decomposes in $Q(\sqrt{d})$. Then a prime ideal $\mathfrak{q}$ of $F\mathfrak{o}$ which lies above $\mathfrak{p}_1$ is of degree 1, since the closures of $F$ and $Q(\sqrt{d})$ in $(F\mathfrak{o})_{\mathfrak{q}}$ are isomorphic to $Q_{\mathfrak{q}}$. Since $F\mathfrak{o}/Q$ is a Galois extension, the degree of any prime ideal $\mathfrak{q}$ of $F\mathfrak{o}$ lying above $p$, in particular lying above $\mathfrak{p}_2$ has degree 1. It is a contradiction.

Conversely, suppose that $p$ remains prime in $Q(\sqrt{d})$. Let $\mathfrak{q}$ be any prime ideal of $F\mathfrak{o}$ lying above $p$. Since $\mathfrak{q} \cap Q(\sqrt{d}) = pO_{Q(\sqrt{d})}$ has degree 2, the degree of $\mathfrak{q}$ is even, and is equal to 2 or 6. If the degree is 6, then the whole Galois group coincides the decomposition group and hence is cyclic. It is a contradiction. Hence the degree of $\mathfrak{q}$ is 2. We may suppose that the decomposition group $Z$ of $\mathfrak{q}$ is generated by the complex conjugation $j$, taking a conjugate of $\mathfrak{q}$ if necessary. Then the field corresponding to $Z$ is $F$, and the number of prime ideals of $F$ lying above $p$. By identifying $Gal(F\mathfrak{o}/Q)$, $j$ with the symmetric group $S_2$ and a permutation $(1, 2)$, respectively, it is easy to see $\#(Z \setminus Gal(F\mathfrak{o}/Q)/Z) = 2$ and hence $p$ is a product of two prime ideals in $F$.

LEMMA 1.2. Let $m, n$ be natural numbers and set $L = F(\zeta_m)$. Then a polynomial $x^n - \epsilon$ is irreducible over $L$.

Proof. We have only to show that if $q$ is a prime divisor of $n$, then $\epsilon \notin L^q$ and that if 4 divides $n$, then $-4\epsilon \notin L^q$. Suppose that $\epsilon \in L^q$ for an odd prime number $q$; then there is an element $\alpha$ in $L$ such that $\epsilon = \alpha^q$. Since $L/F$ is abelian, $F(\alpha)/F$ is also abelian. Because $\epsilon$ is a fundamental unit of $F$, $\alpha \notin F$ and hence $F(\alpha) \neq F$. Any conjugate of $\alpha$ over $F$ is of the form $\alpha^q$ for some $q$th root $\eta$ of unity. Since $F(\alpha)/F$ is a non-trivial Galois extension, there is a primitive $q$th root $\zeta_q$ of unity such that $\zeta_q \in F(\alpha) \subset L$. Then there is an integer $a$ such that $\zeta_q^a \alpha (\in L)$ is real and hence we may suppose that $\alpha$ is real. By iterating the above, we obtain a contradiction $\zeta_q \in F(\alpha) \subset L$. Next, we suppose $\sqrt{\epsilon} \notin L$. Because of $F \cap Q(\zeta_m) = Q$, $Gal(L/F) = Gal(F(\zeta_m)/F) \cong Gal(Q(\zeta_m)/Q)$ holds. Since $F(\sqrt{\epsilon})$ is quadratic over $F$, there is a square-free integer $t$ such that $F(\sqrt{\epsilon}) = F \cdot Q(\sqrt{t}) = F(\sqrt{t})$. Hence we have $\sqrt{t} = b \sqrt{\epsilon}$ for some $b \in F$, and then

$$tO_F = (bO_F)^2.$$ (1)

It implies that if $p$ is a prime divisor of $t$, then $p$ ramifies in $F$, and so $(p) = p^3$ or $p^2p_1^2$ in $F$. This contradicts (1). Hence $t$ coincides $-1$ and
follows. If $\sqrt{-2} \not\in \mathbb{L}$. Hence we have $\sqrt{2} \not\in \mathbb{L}$. Last, suppose $-4e \in \mathbb{L}$ and take an element $\beta \in \mathbb{L}$ such that $-4e = \beta^4$. Since $L/F$ is abelian, $F(\beta)/F$ is also abelian. If $[F(\beta) : F] = 1$, then $\beta \in F \subset \mathbb{R}$ implies a contradiction $0 < \beta^4 = -4e < 0$. Suppose $[F(\beta) : F] = 2$; since $F \neq F(\sqrt{-4e}) \subset F(\beta)$, we have $F(\sqrt{-4e}) = F(\beta)$. Writing $\beta = u + v \sqrt{-4e}$ ($u, v \in F$), we have $\pm \sqrt{-4e} = \beta^2 = u^2 - 4ev^2 + 2uv \sqrt{-4e}$ and hence $u^2 - 4ev^2 = 0$. This means $e = (u/2v)^2 \in F^2$, which is a contradiction. Suppose $[F(\beta) : F] = 4$; since $F(\beta)/F$ is abelian, $F(\beta) \supset \sqrt{-1}$ follows. If $F(\sqrt{-4e}) = F(\sqrt{-1})$, then $\sqrt{-4e}/\sqrt{-1} \in F$ follows, which implies the contradiction $\sqrt{-e} \in F$. If $F(\sqrt{-4e}) \neq F(\sqrt{-1})$, then $F(\sqrt{-4e})$ and $F(\sqrt{-1})$ coincide and then $\sqrt{-4e}/\sqrt{-1} \in F(\sqrt{-4e})$ follows. Setting $\sqrt{-4e}/\sqrt{-1} = a + \sqrt{-4e} b$ ($a, b \in F$), we get $a^2 - 4eb^2 = 0$, which yields a contradiction that $e$ is a square in $F$.

**Lemma 1.3.** Let $n$ be a natural number and suppose that $\mathbb{Q}(\theta)/\mathbb{Q}$ is an abelian extension. Then we have $F(\sqrt[5]{e}) \cap \mathbb{Q}^{ab} = \mathbb{Q}$ and $F(\sqrt[5]{e}, \theta) \cap \mathbb{Q}^{ab} = \mathbb{Q}(\theta)$.

**Proof.** Let $m$ be a natural number. By Lemma 1.2, we have

$$[F(\sqrt[5]{e}) : F(\sqrt[5]{e}) \cap \mathbb{Q}(\zeta_m)] = [F(\sqrt[5]{e}, \zeta_m) : \mathbb{Q}(\zeta_m)]$$

$$= [F(\sqrt[5]{e}, \zeta_m) : F(\zeta_m)][F(\zeta_m) : \mathbb{Q}(\zeta_m)]$$

$$= n[F : F \cap \mathbb{Q}(\zeta_m)] = 3n.$$  

On the other hand, $[F(\sqrt[5]{e}) : \mathbb{Q}] = [F(\sqrt[5]{e}) : F][F : \mathbb{Q}] = 3n$ follows also from Lemma 1.2. Thus we have $F(\sqrt[5]{e}) \cap \mathbb{Q}(\zeta_m) = \mathbb{Q}$ for any natural number $m$, and hence $F(\sqrt[5]{e}) \cap \mathbb{Q}^{ab} = \mathbb{Q}$. By Lemma 1.2, $x^n - e$ is irreducible over $F(\theta)$, and then we have

$$[F(\theta, \sqrt[5]{e}) : \mathbb{Q}] = [F(\theta, \sqrt[5]{e}) : F(\theta)][F(\theta) : \mathbb{Q}(\theta)][\mathbb{Q}(\theta) : \mathbb{Q}]$$

$$= 3n[\mathbb{Q}(\theta) : \mathbb{Q}].$$  

On the other hand, denoting the maximal abelian subfield of $F(\theta, \sqrt[5]{e})$ by $K$, we have $F(\sqrt[5]{e}) \cap K = \mathbb{Q}$ as above and since $F(\theta, \sqrt[5]{e})$ is a composite of $F(\sqrt[5]{e})$ and $K$, we have $[F(\theta, \sqrt[5]{e}) : \mathbb{Q}] = [F(\sqrt[5]{e}) : \mathbb{Q}][K : \mathbb{Q}] = 3n[K : \mathbb{Q}]$, which yields $[K : \mathbb{Q}] = [\mathbb{Q}(\theta) : \mathbb{Q}]$ and hence $K = \mathbb{Q}(\theta)$.  

The following is due to [H].

**Lemma 1.4.** We have

$$\langle\text{roots of unity in } F_0, e, e', e''\rangle = 1 \quad \text{or} \quad 3.$$

**Proof.** Let $\sigma \in \text{Gal}(F_0/\mathbb{Q})$ be of order 3 such that $e' = \sigma(e), e'' = \sigma^2(e)$. For fundamental units $\eta_1, \eta_2$ of $F_0$, there are integers $a_1, a_2, b_1, b_2$ so that

$$e = \delta_1 \eta_1^{a_1} \eta_2^{b_1}, \quad e' = \delta_2 \eta_1^{a_2} \eta_2^{b_2},$$

where $\delta_1, \delta_2$ are roots of unity in $F_0$. We have only to $|a_1b_2 - a_2b_1| = 1$ or 3. Because of

$$\begin{pmatrix} \log |e|^2 & \log |e'|^2 \\ \log |e'|^2 & \log |e''|^2 \end{pmatrix} = \begin{pmatrix} a_1 & a_2 \\ b_1 & b_2 \end{pmatrix} \begin{pmatrix} \log |\eta_1|^2 & \log |\sigma(\eta_1)|^2 \\ \log |\eta_2|^2 & \log |\sigma(\eta_2)|^2 \end{pmatrix},$$

we have

$$\log |e|^2 \log |e'|^2 - \log |e'|^2 \log |e''|^2 = (a_1b_2 - a_2b_1)(\log |\eta_1|^2 \log |\sigma(\eta_1)|^2 - \log |\eta_2|^2 \log |\sigma(\eta_2)|^2).$$

The left-hand side is equal to $-3(\log e)^2$ by $e | e'|^2 = 1$. For $\eta \in O_{F_0}^*, |\eta|^2$ is a real positive unit of $F_0$ and hence is in $F$. Therefore we have $|\eta|^2 = e^n$ for some integer $n$. Thus $\log |\eta_1|^2 \log |\sigma(\eta_1)|^2 - \log |\eta_2|^2 \log |\sigma(\eta_2)|^2$ is equal to $m(\log e)^2$ for some integer $m$. Finally we have obtained $-3 = (a_1b_2 - a_2b_1)m$, which yields our assertion. \[\]

**Lemma 1.5.** Let $n$ be a natural number. Then we have:

(i) If $p \mid n$ and $p \neq 3$ for a prime number $p$, then $\sqrt[3]{e} \notin F_0(\zeta_{2n}, \sqrt[3]{e}).$

(ii) If $4 \mid n$, then $\sqrt[4]{-4e} \notin F_0(\zeta_{2n}, \sqrt[4]{e}).$

(iii) If $9 \mid n$, then $\sqrt[9]{e} \notin F_0(\zeta_{2n}, \sqrt[9]{e}).$

**Proof.** Suppose that for a prime number $p(\neq 3)$ with $p \mid n$, $\sqrt[p]{e} \in F_0(\zeta_{2n}, \sqrt[p]{e})$ holds. By Lemma 1.2, $F_0(\zeta_{2n}, \sqrt[p]{e})$ and $F_0(\zeta_{2n}, \sqrt[3]{e})$ are cyclic extensions of $F_0(\zeta_{2n})$ of degree $p$ in $F_0(\zeta_{2n}, \sqrt[3]{e})$ which is also cyclic over $F_0(\zeta_{2n})$. Hence $F_0(\zeta_{2n}, \sqrt[3]{e})$ and $F_0(\zeta_{2n}, \sqrt[9]{e})$ coincide. Thus we have $w := \sqrt[3]{e}/\sqrt[9]{e} \in F_0(\zeta_{2n})$ for some integer $a$. Suppose $w \in F_0$; then $w^p = e' e^{2\pi i/3}$ holds and Lemma 1.4 yields $w = \delta e' e^{c}$ for a root $\delta$ of unity in $F_0$ and integers $b, c$. Therefore we have $\delta e' e^{c} = e' e^{-a}$ and hence from the
multiplicative independence of \( e, e' \) follows a contradiction \( pc = 1 \). Hence we have \( w \notin F_0 \) and therefore \( x^p - e^x \) is irreducible over \( F_0 \) since \( p \) is a prime number. Thus we have \( \{ F_0(w) : F_0 \} = p \), and from \( F_0(\zeta_{2n}) \supset F_0(w) \supset F_0 \) follows that \( F_0(w)/F_0 \) is an abelian extension of degree \( p \). Hence \( F_0(w) \) contains a conjugate \( \zeta_{2n} \) of \( w \) over \( F_0 \) and \( \zeta_{2n} \), too, and then

\[
p = [F_0(w) : F_0] = [F_0(\zeta_{2n}) : F_0(\zeta_{2n})][F_0(\zeta_{2n}) : F_0] \]

implies \( [F_0(\zeta_{2n}) : F_0] = 1 \), which implies \( \zeta_{2n} \in F_0 \) and so \( p = 2 \) and we conclude \( \sqrt{e}/\sqrt{e} \in F_0(\zeta_{2n}) \). Since \( F_0(\zeta_{2n})/\mathbb{Q} \) is a Galois extension and \( e^{-1}/e^2 = e^2/e' \) is a conjugate of \( e'/e \), \( \sqrt{e} \in F_0(\zeta_{2n}) \) holds. It contradicts Lemma 1.2. Thus we have shown (i).

Next suppose \( 4|n \) and \( \sqrt{-4e} \in F_0(\zeta_{2n}, \sqrt{e}) \); then \( -4e' \in F_0(\zeta_{2n}, \sqrt{e}) \) and \( \sqrt{e} \in F_0(\zeta_{2n}, \sqrt{e}) \) hold. It contradicts (i) for \( p = 2 \).

Last suppose \( 9|n \) and \( \sqrt{3} \in F_0(\zeta_{2n}, \sqrt{e}) \). By Lemma 1.2, \( F_0(\zeta_{2n}, \sqrt{e}) \), \( F_0(\zeta_{2n}, \sqrt{e}) \) and \( F_0(\zeta_{2n}, \sqrt{e}) \) are cyclic extensions of degree \( 9, 9, 9 \) over \( F_0(\zeta_{2n}) \), respectively. Hence we get \( F_0(\zeta_{2n}, \sqrt{e}) \) and there exists an integer \( a \) such that \( \sqrt{e}/\sqrt{e} \in F_0(\zeta_{2n}) \). If \( a \equiv 1 \mod 3 \), then \( \sqrt{e}/\sqrt{e} = 1/\sqrt{e} \in F_0(\zeta_{2n}) \) follows. It contradicts Lemma 1.2. Thus we may assume \( a = 1, 4 \) or \( 7 \). Suppose \( a = 1 \); then \( \sqrt{e}/\sqrt{e} \) and the complex conjugation \( \sqrt{e}/\sqrt{e} \) are in \( F_0(\zeta_{2n}) \) and then \( F_0(\zeta_{2n}) \) and \( \sqrt{e}/\sqrt{e} \) hold. \( \sqrt{e}/\sqrt{e} = 1/\sqrt{e} \), which contradicts Lemma 1.2. Suppose \( a = 4 \). Since \( e/e^4 \) and hence \( e/e^4 \) is a conjugate of \( e'/e' \), we have \( \sqrt{e}/e^4 \in F_0(\zeta_{2n}) \) and then \( \sqrt{e}/e^4 \in \sqrt{e}/e^4 \in F_0(\zeta_{2n}), \) which is a contradiction, too. The assumption \( a = 7 \) implies \( \sqrt{e}/e = e/\sqrt{e} = e/\sqrt{e} = e/\sqrt{e} \in F_0(\zeta_{2n}) \), which is a contradiction.

**Lemma 1.6.** If \( F \) is pure cubic and \( x^3 - e \) is irreducible over \( F_0(\sqrt{e}) \), then \( K(3) \cap \mathbb{Q}^{ab} = \mathbb{Q}(\Omega) \) holds for \( \Omega := (1 + ee' + e) \sqrt{e}/e \) and \( [\mathbb{Q}(\Omega) : \mathbb{Q}] = 6, \mathbb{Q}(\Omega) \geq \mathbb{Q}(3) \).

**Proof.** Take \( \rho \in \text{Gal}(K(3)/\mathbb{Q}) \) so that \( \rho(e) = e' \) and \( \rho^2(e) = e' \). Since \( F \) is pure cubic, \( \mathbb{Q}(\sqrt{e}) = \mathbb{Q}(\zeta_3) \) holds and \( \rho(\zeta_3) = \zeta_3 \) is valid, since the order of \( \rho_{ab} \zeta_3 \) is 3. The assumption implies \( \text{Gal}(K(3)/F_0) \cong (\mathbb{Z}/3\mathbb{Z})^2 \). We define \( \kappa_{a,b} \in \text{Gal}(K(3)/F_0) \) by \( \kappa_{a,b}(\sqrt{e}) = \zeta_3 \sqrt{e} \), \( \kappa_{a,b}(\rho(\sqrt{e})) = \zeta_2 \rho(\sqrt{e}) \), then \( \text{Gal}(K(3)/\mathbb{Q}) \) is generated by \( \kappa_{a,b}, \rho, j \), where \( j \) means the complex conjugation. We assume \( \sqrt{e} \) is a real number and normalize \( \rho \) so that \( \sqrt{e} \rho(\sqrt{e}) \rho^2(\sqrt{e}) = 1 \). It can be done as follows: Suppose \( \sqrt{e} \rho(\sqrt{e}) \rho^2(\sqrt{e}) = \zeta_3 \) and set \( \rho' = \kappa_{a,0} \rho \); then

\[
\rho'(\sqrt{e}) = \rho(\sqrt{e})
\]
\[ \rho^2(\sqrt[3]{e}) = \kappa_{a,0}(\rho^2(\sqrt[3]{e})) = \kappa_{a,0}(\zeta_3 \sqrt[3]{e}^{-1} \rho(\sqrt[3]{e})^{-1}) = \zeta_3^a \rho^2(\sqrt[3]{e}). \]

Hence we have
\[ \frac{\sqrt[3]{e}}{} \rho^2(\sqrt[3]{e}) \rho^{-1}(\sqrt[3]{e}) = \frac{\sqrt[3]{e}}{} \rho(\sqrt[3]{e}) \zeta_3^a \rho^2(\sqrt[3]{e}) = 1. \]

Now we redefine \( \kappa_{a,b} \) subject to the new \( \rho \). Then we have
\[ \frac{\sqrt[3]{e}}{} \rho(\sqrt[3]{e}) \rho^2(\sqrt[3]{e}) = 1, \quad \frac{\sqrt[3]{e}}{} \rho(\sqrt[3]{e}) \rho(\sqrt[3]{e}) = 1, \]
where the second follows from the fact the left-hand side is a real positive third root of unity. Now we show
\[ \kappa_{a,b}^{-1} \rho^{-1} \kappa_{a,b} \rho = \kappa_{b,a}, \quad \kappa_{a,b}^{-1} \kappa_{a,b} j = \kappa_{a,b}, \quad \rho^{-1} j \rho = \rho. \]

\[ \kappa_{a,b} \rho(\sqrt[3]{e}) = \zeta_3^b \rho(\sqrt[3]{e}) = \rho \kappa_{b,a}(\sqrt[3]{e}) \]
is obvious. Then
\[ \kappa_{a,b} \rho(\sqrt[3]{e}) = \kappa_{a,b}(\sqrt[3]{e}^{-1} \rho(\sqrt[3]{e})^{-1}) \]
\[ = \zeta_3^{-a-b} \sqrt[3]{e}^{-1} \rho(\sqrt[3]{e})^{-1} = \zeta_3^{-a-b} \rho^2(\sqrt[3]{e}) \]
and
\[ \rho \kappa_{b,a}(\sqrt[3]{e}) = \zeta_3^{2b-a} \rho^2(\sqrt[3]{e}) = \zeta_3^{-a-b} \rho^2(\sqrt[3]{e}) \]
imply \( \kappa_{a,b} \rho = \rho \kappa_{b,a} \), which means the first equation. Next we have
\[ \kappa_{a,b}^{-1} j \kappa_{a,b} j(\sqrt[3]{e}) = \kappa_{a,b}(\zeta_3^a \sqrt[3]{e}) = \zeta_3^a \kappa_{a,b}(\sqrt[3]{e}) = \zeta_3^a \sqrt[3]{e} = \kappa_{a,b}(\sqrt[3]{e}), \]
and
\[ \kappa_{a,b}^{-1} j \kappa_{a,b} j(\rho(\sqrt[3]{e})) = \kappa_{a,b}^{-1} j \kappa_{a,b}(\sqrt[3]{e}^{-1} \rho(\sqrt[3]{e})^{-1}) = \kappa_{a,b}(j \zeta_3^{-a-b} \sqrt[3]{e}^{-1} \rho(\sqrt[3]{e})^{-1}) \]
\[ = \zeta_3^{a+b} \kappa_{a,b}(j \sqrt[3]{e}^{-1} \rho(\sqrt[3]{e})^{-1}) = \zeta_3^{a+b} \kappa_{a,b}(\rho(\sqrt[3]{e})) \]
\[ = \zeta_3^a \rho(\sqrt[3]{e}) = \kappa_{a,b}(\rho(\sqrt[3]{e})). \]

Hence the second equation holds. Last we see
\[ \rho^{-1} j \rho(\sqrt[3]{e}) = \rho^{-1} \rho(\sqrt[3]{e}) = \rho^{-1} \rho(\sqrt[3]{e}) = \rho^{-1} \rho(\sqrt[3]{e}) = \rho(\sqrt[3]{e}) \]
and
\[ \rho^{-1} j \rho(\sqrt[3]{e}) = \rho^{-1} j \rho(\sqrt[3]{e}) \rho(\sqrt[3]{e})^{-1} \]
\[ = \rho^{-1} j \rho(\sqrt[3]{e}) \rho^2(\sqrt[3]{e})^{-1} = \rho^{-1} j \rho(\sqrt[3]{e}) \rho^2(\sqrt[3]{e}). \]
Here \( r^3 = id. \) follows from
\[
\rho^3(\sqrt[3]{\epsilon}) = \rho(\sqrt[3]{\epsilon}) \rho(\sqrt[3]{\epsilon})^{-1} = (\rho(\sqrt[3]{\epsilon}) \rho^2(\sqrt[3]{\epsilon}))^{-1} = \sqrt[3]{\epsilon}
\]
and then \( \rho^3(\rho^2(\sqrt[3]{\epsilon})) = \rho(\sqrt[3]{\epsilon}). \) Hence the commutator group \( [G, G] \) for the Galois group \( G = \text{Gal}(K(3)/Q) \) is generated by \( \kappa_{a,b} \) \((a = \pm 1), \rho. \) Since \( \kappa_{a,b} \) and \( \rho \) is commutative, we have \#\([G, G]\) = 3\(^2\), and hence the degree of the maximal abelian subfield of \( K(3) \) is 6. We take \( \rho(\sqrt[3]{\epsilon})/\sqrt[3]{\epsilon} \) as a third root of \( \epsilon' \). The assertion of the lemma does not depend on this choice. If \( \Omega = 0, \) then \( 1 + \varepsilon \rho^3(\epsilon) + \varepsilon = 0 \) and hence \( \rho^3(\epsilon) = -\varepsilon/(1 + \epsilon) \) holds. But it is a contradiction since \( \rho^3(\epsilon) \) is not real. Next let us see that \([G, G]\) fixes \( \Omega \).

\[
\rho(\Omega) = (1 + \rho(\varepsilon) \varepsilon + \rho(\varepsilon)) \rho^2(\sqrt[3]{\epsilon}) / \rho(\sqrt[3]{\epsilon})
= (1 + \rho(\varepsilon) \varepsilon + \rho(\varepsilon)) \rho(\varepsilon)^{-1} \rho(\sqrt[3]{\epsilon}) / \sqrt[3]{\epsilon}
= (\varepsilon \rho^3(\epsilon) + \varepsilon + 1) \rho(\sqrt[3]{\epsilon}) / \sqrt[3]{\epsilon} = \Omega.
\]
\
\( \kappa_{a,b}(\Omega) = \Omega \) is obvious. Hence we have \( Q(\Omega) \subset K(3) \cap Q^{ab}, \) and hence \( Q(\Omega)/Q \) is abelian. On the other hand, \( \kappa_{a,b}(\Omega) = \zeta_3 \Omega \) implies \( [Q(\Omega) : Q] \) \( \geq 3. \) Since \( Q(\Omega)/Q \) is abelian, we have \( Q(\Omega) \ni \kappa_{a,b}(\Omega) = \zeta_3 \Omega \) and hence \( Q(\Omega) \ni \zeta_3, \) which yields that \([Q(\Omega) : Q] \) is even and hence \([Q(\Omega) : Q] \geq 6. \) By virtue of \([K(3) \cap Q^{ab}] : Q\) = 6, we have \([Q(\Omega) : Q] \) = 6.

**Remark.** \( \Omega \) is a root of
\[
x^6 - (9 + 6a + 6b + ab) x^3 + (3 + a + b)^2 = 0,
\]
where \( a := \text{tr}_{F_0/Q} \zeta, b := \text{tr}_{F_0/Q} \zeta^{-1}. \)

**Lemma 1.7.** The following three assertions are equivalent.

(i) \( x^3 - \epsilon' \) is reducible over \( F_0(\sqrt[3]{\epsilon}). \)

(ii) \( x^3 - \epsilon' \) is reducible over \( F_0(\zeta_3, \sqrt[3]{\epsilon}). \)

(iii) \( x^3 - \epsilon'/\epsilon \) is reducible over \( F_0. \)

**Proof.** The assertion (ii) follows obviously from (i). Let us show (ii) \( \Rightarrow \) (iii). Suppose (ii); then Lemma 1.2 yields that \( F_0(\zeta_3, \sqrt[3]{\epsilon}) \subset F_0(\zeta_3, \sqrt[3]{\epsilon}) \) are extensions of degree 3 over \( F_0(\zeta_3) \) and hence they coincide. Take an integer \( a \) \((= \pm 1)\) so that \( \sqrt[3]{\epsilon'} = \sqrt[3]{\epsilon'} f, f \in F_0(\zeta_3) \). If \( a = -1, \) then \( f = \sqrt[3]{\epsilon'} \sqrt[3]{\epsilon'} = \sqrt[3]{\epsilon'}^{-1} \) implies \( \sqrt[3]{\epsilon'} \in F_0(\zeta_3), \) which is a contradiction. Hence we have \( a = 1 \) and \( f^3 = \epsilon'/\epsilon. \) If \( \zeta_3 \in F_0, \) then \( f \) is clearly in \( F_0. \) If \( \zeta_3 \notin F_0, \) we
write \( f = f_1 + \sqrt{-3} f_2 \) with \( f_1 \in F_0 \). Since \( f^3 = f_1^3 - 9 f_1 f_2^2 + 3 \sqrt{-3} (f_1^2 f_2 - f_2^2) \in F_0 \), we have \( f_1^2 f_2 - f_2^2 = 0 \), i.e., \( f_1 = \pm f_2 \) or \( f_2 = 0 \). If \( f_2 = 0 \), then \( f = f_1 \in F_0 \) holds. If \( f_2 = \delta f_1 \) (\( \delta = \pm 1 \)), then \( f = (1 + \delta \sqrt{-3}) f_1 \) holds and \( (1 + \delta \sqrt{-3})^3 = -8 \) implies, then \( e'/e = f^3 = (2f_1)^3 \). The assertion (iii) implies easily (i).

\[\text{Lemma 1.8.}\] Let \( n \) be a natural number divisible by 3. Then the following three assertions are equivalent.

(i) \( x^3 - e' \) is reducible over \( F_0(\zeta_{2n}, \sqrt[6]{3}) \).

(ii) Either (ii.1) \( x^3 - e' \) is reducible over \( F_0(\sqrt[6]{3}) \) or (ii.2) \( F \) is pure cubic, \( x^3 - e' \) is irreducible over \( F_0(\sqrt[6]{3}) \) and

\[\Omega := (1 + e'e'' + e) \sqrt[6]{3} \in \mathbb{Q}(\zeta_{2n}).\]

(iii) \( x^3 - e' \) is reducible over \( F_0(\zeta_{2n}, \sqrt[6]{3}) \).

\[\text{Proof.}\] (ii) \(\Rightarrow\) (iii) and (iii) \(\Rightarrow\) (i) are clear. We show (i) \(\Rightarrow\) (ii). Suppose (i); then \( F_0(\zeta_{2n}, \sqrt[6]{3}) \) and \( F_0(\zeta_{2n}, \sqrt[6]{3}) \) are subfields of degree 3 of a cyclic extension \( F_0(\zeta_{2n}, \sqrt[6]{3})/F_0(\zeta_{2n}) \) and hence they coincide. As in the proof of Lemma 1.7, we have

\[\sqrt[6]{3} \in F_0(\zeta_{2n}).\]

Suppose that \( x^3 - e' \) is irreducible over \( F_0(\sqrt[6]{3}) \). Setting \( w := \sqrt[6]{3}/e \), we have \( \sqrt{w} \in F_0(\zeta_{2n}) \) by the above. Since \( F_0(\zeta_{2n})/F_0 \) is abelian, \( F_0(\sqrt{w})/F_0 \) is also abelian and \([F_0(\sqrt{w}) : F_0] = 3\) by Lemma 1.7. Hence \( \zeta_3 \in F_0(\sqrt{w}) \) holds, and then we have

\[3 = [F_0(\sqrt{w}) : F_0] = [F_0(\sqrt{w}) : F_0(\zeta_3)][F_0(\zeta_3) : F_0],\]

which implies \([F_0(\zeta_3) : F_0] = 1\), i.e., \( \zeta_3 \in F_0 \), which implies \( \mathbb{Q}(\sqrt{d}) = \mathbb{Q}(\zeta_3) \). From it follows that \( F \) is pure cubic. \( \sqrt{w} \in F_0(\zeta_{2n}) \) implies \( \Omega \in F_0(\zeta_{2n}) \).

Since \( \mathbb{Q}(\Omega) \in \mathbb{Q}^{ab} \) by Lemma 1.6, we have \( \mathbb{Q}(\Omega) \in F_0(\zeta_{2n}) \cap \mathbb{Q}^{ab} = \mathbb{Q}(\sqrt{d}, \zeta_{2n}) = \mathbb{Q}(\zeta_{2n}). \) Thus we have (ii.2).

\[\text{Lemma 1.9.}\] For a natural number \( m \), \([K(m) : F_0(\zeta_{2m})] = m^2/3\) if \( 3 \mid m \) and \( x^3 - e' \) is reducible over \( F_0(\zeta_{2m}, \sqrt[6]{3}) \), and to \( m^2 \), otherwise.
Proof. First, we recall that $x^m - e'$ is irreducible over $F_0(\zeta_{2m}, \sqrt[m]{e})$ if and only if $e'$ is not a $p$th power element in $F_0(\zeta_{2m}, \sqrt[m]{e})$ for any prime divisor $p$ of $m$ and $-4e'$ is not a fourth power element if $4|m$. By Lemma 1.5, $x^m - e'$ is reducible over $F_0(\zeta_{2m}, \sqrt[m]{e})$ if and only if (i) $3|m$ and $\sqrt[3]{d} \in F_0(\zeta_{2m}, \sqrt[m]{e})$, or (ii) $4|m$ and $\sqrt[4]{-4e'} \in F_0(\zeta_{2m}, \sqrt[m]{e})$. Part (ii) contradicts (ii) in Lemma 1.5. Hence $x^m - e'$ is reducible over $F_0(\zeta_{2m}, \sqrt[m]{e})$ if and only if $3|m$ and $\sqrt[3]{d} \in F_0(\zeta_{2m}, \sqrt[m]{e})$ and then (iii) in Lemma 1.5 implies that $x^3 - \sqrt[3]{d}e'$ is irreducible over $F_0(\zeta_{2m}, \sqrt[m]{e})$, which completes the proof with Lemma 1.2.

Lemma 1.10. For a natural number $m$, we set

$$\delta_1(m) := \begin{cases} 1 & \text{if } 3|m \text{ and } x^3 - e' \text{ is reducible over } F_0(\zeta_{2m}, \sqrt[m]{e}), \\ 3 & \text{otherwise,} \end{cases}$$

$$\delta_2(m) := \begin{cases} 1 & \text{if } \sqrt[3]{d} \in \mathbb{Q}(\zeta_{2m}), \\ 2 & \text{otherwise.} \end{cases}$$

Then we have

$$[K(m) : \mathbb{Q}] = m^2 \varphi(2m) \delta_1(m) \delta_2(m),$$

where $\varphi$ is Euler's function. If $m, n$ are relatively prime natural numbers, then we have

$$[K(m) \cap K(n) : F_0] = \frac{[K(m) : \mathbb{Q}][K(n) : \mathbb{Q}]}{6[K(mn) : \mathbb{Q}]} = \frac{\delta_1(m) \delta_1(n) \delta_2(m) \delta_2(n)}{6\delta_1(mn) \delta_2(mn)}.$$

Proof. It is easy to see

$$[K(m) : \mathbb{Q}] = [K(m) : F_0(\zeta_{2m})][F_0(\zeta_{2m}) : \mathbb{Q}] = m^2 / 3 \cdot \delta_1(m) \cdot 3[\mathbb{Q}(\sqrt[3]{d}, \zeta_{2m}) : \mathbb{Q}] = m^2 \varphi(2m) \delta_1(m) \delta_2(m).$$

Since $K(m) K(n) = K(mn)$ if $(m, n) = 1$, we have

$$[K(mn) : \mathbb{Q}] = \frac{[K(m) : \mathbb{Q}][K(n) : \mathbb{Q}]}{[K(m) \cap K(n) : \mathbb{Q}]} = \frac{[K(m) : \mathbb{Q}][K(n) : \mathbb{Q}]}{6[K(m) \cap K(n) : F_0]},$$

which completes the proof.
Lemma 1.11. Let m, n be relatively prime natural numbers with $3 \nmid n$.

1. $[K(m) \cap K(n) : F_0]$ divides 6.
2. $[K(m) \cap K(n) : F_0] \equiv 0 \mod 3$ if and only if F is pure cubic, $3 \mid m$, $x^3 - \varepsilon'$ is irreducible over $F_0(\sqrt[3]{\varepsilon})$, $\Omega \notin \mathbb{Q}(\zeta_{2m})$ and $\Omega \in \mathbb{Q}(\zeta_{2m})$ hold.
3. $[K(m) \cap K(n) : F_0] \equiv 0 \mod 2$ if and only if $\delta_2(m) = \delta_2(n) = 2$ and $\delta_2(mn) = 1$.
4. When $\delta_2(mn) = 1$, i.e., $d \mid 2mn$, we decompose $d$ as $d = ab (a \mid 2m, b \mid 2n)$, where $a, b$ are 1 or discriminants of quadratic fields. Then the condition $[K(m) \cap K(n) : F_0] \equiv 0 \mod 2$ is equivalent to $a \neq 1, b \neq 1$ and then we have $K(m) \cap K(n) = F_0(\sqrt[3]{\varepsilon}) \neq F_0$.
5. $(n, 6d) = 1$ implies $K(m) \cap K(n) = F_0$ and $[K(mn) : \mathbb{Q}] = 6^{-1}[K(m) : \mathbb{Q}][K(n) : \mathbb{Q}]$.

Proof. By the previous lemma and $3 \nmid n$, we have

$$[K(m) \cap K(n) : F_0] = \frac{\delta_1(m)}{\delta_1(mn)} \cdot \frac{\delta_2(m)}{\delta_2(mn)} \cdot \frac{\delta_2(n)}{\delta_2(mn)}.$$
virtue of $4 | b | d$ and $2m$. Similarly, we have $\delta_2(n) = 2$. Let us prove the last assertion. Suppose $(n, 6d) = 1$. Assume $[K(m) \cap K(n) : F_0] \equiv 0 \mod 3$. Since $\Omega \in K(3)$ by definition in Lemma 1.6, prime divisors of the conductor of an abelian field $\mathbb{Q}(\Omega)$ divide $6d$. Hence $\mathbb{Q}(\Omega) \subset \mathbb{Q}(\epsilon_{2m})$, which is a contradiction in the assertion (2). If $[K(m) \cap K(n) : F_0] \equiv 0 \mod 2$, then for $b$ in (4), $b | (2n, d)$ and $d = 2$ implies $b = 1$, which contradicts $[K(m) \cap K(n) : F_0] \equiv 0 \mod 2$. Thus we have $([K(m) \cap K(n) : F_0], 6) = 1$ and hence $K(m) \cap K(n) = F_0$.

**Lemma 1.12.** Let $n$ be a natural number with $3 \nmid n$. Then $[K(3) \cap K(n) : F_0] \equiv 0 \mod 3$ if and only if $F$ is pure cubic, $x^3 - \epsilon'$ is irreducible over $F_0(\sqrt[3]{\epsilon})$ and $\mathbb{Q}(\Omega) \subset \mathbb{Q}(\epsilon_n)$. And moreover it is equivalent to $K(3) \cap K(n) = F_0(\Omega) \cap F_0$ with $[F_0(\Omega) : F_0] = 3$.

**Proof.** We use the assertion (2) of Lemma 1.11. By Lemma 1.6, the condition $\mathbb{Q}(\Omega) \in \mathbb{Q}(\epsilon_n)$ is automatically excluded, since $[\mathbb{Q}(\Omega) : \mathbb{Q}] = 6$. It implies the first equivalence. Suppose $[K(3) \cap K(n) : F_0] \equiv 0 \mod 3$; then $K(n)$ contains $\epsilon_n$ since $F$ is pure cubic. Hence $K(n) = F_0(\epsilon_n, \sqrt[3]{\epsilon}, \sqrt[3]{\epsilon'}) \supset \mathbb{Q}(\epsilon_n) \in \mathbb{Q}(\Omega)$ holds and then $K(3) \cap K(n) = F_0(\Omega)$. It is easy to see $[F_0(\Omega) : F_0] = \mathbb{Q}(\Omega) = 6^{-1}[F_0(\Omega) : \mathbb{Q}] = 6^{-1}[F : \mathbb{Q}][\mathbb{Q}(\Omega) : \mathbb{Q}] = 3$ by Lemma 1.6. Therefore the assertion is clear.

**Lemma 1.13.** Let $p$ be a prime ideal of $F$ of degree $f$ and lying above an odd prime number $p$ and let $n$ be a natural number. Then $n | I(p)$ holds if and only if $p^f \equiv 1 \mod 2n$ and $x^e = \epsilon$ has a root in $F_p$.

**Proof.** By virtue of $p \neq 2$, we have $1 \equiv -1 \mod p$ and hence $#E(p)$ is even. Set $#E(p) = 2r$. Suppose $n | I(p)$; then $n$ divides $(p^f - 1)/(2r)$, which implies $p^f \equiv 1 \mod 2n$. Take a generator $\alpha \in O_F$ of the group $(O_F/p)^*$ and write $\epsilon \equiv \alpha^s \mod p$. Then $1 \equiv \alpha^{2r} \equiv \alpha^{2m} \mod p$ yields $2ra = (p^f - 1)t$ for some integer $t$. Write $(p^f - 1)/(2r) = m u$ for an integer $u$, we get $a = n u t$ and hence $\epsilon \equiv (\alpha^{u t})^s \mod p$. Since $n$ and $p$ are relatively prime, $x^e = \epsilon$ has a root in $F_p$. Conversely we assume $p^f \equiv 1 \mod 2n$ and $x^e = \epsilon$ has a root in $F_p$. Then there exists an element $\beta \in O_F$ such that $\beta^e \equiv \epsilon \mod p$, and write $\beta \equiv \alpha^m \mod p$. The order of $\epsilon \mod p$ in $(O_F/p)^*$ is $r$ or $2r$. First, suppose that it is equal to $r$. If $r$ is even, then $\epsilon^r \equiv 1 \mod p$ yields that $E(p)$ is generated by $\epsilon \mod p$ and hence $#E(p) = r$ which contradicts the definition of $r$. Hence $r$ is odd. $\epsilon \equiv \alpha^{m} \mod p$ implies $p^f - 1 | mn$ and we can write $mn = w(p^f - 1)$. If an integer $q$ divides $r$ and $w = 1$, then $\epsilon^{r/q} \equiv 1 \mod p$ holds, which is a contradiction, and so we have $(r, w) = 1$. On the other hand, $2n$ divides $p^f - 1$ and it means that $m/2 : r = w(p^f - 1)/(2n)$ is an integer. From $(r, w) = 1$ follows that $r | (p^f - 1)/(2n)$, i.e., $n | I(p)$. Second, suppose that the order of $\epsilon \mod p$ in $(O_F/p)^*$ is equal to $2r$. $\epsilon \equiv \alpha^{m} \mod p$
implies $p^f - 1 | 2mn$ and write $2mn = u(p^f - 1)$ for an integer $u$. Similarly to the above, $(r, u) = 1$ holds, and $mr = u \cdot (p^f - 1)/(2n)$ yields that $(p^f - 1)/(2n)$ is an integer, which is equivalent to $n | I(p)$.

2. PRIME IDEALS OF DEGREE 1

For a positive number $x$, we denote by $\mathcal{P}_{(1,1)}(x)$ the set of prime ideals $p$ of degree 1 of $F$ such that for a prime number $p$ lying below $p$, $p$ is odd, less than $x$, unramified in $F$, and completely decomposable in $F$. $\mathcal{P}_{(1,2)}(x)$ stands for the set of prime ideals $p$ of degree 1 of $F$ such that, for a prime number $p$ lying below $p$, $p$ is odd, less than $x$, unramified in $F$, and $p = pq$ for a prime ideal $q$ of degree 2 in $F$. Throughout this section, we abbreviate $\mathcal{P}_{(1,1)}(x)$ and $\mathcal{P}_{(1,2)}(x)$ to $\mathcal{P}(x)$, and $F_0(\zeta_{2n}, \sqrt[2]{\epsilon})$ to $F_0$ for a natural number $n$.

**Proposition 2.1.** Let $n$ be a natural number and $p$ a prime ideal in $\mathcal{P}(x)$ such that $p$ is unramified in $F_0$. Let $\mathfrak{P}$ be a prime ideal lying above $p$ of $F_0$ and set $\rho = (F_0/F)/\mathfrak{P}$ (the Frobenius automorphism). Then we have $n | I(p)$ and $p \in \mathcal{P}_{(1,1)}(x)$ if and only if $\rho = id$. holds, and we have $n | I(p)$ and $p \in \mathcal{P}_{(1,2)}(x)$ if and only if $[F_n: F(\zeta_{2n}, \sqrt[2]{\epsilon})] = 2$ and $\rho$ is the non-trivial automorphism of $\text{Gal}(F_n/F(\zeta_{2n}, \sqrt[2]{\epsilon}))$.

**Proof.** Let $p$ be a prime number lying below $p$. From Lemma 1.13 follows that $n | I(p)$ if and only if $p \equiv 1 \mod 2n$ and $x^n = \epsilon$ has a root in $F_0$.

First, suppose $n | I(p)$ and $p \in \mathcal{P}_{(1,1)}(x)$; then Lemma 1.1 yields that $p$ decomposes in $Q(\sqrt[n]{d})$ and hence $p \equiv 1 \mod 2n$ implies $\rho = id.$ on $Q(\zeta_{2n}, \sqrt[2]{d})$. The closure of $F(\zeta_{2n}, \sqrt[2]{d})$ in $(F_0)_0$ is $Q$, and $x^n = \epsilon$ is completely decomposable over $F_0$ since $x^n = \epsilon$ has a root in $F_0$ and $F_0(\zeta_{2n}, \sqrt[2]{d})$ contains $\zeta_{2n}$. It means that $(F_0)_0 \simeq Q$, and hence $\rho$ is the identity. If, conversely, $\rho$ is the identity, then $(F_0)_0 \simeq Q$ holds and so $n | I(p)$. And the fact that $\rho$ is trivial on $Q(\sqrt[n]{d})$ yields that $p$ decomposes in $Q(\sqrt[n]{d})$ and hence that by Lemma 1.1 $p$ is completely decomposable in $F$, because $\mathfrak{P} \cap F$ is of degree 1.

Next suppose $n | I(p)$ and $p \in \mathcal{P}_{(1,2)}(x)$; then $p$ remains prime in $Q(\sqrt[n]{d})$ by Lemma 1.1. Then $(F_0)_0 = (F_0(\zeta_{2n}, \sqrt[2]{d}))_0$ is a unique unramified quadratic extension of $Q_0$ and hence the order of $p$ is two and $\rho$ acts trivially on $F(\zeta_{2n}, \sqrt[2]{d})$. Thus $\text{Gal}(F_n/F(\zeta_{2n}, \sqrt[2]{d}))$ consists of $id.$ and $\rho$. If, conversely it is the case, then the closure of $F(\zeta_{2n}, \sqrt[2]{d})$ in $(F_0)_0$ is isomorphic to $Q$, and hence we have $n | I(p)$. Since $\rho(\sqrt[n]{d}) = -\sqrt[n]{d}$, $p$ is the product of $p$ and a prime ideal of degree 2 in $F$ and hence $p \in \mathcal{P}_{(1,2)}(x)$.
Lemma 2.1. We have

\[ [F_n : F] = \begin{cases} n\varphi(2n) & \text{if } \sqrt{d} \in \mathbb{Q}(\zeta_{2n}), \\ 2n\varphi(2n) & \text{if } \sqrt{d} \notin \mathbb{Q}(\zeta_{2n}). \end{cases} \]

Proof. It is easy to see

\[ [F_n : \mathbb{Q}] = [F(\sqrt{d}, \zeta_{2n}, \sqrt{\zeta}) : \mathbb{Q}] = [F(\sqrt{d}, \zeta_{2n}) : F(\sqrt{d}, \zeta_{2n})][F(\sqrt{d}, \zeta_{2n}) : \mathbb{Q}] = 3n[\mathbb{Q}(\sqrt{d}, \zeta_{2n}) : \mathbb{Q}]. \]

It yields the assertion.

Lemma 2.2. By denoting the discriminant of a field \( K \) by \( d(K) \), \( |d(F_n)| \) divides

\[ |d(F_0)^{n\varphi(2n)} n^{n\varphi(2n)} |d(\mathbb{Q}(\zeta_{2n}))|^{6n}. \]

Proof. This follows easily from the theory of discriminants.

For a positive numbers \( x, \eta, \eta_1, \eta_2 \) and a natural number \( n \), we set

\[ N(x) := \#\{ p \in \mathbb{P}(x) \mid I(p) = 1 \}, \]
\[ N(x, \eta) := \#\{ p \in \mathbb{P}(x) \mid q \mid I(p) \text{ for } q \leq \eta \}, \]
\[ M(x, \eta_1, \eta_2) := \#\{ p \in \mathbb{P}(x) \mid q \mid I(p) \text{ for } \eta_1 < q \leq \eta_2 \}, \]
\[ P(x, n) := \#\{ p \in \mathbb{P}(x) \mid n \mid I(p) \}, \]

where \( q \) stands for prime numbers, and moreover set

\[ \xi_1 := 6^{-1} \log x, \quad \xi_2 := \sqrt{x (\log x)^{-2}}, \quad \xi_3 := \sqrt{x \log x}. \]

By the definition, we have

\[ N(x, \xi_1) - M(x, \xi_1, x) \leq N(x) \leq N(x, \xi_1), \]

and hence \( N(x) = N(x, \xi_1) + O(M(x, \xi_1, x)) \) and

\[ M(x, \xi_1, x) \leq M(x, \xi_1, \xi_2) + M(x, \xi_2, \xi_3) + M(x, \xi_3, x). \]

We follow a method of Hooley [Ho] to obtain an asymptotic formula for \( N(x) \).

Lemma 2.3. \( M(x, \xi_3, x) = O(x(\log x)^{-2}). \)
Proof. Let \( p \in \mathbb{P}(x) \) and suppose that a prime number \( q \) satisfies \( \xi_3 < q \leq x \) and \( q \mid I(p) \). Denoting a prime number lying below \( p \) by \( p' \), we have \( q \mid (p-1)/\#E(p) \) and hence \( \#E(p) \mid (p-1)/q \). It yields \( e^{(p-1)/q} \equiv 1 \mod p \) and so \( \mathbb{N}_{F/Q}(e^{(p-1)/q} - 1) \equiv 0 \mod p \). Noting \( (p-1)/q \leq x/\sqrt{x \log x} = \sqrt{x/(\log x)^{-1}} \), we see

\[
2^{M(x, \xi_3, x)} < \prod_{1 \leq m \leq \sqrt{x/(\log x)^{-1}}} \prod_{1 \leq m \leq \sqrt{x/(\log x)^{-1}}} |\mathbb{N}_{F/Q}(e^m - 1)|,
\]

where \( p \) denotes prime numbers which contribute to \( M(x, \xi_3, x) \). Since we have \( |\mathbb{N}_{F/Q}(e^m - 1)| = |e^m - 1| |e' - 1| |e'' - 1| \leq 4e^m \) by \( |e|^2 = e^{-1} < 1 \), we get

\[
M(x, \xi_3, x) \log 2 \leq \sum_{1 \leq m \leq \sqrt{x/(\log x)^{-1}}} (\log 4 + m \log e) = O(x(\log x)^{-2}).
\]

**Lemma 2.4.** \( M(x, \xi_2, \xi_3) = O(x \log \log x/(\log x)^2) \).

Proof. For a prime ideal \( p \) contributing to \( M(x, \xi_2, \xi_3) \), there is a prime number \( q \) such that \( \xi_2 < q \leq \xi_3 \) and \( q \mid I(p) \mid p-1 \). Hence we have

\[
M(x, \xi_2, \xi_3) \leq 3 \sum_{\xi_2 < q \leq \xi_3} \#\{\text{prime numbers } p \text{ such that } p \equiv 1 \mod q \text{ and } p \leq x \}
= O(x \log \log x/(\log x)^2)
\]

as in [Ho].

**Lemma 2.5.** \( M(x, \xi_1, \xi_2) \leq \sum_{\xi_1 < q \leq \xi_2} P(x, q) \), where \( q \) stands for prime numbers.

Proof. It is clear.

**Lemma 2.6.** \( N(x, \xi_1) = \sum_{n \mid \mathcal{Q}(\xi_1)} \mu(n) P(x, n) \), where \( \mathcal{Q}(\xi_1) = \prod_{q \leq \xi_1} q \) (\( q \) denotes prime numbers).

The proof is quite similar as in the Introduction.

Summing up, we have

\[
N(x) = \sum_{n \mid \mathcal{Q}(\xi_1)} \mu(n) P(x, n) + O\left( \sum_{\xi_1 < q \leq \xi_2} P(x, q) \right) + O(x \log \log x/(\log x)^2) + O(1).
\]

Now we define the conjugacy class \( C_n \) of \( Gal(F_n/F) \) with \#\( C_n \leq 1 \) such that \( C_n = \{id.\} \) if \( P(x) = P_{(1,1,1)}(x) \), and \( C_n = \{\text{the non-trivial automorphism in } Gal(F_n/F(\zeta_{2n}, \sqrt{7}))\} \) if \( P(x) = P_{(1,2)}(x) \) and \( [F_n: F(\zeta_{2n}, \sqrt{7})] = 2 \), and \( C_n \) is empty if \( P(x) = P_{(1,2)} \) and \( F_n = F(\zeta_{2n}, \sqrt{7}) \). Then we have
Lemma 2.7. \(|P(x, n) - \pi_{C_n}(x, F_n/F)| = O(\sqrt{x}/\log x + \omega(n))\), where \(\omega(n)\) is the number of prime divisors of \(n\).

Proof. By virtue of Proposition 2.1, we have only to remark that the number of prime ideals ramified in \(F_n/F\) is \(O(\omega(n))\) and the number of prime ideals \(p\) of degree \(\geq 2\) and \(N_{F/Q}(p) \leq x\) is \(O(\sqrt{x}/\log x)\) by the prime number theorem.

Lemma 2.8. We have

\[
\sum_{n \mid Q(t_1)} \mu(n) P(x, n) = \sum_{n \mid Q(t_1)} \mu(n) \pi_{C_n}(x, F_n/F) + O(x \log \log x/\log x^2),
\]

\[
\sum_{\xi_1 < q < \xi_2} P(x, q) = \sum_{\xi_1 < q < \xi_2} \pi_{C_q}(x, F_q/F) + O(x \log \log x/\log x^2),
\]

where \(q\) stands for prime numbers.

Proof. We have only to show that

\[
\sqrt{x} (\log x)^{-1} \sum_{n \mid Q(t_1)} 1, \sum_{n \mid Q(t_1)} \omega(n), \sqrt{x} (\log x)^{-1} \sum_{\xi_1 < q < \xi_2} 1, \text{ and } \sum_{\xi_1 < q < \xi_2} \omega(q)
\]

are estimated by \(O(x \log \log x/\log x^2)\). It is easy to see, by using \(\pi(\xi_1) < 12\xi_1/\log \xi_1\) for the counting function \(\pi\) of prime numbers

\[
\sum_{n \mid Q(t_1)} 1 = 2^{\pi(\xi_1)} < 2^{12\xi_1/\log \xi_1}
\]

\[
= 2^{2 \log x/\log(6^{-1} \log x)} < x^{0.1}
\]

for a sufficiently large \(x\), and hence we have

\[
\sqrt{x} (\log x)^{-1} \sum_{n \mid Q(t_1)} 1 < x^{0.1}(\log x)^{-1} = O(x \log \log x/\log x^2).
\]

Second, we see

\[
\sum_{n \mid Q(t_1)} \omega(n) = \sum_{n \mid Q(t_1)} \sum_{p \mid n} 1 = \sum_{p \mid Q(t_1)} \sum_{p \mid n, n \mid Q(t_1)} 1
\]

\[
= \sum_{p \mid Q(\xi_1)} \tau(Q(\xi_1)/p) = \tau(Q(\xi_1)/2) \pi(\xi_1),
\]
where \( p \) denotes prime numbers and \( \tau(n) \) is the number of positive divisors of \( n \). Therefore, we have

\[
\sum_{n \mid Q(t_1)} \omega(n) = O(2^{12\xi_1/\log \xi_1} \cdot 12\xi_1/\log \xi_1) = O(x^{0.1})
\]

for a sufficiently large \( x \). Thus \( \sum_{n \mid Q(t_1)} \omega(n) = O(x \log \log x / (\log x)^2) \) holds for a sufficiently large \( x \). Since \( \sum_{\zeta_1 < \eta < \zeta_2} 1 < \zeta_2 = \sqrt{x} (\log x)^{-2} \), we have the required estimate for the third, and similarly for the fourth because of \( \omega(q) = 1 \) for prime numbers \( q \).

Thus we have

\[
N(x) = \sum_{n \mid Q(t_1)} \mu(n) \pi_C(x, F_n / F) + O \left( \sum_{\zeta_1 < \eta < \zeta_2} \pi_C(x, F_\eta / F) \right) + O(x \log \log x / (\log x)^2).
\]

Now we apply the Chebotarev density theorem under the GRH [LO, S].

**Theorem.** Let \( E/K \) be a Galois extension and \( C \) a subset of \( \text{Gal}(E/K) \) which is a union of conjugacy classes. Then we have, under the GRH for the Dedekind zeta function for \( E \)

\[
\left| \frac{\pi_C(x, E/K)}{[E : K]} - \frac{\#C}{[E : K]} \text{Li}(x) \right| < c \frac{\#C}{[E : K]} \sqrt{x} (\log |d(E)| + [E : Q] \log x),
\]

where \( d(E) \) is the discriminant of \( E \) and \( c \) is an absolute constant.

**Lemma 2.9.** Under the GRH, we have

\[
\sum_{\zeta_1 < \eta < \zeta_2} \pi_C(x, F_\eta / F) = O(x \log \log x / (\log x)^2),
\]

where \( q \) stands for prime numbers.

**Proof.** We have only to show that

\[
\left( \sum_{\zeta_1 < \eta < \zeta_2} [F_\eta : F]^{-1} \right) \text{Li}(x),
\]

\[
\left( \sum_{\zeta_1 \leq \eta < \zeta_2} \log |d(F_\eta)| \right) \sqrt{x}, \left( \sum_{\zeta_1 \leq \eta < \zeta_2} [F_\eta : Q] / [F_\eta : F] \right) \sqrt{x} \log x
\]
are bounded by $O(x \log x / (\log x)^2)$. By virtue of Lemma 2.1, we see

\[ \sum_{\zeta_1 < \zeta < \zeta_2} [F_q : F]^{-1} \ll \sum_{\zeta_1 < \zeta < \zeta_2} 1/q(q-1) \ll \sum_{\zeta_1 < \zeta < \zeta_2} 1/q^2 \]

\[ < \sum_{n > \zeta_1} \frac{1}{n^2} \ll \int_{\zeta_1}^\infty x^{-2} dx = 1/\zeta_1 = 6/\log x \]

and then $\text{Li}(x)/\log(x) = O(x/(\log x)^2) = O(x \log \log x / (\log x)^2)$ gives the estimate for the first. Lemma 2.2 yields

\[ \log |d(F_q)| \leq q(q-1) \log |d(F_0)| + 6q(q-1) \log q \]

\[ + 6q(q-2) \log q, \]

and hence we have

\[ \sum_{\zeta_1 < \zeta < \zeta_2} [F_q : F]^{-1} \log |d(F_q)| \ll \sum_{\zeta_1 < \zeta < \zeta_2} (\log |d(F_0)| + \log q) \]

\[ \ll \log |d(F_0)| \cdot \frac{\sqrt{x}}{(\log x)^2} + \frac{\sqrt{x}}{(\log x)^2}, \]

which gives the estimate for the second. Here we used a famous inequality $\theta(x) = \sum_{\zeta < x} \log q < x$. The estimate for the third follows from $[F_q : \mathbb{Q}] / [F_q : F] = 3$ and $\sum_{\zeta_1 < \zeta < \zeta_2} 1 \ll (\sqrt{x}/(\log x)^2) / \log((\sqrt{x}/(\log x)^2))$.  

**Lemma 2.10.** Under the GRH, we have

\[ \sum_{n \geq 1} \mu(n) \pi_{C_n}(x, F_n / F) = c_0 \text{Li}(x) + O(x \log \log x / (\log x)^2) \]

for $c_0 := \sum_{n > 1} \mu(n) \# C_n / [F_n : F]$.

**Proof.** By the Chebotarev density theorem, we find

\[ \sum_{n \geq 1} \mu(n) \pi_{C_n}(x, F_n / F) \]

\[ = \sum_{n \geq 1} \frac{\mu(n) \# C_n \text{Li}(x)}{[F_n : F]} \]

\[ + O \left( \sum_{n \geq 1} \frac{\sqrt{x}}{[F_n : F]} (\log |d(F_n)| + [F_n : \mathbb{Q}] \log x) \right). \]
Since $\sum_{n \mid Q(t)} 1 = O(x^{\alpha})$ as before, it is easy to see that the contributions of the last term is $O(x \log \log x/(\log x)^2)$. Next, for the second term we see

$$\sum_{n \mid Q(t)} \log |d(F_n)| \left\lbrack F_n : F \right\rbrack$$

$$\ll \sum_{n \mid Q(t)} [F_n : F]^{-1} (n \varphi(2n) \log |d(F_0)|) + 6n \varphi(2n) \log n + 6n \log |d(Q(\zeta_{2n}))|$$

$$\ll \sum_{n \mid Q(t)} \log n \quad (\text{by Lemma 2.1 and } d(Q(\zeta_{2n})) | (2n)^{\varphi(2n)})$$

$$< \log O(\xi_1) \sum_{n \mid Q(t)} 1.$$  

Then $\log O(\xi_1) = \sum_{q \leq \xi_1} \log q \ll \xi_1 = (\log x)/6$ and $\sum_{n \mid Q(t)} 1 < x^{\alpha}$ as above yield the estimate $O(x \log \log x/(\log x)^2)$ for the second. Last, we show $\sum_{n \mid Q(t)} \mu(n) \#C_n/[F_n : F] = c_0 + O(1/\log x)$, which completes the proof of the lemma.

It is easy to see

$$\sum_{n \mid Q(t)} \mu(n) \#C_n/[F_n : F] = c_0 + O \left( \sum_m 1/[F_n : F] \right),$$

where $m$ runs over the set of integers such that one of prime divisors of $m$ is larger than $\xi_1$. For such $m$’s, we have

$$\sum_m 1/[F_n : F] \ll \sum_m 1/m \varphi(m) < \sum_{n > \xi_1} 1/n \varphi(n)$$

$$\ll \sum_{n > \xi_1} n^{-2} \cdot n = \sum_{n > \xi_1} n^{-2} \prod_{p \mid n} (1-p^{-2})^{-1} \prod_{p \mid n} (1+p^{-1})$$

$$\ll \zeta(2) \sum_{n > \xi_1} n^{-2} \sum_{k \mid n} k^{-1} \ll \sum_{k \mid n, \zeta_1 < n} k^{-1} \sum_{k \mid n, \zeta_1 < n} n^{-2}$$

$$= \sum_{k = 1}^{\infty} k^{-1} \sum_{t > \zeta_1/k} (\ell k)^{-2} = \sum_{k = 1}^{\infty} k^{-3} \sum_{t > \zeta_1/k} \ell^{-2}$$

$$\ll \sum_{k = 1}^{\infty} k^{-3} \cdot k/\zeta_1 \ll 1/\zeta_1 = 6/\log x,$$

which yields the desired inequality. \qed
Remark. In the case of $P(x) = P_{(1,1,1)}(x)$,

\[ P(x, 1) = \#P(x) \]

= 3 times the number of primes $p$ which is less than or equal to $x$ and completely decomposable in $F$

= 3 times the number of primes $p$ which is less than or equal to $x$ and completely decomposable in $F_0$

\[ = 1/2 \cdot \text{Li}(x) + \text{error holds and so } \#C_1/[F_1 : F] \text{ should be } 1/2. \]

Similarly, $\#P_{(1,2)}(x) = \# \{ p \leq x \mid (p) = p_1p_2 \} = \# \{ p \leq x \mid p \text{ remains prime in } \mathbb{Q}(\sqrt{d}) \} = 1/2 \cdot \text{Li}(x) + \text{error forces } \#C_1/[F_1 : F] = 1/2$ again.

**Theorem 2.1.** Under the GRH, we have

\[ N(x) = c_0 \cdot \text{Li}(x) + O(x \log \log x / (\log x)^2), \]

where $c_0 = \sum_{n > 1} \mu(n) \#C_n/[F_n : F]$ is positive.

**Proof.** The proof of the positivity of $c_0$ remains.

The case of $P(x) = P_{(1,1,1)}(x)$.

From Lemma 2.1 follows

\[ c_0 = \sum_{n = 1}^{\infty} \mu(n)/[F_n : F] \]

\[ = \sum_{n \geq 1}^{\infty} \frac{\mu(n)/n\varphi(2n)}{d \mid 2n} + 2^{-1} \sum_{n \geq 1}^{\infty} \frac{\mu(n)/n\varphi(2n)}{d \not \mid 2n} \]

\[ = 2^{-1} \sum_{n \geq 1}^{\infty} \frac{\mu(n)/n\varphi(2n)}{d \mid 2n} + 2^{-1} \sum_{n \geq 1}^{\infty} \frac{\mu(n)/n\varphi(2n)}{d \not \mid 2n}. \]

Here we see

\[ \sum_{n \geq 1}^{\infty} \frac{\mu(n)/n\varphi(2n)}{d \mid 2n} = \sum_{n \text{ even}}^{\infty} \frac{\mu(n)/n\varphi(n)}{n} + \sum_{n \text{ even}}^{\infty} \frac{\mu(n)/(n \cdot 2\varphi(n/2))}{n} \]

\[ = \left(1 - 1/4\right) \prod_{p \neq 2} (1 - 1/p(p-1)) = 3/2 \cdot A, \]

where $A := \prod_{p \neq 2} (1 - 1/p(p-1))$ is the Artin constant. Set

\[ c_1 := \sum_{n \geq 1}^{\infty} \frac{\mu(n)/n\varphi(2n)}{d \mid 2n}. \]

If $8 \mid \overline{d}$, then $c_1 = 0$ is clear, and hence $c_0 = 3/4 \cdot A > 0$. 

338 YOSHIYUKI KITAOKA
Suppose $4 \parallel \tilde{d}$; then we have

$$c_1 = \sum_{\substack{n \geq 1 \\text{add} \\tilde{d} \mid 4m}} \mu(2m)/(2m \varphi(4m)) = -4^{-1} \sum_{\substack{n \geq 1 \\text{add} \\tilde{d} \mid 4m}} \mu(m)/m \varphi(m)$$

$$= -4^{-1} \mu(\tilde{d}/4)/(\tilde{d}/4 \cdot \varphi(\tilde{d}/4)) \cdot \prod_{p \mid \tilde{d}} (1 - 1/p(p - 1))$$

$$= -\mu(\tilde{d}/4)/(\tilde{d} \varphi(\tilde{d}/4)) \cdot \prod_{p \mid \tilde{d}} (p(p - 1)/(p^2 - p - 1)) \cdot A$$

$$= -\mu(\tilde{d}/4)/(\tilde{d} \varphi(\tilde{d}/4)) \cdot \prod_{p \mid \tilde{d}} (p^2 - p - 1)^{-1} \cdot A.$$

Hence we have $c_0 = 4^{-1}(3 - \mu(\tilde{d}/4) \prod_{p \mid \tilde{d}} (p^2 - p - 1)^{-1}) \cdot A > 0$.

Suppose $2 \not\mid \tilde{d}$; then we have

$$c_1 = \sum_{\tilde{d} \mid 2n} \mu(n)/n \varphi(2n) = \sum_{k \geq 1} \mu(k \tilde{d})/k \tilde{d} \varphi(2k \tilde{d})$$

$$= \mu(\tilde{d})/\tilde{d} \varphi(\tilde{d}) \sum_{(k, \tilde{d}) = 1} \mu(k)/k \varphi(2k)$$

$$= \mu(\tilde{d})/\tilde{d} \varphi(\tilde{d}) \left\{ \sum_{(k, 2\tilde{d}) = 1} \mu(k)/k \varphi(k) - 4^{-1} \sum_{(k, 2\tilde{d}) = 1} \mu(k)/k \varphi(k) \right\}$$

$$= 3/4 \cdot \mu(\tilde{d})/\tilde{d} \varphi(\tilde{d}) \prod_{p \mid 2\tilde{d}} (1 - 1/p(p - 1))$$

$$= 3/2 \cdot \mu(\tilde{d}) \prod_{p \mid 2\tilde{d}} (p^2 - p - 1)^{-1} \cdot A.$$

Thus we have $c_0 = 3/4 \cdot (1 + \mu(\tilde{d}) \prod_{p \mid 2\tilde{d}} (p^2 - p - 1)^{-1}) \cdot A > 0$.

The case of $P(x) = P_{(1, 2)}(x)$.

The condition $[F_\alpha : F(\zeta_{2n}, \sqrt{\alpha})] = 2$ is equivalent to $\sqrt{\alpha} \not\in F(\zeta_{2n}, \sqrt{\alpha})$, which is equivalent to $\sqrt{\alpha} \not\in \mathbb{Q}(\zeta_{2n})$, i.e., $\tilde{d} \not\mid 2n$ by Lemma 1.3. Thus in this case

$$c_0 = \sum_{n \geq 1} \mu(n)/[F_\alpha : F] = \sum_{n \geq 1} \mu(n)/2n \varphi(2n)$$

$$= \frac{1}{2} \sum_{n \geq 1} \mu(n)/n \varphi(2n) - \frac{1}{2} \sum_{n \geq 1} \mu(n)/n \varphi(2n)$$

$$= \frac{1}{2} A - \frac{1}{2} c_1 > 0,$$

using the above evaluation of $c_1$. □
3. PRIME IDEALS OF DEGREE 2

In this and the next section, we study the prime ideals of degree 2 and 3, respectively. However, we do not succeed to give the assertion analogous to Theorem 2.1, but conjecture the positive density \( c_3 \) explicitly.

**Lemma 3.1.** Let \( p \) be an odd prime number which is unramified in \( F_0 \) and remains prime in \( \mathbb{Q}(\sqrt{-d}) \). Let \( (p) = p_1p_2 \) be the decomposition in \( F \) with prime ideals \( p_i \) of degree \( i \), and \( r_i \) the order of \( e \mod p_i \) in \((O_F/p_i)^*\). Then we have

\[
I(p_1) | I(p_2), \quad I(p_2) I(p_1)^{-1} | p + 1, \quad (I(p_2) I(p_1)^{-1}, I(p_1)) | 2,
\]

\[
\text{if } r_1 | r_2, \quad r_2 | (p + 1) r_1, \quad \#E(p_1) | \#E(p_2).
\]

**Proof.** Let \( \mathfrak{P}_1 \) be a prime ideal of \( F_0 \) lying above \( p_1 \). Since \( p \) remains prime in \( \mathbb{Q}(\sqrt{-d}) \), the degree of \( \mathfrak{P}_1 \) is two and hence \( p_1 \) remains prime in \( F_0 \) and \( p_2 \) decomposes in \( F_0 \). Let \( j \) be the complex conjugation and \( \rho \in Gal(F_0/\mathbb{Q}) \) an automorphism of degree 3. Set \( \mathfrak{P}_2 := \rho(\mathfrak{P}_1), \mathfrak{P}_3 := \rho^2(\mathfrak{P}_1) \); then \( p_2 = \mathfrak{P}_2 \mathfrak{P}_3 \). By virtue of \( j(p_1) = p_1 \), we have \( j(\mathfrak{P}_1) = \mathfrak{P}_1 \) and \( j(\mathfrak{P}_2) = \mathfrak{P}_3 \). Since \( j \) is the Frobenius automorphism of \( \mathfrak{P}_1 \), \( \rho \rho^{-1} \) is one for \( \mathfrak{P}_2 \). Hence we have \( \rho \rho^{-1}(\mathfrak{P}_1) \equiv \mathfrak{P}_1 \mod \mathfrak{P}_2 \) and then \( \rho \rho^{-1}(\mathfrak{P}_1) \equiv \mathfrak{P}_1 \mod \mathfrak{P}_2 \), which implies \( N_{F_0/F}(\mathfrak{P}_1) = \mathfrak{P}_1 \cdot \mathfrak{P}_2 \cdot \mathfrak{P}_3 = \mathfrak{P}_1 \cdot \mathfrak{P}_2 \cdot \mathfrak{P}_2 \cdot \mathfrak{P}_3 = \mathfrak{P}_1 \cdot \mathfrak{P}_2 \cdot \mathfrak{P}_2 \cdot \mathfrak{P}_3 = \mathfrak{P}_1 \cdot \mathfrak{P}_2 \cdot \mathfrak{P}_3 \cdot \mathfrak{P}_3 = \mathfrak{P}_1 \cdot \mathfrak{P}_2 \cdot \mathfrak{P}_3 \cdot \mathfrak{P}_3 \).

Choose a generator \( \alpha \in O_F \) of \((O_F/p_2)^*\) and set \( \varepsilon \equiv \alpha^* \mod p_2 \). Then \( \varepsilon^2 = \alpha^2 \equiv 1 \mod p_2 \) implies \( \alpha = \alpha^{-1} \mod p_2 \) for an integer \( u \). \( (u, r_2) = 1 \) is easy. Since \( \varepsilon^2 \equiv \alpha^2 \mod \mathfrak{P}_3 \), we have \( \rho(\varepsilon) \equiv \varepsilon \mod \mathfrak{P}_3 \) and hence

\[
\rho(\varepsilon) = \rho(\alpha) \equiv (\rho(\alpha) \cdot j(\rho(\alpha)))^* \mod \mathfrak{P}_3.
\]

On the other hand, we know \( N_{F_1/F}(\varepsilon) = \varepsilon \rho(\varepsilon) \rho^2(\varepsilon) = \varepsilon \rho(\varepsilon) j(\rho(\varepsilon)) = 1 \) and then \( \varepsilon^{-1} \equiv N_{F_1/F}(\rho(\alpha))^* \mod \mathfrak{P}_3 \). This yields \( \varepsilon^{-1} = N_{F_1/F}(\rho(\alpha))^n \mod p_1 \equiv 1 \mod p_1 \), and hence \( r_1 | r_2 \) holds. Set \( \delta_1 = \#E(p_1)/r_1 \) (\( = 1 \) or 2). If \( 2 | r_1 \), then \( \varepsilon^{r_1/2} \equiv -1 \mod p_1 \) and so \( \delta_1 = 1 \) holds. If \( 2 \nmid r_1 \), then \( \varepsilon^r \equiv -1 \mod p_1 \) for any integer \( n \) and so \( \delta_1 = 2 \). Thus \( 2 \nmid r_1 \) is equivalent to \( \delta_1 = 2 \). By \( r_1 | r_2 \) above, \( \delta_2 = 2 \) implies \( \delta_1 = 2 \) and hence \( \delta_1 / \delta_2 \) is an integer. Now we see that

\[
I(p_2) / I(p_1) = (p^2 - 1)/\delta_2 r_2 \cdot \delta_1 r_1 / (p - 1) = \delta_1 / \delta_2 \cdot (p + 1) r_1 / r_2.
\]
is an integer by \( r_2 | (p+1) \). Next, \( (I(p_2)/I(p_1)) = \delta_1 / \delta_2 \cdot (p+1)/(r_2/r_1) \) divides \( p+1 \) if \( \delta_1 = \delta_2 \). If \( \delta_1 \neq \delta_2 \), then \( \delta_1 = 2 \) and \( \delta_2 = 1 \) hold and then \( r_1 \) is odd and \( r_2 \) is even and so \( r_2/2r_1 \) is an integer. Hence \( I(p_2)/I(p_1) = (p+1)/(r_2/2r_1) \in \mathbb{Z} \) yields that \( I(p_2)/I(p_1) \) divides \( p+1 \). Hence \( #E(p_2)/#E(p_1) = (p+1)/I(p_1)/I(p_2) \) is an integer. Lastly, \( (I(p_2)/I(p_1), I(p_1)) \) divides \( (p+1, p-1) = 2 \).

**Lemma 3.2.** Assumptions and notations being as in Lemma 3.1, \( r_1 \) is even if and only if \( I(p_2)/I(p_1) \) is odd.

**Proof.** We use the notations of the proof of the previous lemma. First, suppose \( I(p_2)/I(p_1) \) is odd. We show \( #E(p_2) = r_2 \). If \( r_2 \) is odd, then \( #E(p_2) = 2r_2 \equiv 2 \mod 4 \), which contradicts \( #E(p_2) = (p+1)/I(p_2)/I(p_1) \cdot #E(p_1) \equiv 0 \mod 4 \). Hence \( r_2 \) is even and then \( #E(p_2) = r_2 \). If \( r_1 \) is odd, then \( #E(p_1) = 2r_1 \) holds and

\[
I(p_2)/I(p_1) = (p+1)/I(p_1)/I(p_2) = (p+1)/2r_1/r_2 \equiv 0 \mod 2
\]

by Lemma 3.1, which contradicts the assumption. Thus \( r_1 \) is even.

Conversely, suppose that \( I(p_2)/I(p_1) \) is even. It yields

\[
#E(p_2) | (p+1) #E(p_1)/2
\]

\[
\Rightarrow e^{(p+1)#E(p_1)/2} \equiv 1 \mod p_2
\]

\[
\Rightarrow e^{(p+1)#E(p_1)/2} \equiv 1 \mod \Psi_2 \Rightarrow (e \cdot \rho j p^{-1}(e))^{#E(p_1)/2} \equiv 1 \mod \Psi_2
\]

\[
\Rightarrow \rho(e)^{#E(p_1)/2} \equiv 1 \mod \Psi_2 \quad (by \: p j p^{-1}(e) = \rho \gamma(e), \: \varepsilon p(e) \: \rho \gamma(e) = 1)
\]

\[
\Rightarrow e^{#E(p_1)/2} \equiv 1 \mod \Psi_1 \Rightarrow e^{#E(p_1)/2} \equiv 1 \mod p_1
\]

Hence \( #E(p_1) \neq r_1 \) holds and then \( r_1 \) is odd.

**Proposition 3.1.** Assumptions and notations being as in Lemma 3.1, let \( n \) be a natural number. \( n|I(p_1)|I(p_2) \) implies \( n \mid p+1 \), and under the assumption \( n \mid p+1 \), we have

\[
n|I(p_1)|I(p_2) \iff \begin{cases} n \mid I(p_2) & \text{if } 2 \nmid n \text{ or } 4 \mid n, \\ 2^{a_{d_1}(p-1)/2}n \mid I(p_2) & \text{if } 2 \nmid n, \end{cases}
\]

where \( a := \text{ord}_2 \) is defined by \( 2^a \mid m \).

**Proof.** The first assertion follows from Lemma 3.1. Hereafter we suppose \( n \mid p+1 \). First suppose that \( 2 \nmid n \) or \( 4 \mid n \). We have only to prove that \( n \mid I(p_2) \) implies \( n|I(p_1)|I(p_2) \). Suppose \( n \mid I(p_2) \). By virtue of \( n \mid p+1 \), we have \( (n, p-1) = 1 \) or \( 2 \). If \( n \) is odd, then \( (n, p-1) = 1 \) holds and then
(n, I(p_i)) = 1. Since n | I(p_2) and I(p_1) | I(p_2) by Lemma 3.1, we obtain nI(p_1) | I(p_2). If 4 | n, then (n, p−1) = 2 and so (n/2, (p−1)/2) = 1. Hence (p−1)/2 = I(p_1) | #E(p_1)/I(p_1) is odd and so is I(p_1). It implies (n, I(p_1)) = 1 by I(p_1) | p−1 and then nI(p_1) | I(p_2) holds. Next suppose 2 ⊥ n. If nI(p_1) | I(p_2), then I(p_2)/I(p_1) is even and hence r_1 is odd by the previous lemma. It yields #E(p_1) = 2r_1 and I(p_1) = (p−1)/(2r_1) = 0 mod 2ord_p((p−1)/2) and 2ord_p((p−1)/2)n | I(p_2). Conversely we suppose 2ord_p((p−1)/2)n | I(p_2). Since n/2 is an odd divisor of p+1 and n/2 | I(p_2), the former part of the proof shows n/2 | I(p_1) | I(p_2). We have only to show ord_2 I(p_2) ≥ ord_2(nI(p_1)) to complete the proof. We see easily that from (p−1)/2 | ord_p((p−1)/2) and then ord_2 I(p_2) = ord_2((p−1)/2) + ord_2 n = ord_2((p−1)/2) + 1 ≥ ord_2 I(p_1) + 1 = ord_2(nI(p_1)).

**Proposition 3.2.** Let p be a prime number unramified in K(m) and Q a prime ideal of K(m) lying above p, and set ρ = ((K(m)/Q)/Q). Then (p) = p_1p_2 in F holds for a prime ideal p_i of degree i, and m | I(p_i) holds if and only if p^2 = id. and ρ(√d) = −√d.

**Proof.** Suppose that (p) = p_1p_2 holds for a prime ideal p_i of degree i and m | I(p_i). By Lemma 1.1, p remains prime in Q(√d). It implies ρ(√d) = −√d. Lemma 1.13 yields p^2 ≡ 1 mod 2m and x^m = e has a root in F_{p_2}. On the other hand, by the definition ρ(ζ_{2m}) = ζ_{2m} holds and then ρ^2(ζ_{2m}) = ζ_{2m}. Since the closure of F(ζ_{2m}, √d) in K(m)_Q is an unramified quadratic extension of Q, and x^m = e has a root in the closure, K(m)_Q is also an unramified quadratic extension of Q, which implies ρ^2 = id.

Conversely, suppose ρ^2 = id and ρ(√d) = −√d. The condition ρ(√d) = −√d yields that p remains prime in Q(√d) and hence p has a decomposition (p) = p_1p_2 in F with a prime ideal p_i of degree i by Lemma 1.1. We may assume p_2 = Q ∩ F, taking a conjugate ideal of Q if necessary. From ρ^2 = id follows that K(m)_Q is a quadratic unramified extension of Q, and F_{p_2} is also quadratic and unramified over Q. Therefore x^m = e is soluble in F_{p_2}. ρ_{loca(Z_m)}^2 = id. implies p^2 ≡ 1 mod 2m. Lemma 1.13 implies m | I(p_2).

Now let us prepare several lemmas to prove Proposition 3.3

**Lemma 3.3.** Unless F is pure cubic, there exist infinitely many prime numbers p satisfying that both (p) = p_1p_2 in F for prime ideals p_i of degree i and 3I(p_i) ⊥ I(p_2).
Proof. By the fact that $\mathbb{Q}(\sqrt{d}) = \mathbb{Q}(\sqrt{-3})$ if and only if $F$ is pure cubic, our assumption yields that $F_0$ does not contain $\sqrt{-3}$. Choose $\rho \in \text{Gal}(F_0(\sqrt{-3})/\mathbb{Q})$ so that $\rho(\sqrt{d}) = -\sqrt{d}$ and $\rho(\sqrt{-3}) = \sqrt{-3}$. Let $\mathfrak{P}$ be a prime ideal of $F_0(\sqrt{-3})$ such that $p = ((F_0(\sqrt{-3})/\mathbb{Q})/\mathfrak{P})$ and let $p$ be a prime number lying below $\mathfrak{P}$. Since $\rho(\sqrt{-3}) = \sqrt{-3}$, $p$ decomposes in $\mathbb{Q}(\sqrt{-3})$ and hence $p \equiv 1 \mod 3$ holds. On the other hand, $\rho$ is not trivial in $\mathbb{Q}(\sqrt{d})$, and then $p$ remains prime there and by Lemma 1.1, $p$ decomposes as $(p) = p_1p_2$ in $F$ where the degree of $p_1 = i$. By Lemma 3.1, $I(p_2)/I(p_1)$ divides $p+1$ which is not divisible by 3. Hence $3I(p_1)$ does not divide $I(p_2)$.

Lemma 3.4. Assumptions and notations being as in Lemma 3.1, and suppose that $F$ is pure cubic; then $3I(p_1)|I(p_2)$ if and only if $p_2$ is completely decomposable in $F_0(\sqrt{d})$.

Proof. $p$ remains prime in $\mathbb{Q}(\sqrt{d}) = \mathbb{Q}(\sqrt{-3})$ and hence $p \equiv 2 \mod 3$ holds and $p_2$ decomposes in $F_0$. Suppose $3I(p_1)|I(p_2)$, first. We denote by $r$ the order of $\varepsilon \mod p_2$ in $(O_F/p_2)\mathbb{F}$ and define $\delta = 1$ or $2$ by $#E(p_2) = r\delta$. Let $\alpha \in O_F$ be a primitive root of $p_2$ and define an integer $u$ by $\varepsilon \equiv \alpha^{(p^2-1)/3} \mod p_2$. Then $(u, r) = 1$ holds and $3 \mid I(p_2)$ implies $3r \mid p^2-1$ and hence $3 \mid p^2-1$. Thus we have $\varepsilon \equiv (\alpha^{(u^2-1)/3})^{r} \mod p_2$. This means that $x^3 - \varepsilon \equiv 0 \mod p_2$ has a root and hence $p_2$ is completely decomposable in $F_0(\sqrt{d})$. Conversely, suppose that $p_2$ decompose completely in $F_0(\sqrt{d})$; then there is an element $\beta \in O_F$ such that $\beta \equiv \varepsilon \mod p_2$, which yields $\varepsilon^{(u^2-1)/3} \equiv \beta^{r^2-1} \mod p_2$. It means $r \mid (p^2-1)/3$. Since $#E(p_2) = r$ or $2r$ according as $r$ is even or odd, we have $#E(p_2) \mid (p^2-1)/3$, that is $3 \mid I(p_2)$. The condition $3 \mid p+1$ implies $3I(p_1)|I(p_2)$ by Proposition 3.1.

Lemma 3.5. Suppose that $F$ is pure cubic and that almost all prime ideals of degree 2 of $F_0$ decompose completely in $F_0(\sqrt{d})$; then there is an element $f \in F_0$ such that $f^3 = \varepsilon' / \varepsilon$.

Proof. By Lemma 1.7, we have only to prove that $x^3 - \varepsilon'$ is reducible over $F_0(\sqrt{d})$.

We claim that for an automorphism $\rho \in \text{Gal}(K(3)/\mathbb{Q})$, the order of $\rho$ is two if the order of $\rho_{e_0}$ is two. Suppose that the order of $\rho_{e_0}$ is two; take a prime ideal $\mathfrak{P}$ of $K(3)$ such that $\rho = (((K(3)/\mathbb{Q})/\mathfrak{P})$. By the assumption the order of $\rho_{e_0} = ((F_0/\mathbb{Q})/\mathfrak{P} \cap F_0)$ is two and then $p := \mathfrak{P} \cap F_0$ is of
degree 2. By the assumption of the lemma, we may suppose that \(p\) decomposes completely in \(F_0(\sqrt[3]{e})\). Take an automorphism \(\eta \in Gal(F_0/\mathbb{Q})\) so that \(e' = \eta(e)\); then \(\eta^{-1}(p)\) is also a prime ideal of degree 2 of \(F_0\) and hence \(\eta^{-1}(p)\) decomposes completely in \(F_0(\sqrt[3]{e'})\) and so \(p\) decomposes completely in \(F_0(\sqrt[3]{e'})\). Thus \(p\) decomposes completely in \(K(3) = F_0(\sqrt[3]{e}) \cdot F_0(\sqrt[3]{e'})\). Therefore the degree of \(\mathfrak{P}\) is two and the order of \(\rho\) is also two. We have shown the claim.

Now choose automorphisms \(\rho_1, \rho_2 \in Gal(K(3)/\mathbb{Q})\) such that the order of \(\rho_1|_{\mathfrak{P}_0}\), \(\rho_2|_{\mathfrak{P}_0}\) is two and the order of \((\rho_1\rho_2)|_{\mathfrak{P}_0}\) is three. \((\rho_2\rho_1)|_{\mathfrak{P}_0} = id.\) implies \(Gal(K(3)/\mathbb{Q}(\sqrt[3]{-3})) = \langle Gal(K(3)/F_0), \rho_2\rho_1 \rangle\). Let us show that \(Gal(K(3)/\mathbb{Q}(\sqrt[3]{-3}))\) is abelian. Take any element \(\kappa \in Gal(K(3)/F_0)\); then the order of \((\rho_1\kappa)|_{\mathfrak{P}_0}\) is two and hence by the claim above the order of \(\rho_1\kappa \kappa^{-1}\) is also two. Therefore \(\rho_1\kappa \kappa^{-1} = \kappa^{-1}\) holds for \(i = 1, 2\) and hence \(\rho_1\kappa \rho_1 = \rho_2\kappa \rho_2\) follows. Since the order of \(\rho_i\) is two, it implies \(\rho_2\rho_1 = \kappa \rho_2 \rho_1\), that is \(Gal(K(3)/F_0)\) is commutative with \(\rho_2\rho_1\), and moreover \(K(3)/F_0\) is a Kummer extension. Hence \(Gal(K(3)/\mathbb{Q}(\sqrt[3]{-3}))\) is abelian and hence so is \(Gal(\mathbb{Q}(\sqrt[3]{-3}, \sqrt[3]{e})/\mathbb{Q}(\sqrt[3]{-3}))\). Since there is an automorphism \(\rho \in Gal(F_0/\mathbb{Q})\) such that \(\rho(e) = e'\) and \(\rho(\sqrt[3]{-3}) = \sqrt[3]{-3}\), \(e\) and \(e'\) are conjugate over \(\mathbb{Q}(\sqrt[3]{-3})\). Thus \(\sqrt[3]{e} \in \mathbb{Q}(\sqrt[3]{-3}, \sqrt[3]{e}) \subset F_0(\sqrt[3]{e})\) holds and \(x^3 - e'\) is reducible over \(F_0(\sqrt[3]{e})\).

**Lemma 3.6.** Suppose that \(F\) is pure cubic and there is an element \(f \in F_0\) such that \(f^3 = e'/e\); then for an automorphism \(\rho \in Gal(F_0(\sqrt[3]{e})/\mathbb{Q})\), the order of \(\rho\) is two if the order of \(\rho|_{\mathfrak{P}_0}\) is two.

**Proof.** We note that the existence of the element \(f\) implies that \(F_0(\sqrt[3]{e})/\mathbb{Q}\) is a Galois extension. Let \(j\) be the complex conjugation and define an automorphism \(\eta \in Gal(F_0(\sqrt[3]{e})/F_0)\) by \(\eta(\sqrt[3]{e}) = \zeta_3 \sqrt[3]{e}\), where \(\sqrt[3]{e}\) is supposed to be real. Then we have

\[
j \eta j(\sqrt[3]{e}) = j(\sqrt[3]{e}) = j(\zeta_3 \sqrt[3]{e}) = \zeta_3^2 \sqrt[3]{e} = \eta^{-1}(\sqrt[3]{e})
\]

and hence \(j \eta j = \eta^2 = \eta^{-1}\). Assume that for an element \(\rho \in Gal(F_0(\sqrt[3]{e})/\mathbb{Q})\), the order of \(\rho|_{\mathfrak{P}_0}\) is two. Since both \(\rho|_{\mathfrak{P}_0}\) and \(j|_{\mathfrak{P}_0}\) are of order 2, there exists some \(u \in Gal(F_0(\sqrt[3]{e})/\mathbb{Q})\) such that \((u \rho u^{-1})|_{\mathfrak{P}_0} = j|_{\mathfrak{P}_0}\) and hence \(u \rho u^{-1} = \eta^b\) for an integer \(b\). Now we obtain \(u \rho^2 u^{-1} = j \eta^b j \eta^b = \eta^{-b} \eta^b = id.,\) and hence \(\rho^2 = id..\)
Proposition 3.3. The following two assertions are equivalent.

(i) Let $p$ be a prime number such that $p$ is unramified in $F_0$ and $(p) = p_1p_2$ in $F$ with prime ideals $p_i$ of degree 1. Then $3I(p_1)$ divides $I(p_2)$.

(ii) $F$ is pure cubic and $F_0(\sqrt[3]{2})/\mathbb{Q}$ is a Galois extension.

Proof. (i) $\Rightarrow$ (ii). By Lemma 3.3, $F$ is pure cubic. Suppose that $p$ is a prime ideal of degree 2 of $F_0$. Let $p$ be a prime number lying below $p$ and assume that $p$ is odd and unramified in $F_0$. The Frobenius automorphism corresponding to $p$ in $Gal(F_0/\mathbb{Q})$ is of order two and its restriction to $\mathbb{Q}(\sqrt[3]{3})$ is also of order two, which yields that $p$ remains prime in $\mathbb{Q}((\sqrt[3]{-3})$ and hence by Lemma 1.1, $(p) = p_1p_2$ in $F$ holds for prime ideals $p_i$ of degree 1. Taking a conjugate ideal of $p$ if necessary, we assume $p_2 = p \cap F$; then $3I(p_1) | I(p_2)$ and therefore by virtue of Lemma 3.4, $p_2$ is completely decomposable in $F_0(\sqrt[3]{2})$ and hence so is $p$. Lemma 3.5 yields that $F_0(\sqrt[3]{2})/\mathbb{Q}$ is a Galois extension.

(ii) $\Rightarrow$ (i). Let $p$, $p_1$, $p_2$ be those in (i). Let $\mathfrak{P}$ be a prime ideal of $F_0(\sqrt[3]{2})$ lying above $p_2$ and set $\mathfrak{p} = (F_0(\sqrt[3]{2})/\mathbb{Q})/\mathfrak{P}$. Since $\mathfrak{P} \cap F = p_2$ and the degree of $p_2$ is two, the order of $\rho_{\mathfrak{P}}$ is two. By Lemma 3.6, the order of $p$ is also two, which means that the order of $\mathfrak{P}$ is two. Thus we have shown that $p_2$ is completely decomposable in $F_0(\sqrt[3]{2})$ and Lemma 3.4 yields $3I(p_1) | I(p_2)$.  

It may be interesting to look for an analogue for general algebraic number fields.

Example. Let $F$ be $\mathbb{Q}(\sqrt{2})$. Then it is easy to see $\varepsilon = \sqrt[3]{2} - 1$ and $\varepsilon' = \omega \sqrt[3]{2} - 1$ with $\omega = (-1 + \sqrt[3]{-3})/2$. Then $\varepsilon/\varepsilon' = \eta^3$ for $\eta := (1 - \sqrt[3]{2} + \sqrt[3]{2^2} + \omega(2 + \sqrt[3]{2} - \sqrt[3]{2^2}))/3$ holds and hence $F_0(\sqrt[3]{2})/\mathbb{Q}$ is a Galois extension.

We define by $\mathcal{P}(x)$ in this section the set of prime ideals $p$ of degree 2 in $F$ such that the prime number $p$ lying below $p$ is less than $x$, is odd and is unramified in $F_0$. For a prime ideal $p_2 \in \mathcal{P}(x)$, $p_1$ denotes a prime ideal of degree 1 such that $p_2p_1$ is the decomposition in $F$ of the prime number lying below $p_2$. $I(p_2)$ is divisible by $\delta_{p_2}(p_1)$. We set

\[ N(x) := \# \{ p_2 \in \mathcal{P}(x) | I(p_2) = \delta_{p_2}(p_1) \}, \]
\[ N(x, \eta) := \# \{ p_2 \in \mathcal{P}(x) | q \not| (I(p_2)/\delta_{p_2}(p_1)) \text{ for } q \leq \eta \}, \]
\[ M(x, \eta_1, \eta_2) := \# \{ p_2 \in \mathcal{P}(x) | q \not| (I(p_2)/\delta_{p_2}(p_1)) \text{ for } \eta_1 \leq q \leq \eta_2 \}, \]
\[ P(x, n) := \# \{ p_2 \in \mathcal{P}(x) | n \not| (I(p_2)/\delta_{p_2}(p_1)) \}, \]
where \( q \) stands for prime numbers. For \( \zeta_1 = 6^{-1} \log x \), we have, as in the second section

\[
N(x) = N(x, \zeta_1) + O(M(x, \zeta_1, x))
\]

\[
= \sum_{n|Q(\zeta_1)} \mu(n) P(x, n) + O(M(x, \zeta_1, x)),
\]

where \( Q(\zeta_1) \) is the product of all prime numbers less than \( \zeta_1 \).

Now we define conjugacy classes:

For an odd integer \( n \), we set

\[
C(n) := \{ \rho \in \text{Gal}(K(n)/\mathbb{Q}) \mid \rho^2 = \text{id., } \rho(\sqrt{d}) = -\sqrt{d} \text{ and } \rho(\zeta_n) = \zeta_n^{-1} \}.
\]

For an even integer \( n \) and an integer \( k \), we set

\[
C(n, k) := \{ \rho \in \text{Gal}(K(2^k n)/\mathbb{Q}) \mid \rho^2 = \text{id., } \rho(\sqrt{d}) = -\sqrt{d}, \rho(\zeta_n) = \zeta_n^{-1} \text{ and } \rho(\zeta_{2^k+2}) = -\zeta_{2^k+2} \},
\]

where we note \( \zeta_{2^k+2} \in K(2^k n) \).

**Lemma 3.7.** We have

(i) for an odd square-free integer \( n \),

\[
P(x, n) = \pi_{C(d_F n)}(x, K(\delta_F n)/\mathbb{Q}) + O(\omega(n)),
\]

(ii) for an even square-free integer \( n \),

\[
P(x, n) = \sum_{0 \leq k \leq \log x/\log 2 - 1} \pi_{C(\delta_F n, k)}(x, K(2^k \delta_F n)/\mathbb{Q}) + O(\omega(n)).
\]

**Proof.** First, we note that the number of prime numbers ramified in \( K(n) \) is \( O(\omega(n)) \), since they divide \( nd(F_0) \). Let \( p \) be an odd prime \( \leq x \) and relatively prime to \( nd(F_0) \) and suppose that \( p \) decomposes as \( (p) = p_1 p_2 \) in \( F \) with prime ideals \( p_i \) of degree \( i \). For a square-free integer \( n \), such a prime ideal \( p_2 \) contributes to \( P(x, n) \), i.e., \( \delta_F n I(p_1) | I(p_2) \) if and only if \( \delta_F n | p+1 \) and either \( \delta_F n | I(p_2) \) if \( 2 \nmid n \) or \( 2^{ord_2((p-1)/2)} \delta_F n | I(p_2) \) if \( 2 | n \). By virtue of Proposition 3.1, since the condition \( \delta_F n | p+1 \) is equivalent to \( \delta_F n = \zeta_n^{-1} \), Proposition 3.2 completes the proof if \( n \) is odd. Suppose that \( n \) is even; set \( k = ord_2((p-1)/2) \) and let \( \rho \in \text{Gal}(K(2^k \delta_F n)/\mathbb{Q}) \) be the Frobenius automorphism corresponding to the prime \( p \). Then \( \delta_F n I(p_1) | I(p_2) \) is equivalent to \( \delta_F n | p+1 \) and \( 2^k \delta_F n | I(p_2) \) by Proposition 3.1, which is furthermore
equivalent to $\delta_{p} | p+1$, $\rho^{2} = id.$ and $\rho(\sqrt{d}) = -\sqrt{d}$ by Proposition 3.2. $2^{k+1} | p-1$ is equivalent to $\rho(\zeta_{2^{k+1}}) = \zeta_{2^{k+1}}$ but $\rho(\zeta_{2^{k+1}}) \neq \zeta_{2^{k+1}}$, i.e., $\rho(\zeta_{2^{k+1}}) = -\zeta_{2^{k+1}}$. $2^{k+1} \leq p-1 \leq x$ implies $k \leq \log x / \log 2 - 1$. These complete the proof in case of $2 | n$. 

Taking Lemma 3.7 into account, we conjecture
\[N(x) = c_{0} \log x + O \left( \frac{x}{(\log x)^{2}} \right),\]
where
\[c_{0} := \sum_{n \text{ odd}} \frac{\mu(n) \#C(\delta_{p} n)}{[K(\delta_{p} n) : \mathbb{Q}]} + \sum_{n \text{ even}} \frac{\mu(n) \#C(\delta_{p} n, k)}{[K(2^{k} \delta_{p} n) : \mathbb{Q}]}\]

**Remark.** When $\delta_{p} = 1$, $P(x, 1) = \#P(x) = \#P_{1, 2}(x)$ in Section 2 = $1/2$. $\log x + \text{error urges } \#C(1)/[K(1) : \mathbb{Q}] = 1/2$.

We can show $c_{0} > 0$ by evaluating $\#C(n), \#C(n, k)$. But it is not simple. $c_{0} > 0$ suggests that the lower bound $\delta_{p} I(p_{1})$ for $I(p_{2})$ is good. $c_{0}$ is a rational number times the Artin constant.

### 4. Prime Ideals of Degree 3

**Lemma 4.1.** Let $p$ be an odd prime which remains prime in $F$ and is unramified in $F_{0}$. Then we have
\[\varepsilon^{2^{k+1}+p+1} \equiv 1 \mod (p - 1)/2\]
and the order $r$ of $\varepsilon \mod (p)$ is odd and divides $p^{2} + p + 1$, and $E(\varepsilon(p)) \neq \langle \varepsilon \mod (p) \rangle$.

**Proof.** Let $\mathfrak{P}$ be a prime ideal of $F_{0}$ lying above $p$ and set $p = \mathfrak{P} \cap F = (p)$. Since $\mathfrak{P}$ is of degree 3, $\rho = ((F_{0}/\mathbb{Q})/\mathfrak{P})$ is of order 3. Then we have $1 = N_{P/Q}(\varepsilon) = \rho^{2}(\varepsilon) \rho(\varepsilon) \equiv \varepsilon^{2^{k+1}+p+1} \mod \mathfrak{P}$. Therefore $r$ divides $p^{2} + p + 1$ and hence $r$ is odd. If $E(\varepsilon(p)) = \langle \varepsilon \mod (p) \rangle$, then $-1 \equiv \varepsilon^{t} \mod (p)$ holds for some integer $t$, which contradicts $r$ being odd. Thus we have $#E(p) = 2r | 2(p^{2} + p + 1)$ and $I((p)) = (p^{2} - 1)/#E(p) \equiv 0 \mod (p - 1)/2$. 

**Lemma 4.2.** Let $p$ be as in Lemma 4.1. Then we have
\[\#E((p)), p - 1 = 2 \quad \text{or} \quad 6.\]
Proof. Let \( r \) be the order of \( \varepsilon \mod (p) \) in \((O_2/(p))^{*}\). For \( q = (r, p-1) \), \( q \mid r \mid p^2 + p + 1 \) is clear. Then \( q \mid p-1 \) implies \( p^2 + p + 1 \equiv 3 \mod q \) and from these follows \( q \mid 3 \). Hence \((2r, p-1) \mid 6 \) holds.

Lemma 4.3. Let \( p \) be as in Lemma 4.1. Then \((#E((p)), p-1) = 6 \) if and only if \( p \equiv 1 \mod 3 \) and \( \varepsilon^{(p^2 + p + 1)/3} \equiv 1 \mod (p) \) holds. \((#E((p)), p-1) = 2 \) holds if and only if either \( p \equiv 2 \mod 3 \) or both \( p \equiv 1 \mod 3 \) and \( 3(p-1)/2 \equiv I((p)) \).

Proof. By virtue of the previous lemma, \((#E((p)), p-1) = 6 \) if and only if \( p \equiv 1 \mod 3 \) and \( #E((p)) \equiv 0 \mod 3 \). Suppose, first \( p \equiv 1 \mod 3 \) and \( #E((p)) \equiv 0 \mod 3 \). We assume \( \varepsilon^{(p^2 + p + 1)/3} \equiv 1 \mod (p) \). Let \( r \) be the order of \( \varepsilon \mod (p) \); then \( r \equiv 0 \mod 3 \) holds and the assumption yields \( 3 \mid r \mid (p^2 + p + 1)/3 \) and hence \( p^2 + p + 1 \equiv 0 \mod 9 \) holds. This is a contradiction, because \( p \equiv 1 \mod 3 \) implies \( p^2 + p + 1 \equiv 3 \mod 9 \). Conversely suppose \( p \equiv 1 \mod 3 \) and \( \varepsilon^{(p^2 + p + 1)/3} \not\equiv 1 \mod (p) \). By Lemma 4.1, we know \( \varepsilon^{p^2 + p + 1} \equiv 1 \mod (p) \) and hence the order of \( \varepsilon \mod (p) \) is divisible by 3, and so \( 3 \mid #E((p)) \) holds and then we have \( (#E((p)), p-1) = 6 \). Now \((#E((p)), p-1) = 2 \) is clearly equivalent to either \( p \equiv 1 \mod 3 \) and \( \varepsilon^{(p^2 + p + 1)/3} \equiv 1 \mod (p) \) or \( p \equiv 2 \mod 3 \). Hence we have only to show, under the assumption \( p \equiv 1 \mod 3 \) the condition \( \varepsilon^{(p^2 + p + 1)/3} \equiv 1 \mod (p) \) is equivalent to \( 3(p-1)/2 \mid I((p)) \). Assume \( p \equiv 1 \mod 3 \) and set \( n = 3(p-1)/2 \). First suppose \( n \mid I((p)) \); then Lemma 1.13 implies \( \alpha^n = \varepsilon \) for some \( \alpha \in F_p \) and hence \( \varepsilon^{(p^2 + p + 1)/3} \equiv 1 \mod (p) \), which is nothing but \( \varepsilon^{2(p^2 + p + 1)/3} \equiv 1 \mod (p) \) since \( r \) is odd. Conversely suppose \( \varepsilon^{(p^2 + p + 1)/3} \equiv 1 \mod (p) \). Since \( 2(p^2 + p + 1)/3 = (p^2 - 1)/n \) divides \( p^3 - 1 \), we have \( \varepsilon \equiv \alpha^n \mod (p) \) for some \( \alpha \in O_F \). Moreover the additional condition \( (p^3 - 1)/(2n) = (p^2 + p + 1)/3 \in \mathbb{Z} \) yields \( n \mid I((p)) \) by Lemma 1.13.

Lemma 4.4. Let \( p \) be as in Lemma 4.1, and \( \mathfrak{P} \) a prime ideal of \( K(3) \) lying above \( p \) and set \( p = ((K(3)/\mathfrak{Q})/\mathfrak{P}) \). If \( p \equiv 2 \mod 3 \), then \((#E((p)), p-1) = 2 \) holds. Suppose \( p \equiv 1 \mod 3 \); then setting \( \Omega := (1 + \varepsilon^{1/3} + \varepsilon^{2/3})^{1/3} \varepsilon^{1/3} \), we have \((#E((p)), p-1) = 2 \) if and only if \( \rho(\Omega) = \Omega \).

Proof. The first assertion follows clearly from Lemma 4.2. Hereafter we assume \( p \equiv 1 \mod 3 \). Since \( \mathfrak{P} \cap F_p \) is of degree 3 by the assumption on \( p \), \( \mathfrak{P} \cap F_p \) is also of degree 3 and hence \( \rho(\mathfrak{P} \cap F_p) \) is of order 3 and \( \rho(\varepsilon) = \varepsilon' \) or \( \varepsilon'' \). \( \rho(\varepsilon_1) = \varepsilon_1 \) is clear, and the condition \( \rho(\Omega) = \Omega \) is independent of the choice of the third root of \( \varepsilon' / \varepsilon \). We set \( \omega := \sqrt[3]{\varepsilon} \rho(\sqrt[3]{\varepsilon}) \rho^2(\sqrt[3]{\varepsilon}) \), which is a third
root of unity. First we assume \( \rho(\varepsilon) = \varepsilon' \) and \( \sqrt[3]{\varepsilon'/\varepsilon} = \rho(\sqrt[3]{\varepsilon})/\sqrt[3]{\varepsilon} \). Set \( f = \rho(\sqrt[3]{\varepsilon})/\sqrt[3]{\varepsilon} \); then \( \rho(f) = f \omega / \rho(\varepsilon) \) follows, which implies \( \rho^2(f) = \varepsilon f / \omega \) and hence \( \varepsilon = \omega \rho^2(f) / f \). We see
\[
\rho(\Omega) = (1 + \varepsilon \rho(\varepsilon) + \rho(\varepsilon)) \rho(f) \\
= (1 + \varepsilon \rho(\varepsilon) + \rho(\varepsilon)) f \omega / \rho(\varepsilon) \\
= (\varepsilon \rho^2(\varepsilon) + \varepsilon + 1) f \omega \\
= \Omega \omega.
\]
On the other hand, we have by \( f \equiv \varepsilon^{(p-1)/3} \mod \mathfrak{p} \)
\[
\varepsilon^{(p+1)/3} \equiv (\omega f^{(p-1)}(p^2+p+1)/3) \mod \mathfrak{p} \\
\equiv \omega(\varepsilon^{p^2+p+1}((p-1)/3)(p+1) \mod \mathfrak{p}) \\
\equiv \omega \mod \mathfrak{p},
\]
since \( \varepsilon^{p^2+p+1} \equiv 1 \mod \mathfrak{p} \) by Lemma 4.1. Now we find by Lemma 4.3, \( \#E((p), p-1) = 6 \) holds if and only if \( \omega \neq 1 \) holds. Therefore \( \#E((p), p-1) = 2 \) if and only if \( \omega = 1 \). It completes the proof in case of \( \rho(\varepsilon) = \varepsilon' \). In case of \( \rho(\varepsilon) = \bar{\varepsilon}' \), the conjugate \( \rho' := j \rho j \) by the complex conjugation \( j \), \( \rho'(\varepsilon) = \varepsilon' \) holds. By the above, \( \#E((p), p-1) = 2 \) if and only if \( \sqrt[3]{\varepsilon} \rho'(\sqrt[3]{\varepsilon}) \rho^2(\sqrt[3]{\varepsilon}) = 1 \), which is equivalent to \( \sqrt[3]{\varepsilon} \rho(\sqrt[3]{\varepsilon}) \rho^2(\sqrt[3]{\varepsilon}) = 1 \). Taking \( \rho^2(\sqrt[3]{\varepsilon})/\sqrt[3]{\varepsilon} \) as \( \sqrt[3]{\varepsilon'/\varepsilon} \), we see easily \( \rho(\Omega) = (\sqrt[3]{\varepsilon} \rho(\sqrt[3]{\varepsilon})) \rho^2(\sqrt[3]{\varepsilon}) \Omega \). Thus again we find that \( \#E((p), p-1) = 2 \) is equivalent to \( \rho(\Omega) = \Omega \).

**Remark.** The proof shows that for \( \Omega = (1 + \varepsilon \bar{\varepsilon}' + \varepsilon') \sqrt[3]{\varepsilon'/\varepsilon} \) and an automorphism \( \rho \in \text{Gal}(K(3)/\mathbb{Q}) \) such that \( \rho(\zeta_3) = \zeta_3 \) and \( \rho(\varepsilon) = \varepsilon' \) or \( \bar{\varepsilon}' \), \( \omega := \sqrt[3]{\varepsilon} \rho(\sqrt[3]{\varepsilon}) \rho^2(\sqrt[3]{\varepsilon}) \) is a third root of unity and \( \rho(\Omega)/\Omega = \omega \) or \( \omega^2 \) according to \( \rho(\varepsilon) = \varepsilon' \) or \( \bar{\varepsilon}' \).

**Lemma 4.5.** Let \( p \) be as in Lemma 4.1, and suppose that \( p \) is unramified in \( K(n) \). We consider the three conditions

(i) \( p^2 + p + 1 \equiv 0 \mod n \),

(ii) a prime ideal of \( F_0(\zeta_{2n}) \) lying above \( p \) decomposes completely in \( K(n) \),

(iii) \( 3 \nmid n \).

Then \( n(p-1)/2 | I((p)) \) holds if and only if (i) and (ii) hold in case of \( \#E((p), p-1) = 2 \), and (i), (ii), and (iii) hold in case of \( \#E((p), p-1) = 6 \), respectively.
Proof. Suppose \( n(p-1)/2 | I((p)) \), and denote by \( r \) the order of \( \varepsilon \mod (p) \) and set \( t = I((p))/(n(p-1)/2) \in \mathbb{Z} \). Since \( (p^2+p+1)/n = (p^3-1)/(n(p-1)) = I((p))/\#E((p))/(n(p-1)) = t\#E((p))/2 \) is an integer, \( n \) divides \( p^2+p+1 \), which is the condition (i). Take a generator \( \alpha \in \mathcal{O}_F \) of \( \mathcal{O}_F/(p) \times \) and set \( t = I((p))/(n(p-1)/2) \zeta_n \). Since \( (p^2+1)/n = (p^3-1)/(n(p-1)) = I((p)) \#E((p))/(n(p-1)) = t\#E((p))/2 \) is an integer, \( n \) divides \( p^2+p+1 \), which is the condition (i). Take a generator \( a \in \mathcal{O}_F \) of \( \mathcal{O}_F/(p) \times \) and write \( e = a^{u(p^3-1)/r} \mod (p) \) for an integer \( u \) with \((u,r)=1\). On the other hand, \( p^3-1 = I((p)) \#E((p)) = 0 \mod n(p-1)/2 \cdot r \) holds and hence \( p^3-1 = nrw \) follows for some integer \( w \). Then we have

\[
\varepsilon \equiv \alpha^{unw} \mod (p) \equiv (\alpha^{unw})^\ast \mod (p),
\]

and hence \( x^\ast = \varepsilon \) is solvable over \( F_{(p)} \) since \( p \nmid n \). Thus the condition (ii) holds. Now we assume \((\#E((p)), p-1) = 6 \) moreover. By the assumption, we have \( p^2+p+1 = 3 \mod 9 \) and \( \#E((p)) = 0 \mod 3 \). Then \( 2(p^2+p+1) = nt\#E((p)) \) yields \( 3 \nmid n \). Conversely we assume the conditions (i), (ii). Let \( \Psi \) be a prime ideal of \( K(n) \) lying above \( p \). Since \( p^3-1 = (p-1)(p^2+p+1) = 0 \mod 2n \), the degree of \( \Psi \) is one or three. By the assumption on \( p \), the degree of \( \Psi \) and then of \( \Psi \) are three and hence in \( K(n) \) the closures of \( F \) and \( F_0(\zeta_{2n}) \) coincide. On the other hand, the condition (ii) yields that \( x^\ast = \varepsilon \) is solvable in the closure of \( F_0(\zeta_{2n}) \) in \( K(n) \). Therefore \( x^\ast = \varepsilon \) mod \( \mathcal{O}_F/(p) \) has a solution, since \( \mathcal{O}_F/(p) \equiv \mathcal{O}_{F_0(\zeta_{2n})}/\Psi \cap F_0(\zeta_{2n}) \). Let \( \alpha \in \mathcal{O}_F \) be a generator of \( \mathcal{O}_F/(p) \); then there is an integer \( u \) such that \( (\alpha^u)^\ast = \varepsilon \mod (p) \). Hence we have \( unr \equiv 0 \mod p^3-1 \) for the order \( r \) of \( \varepsilon \mod (p) \), and then \( unr = w(p^3-1) \) for an integer \( w \) with \((r,w)=1\).

We recall \( r \) is odd and \( \#E((p)) = 2r \).

In case of \((\#E((p)), p-1) = 2 \), the conditions \((2r, p-1) = 2 \) and \( 2 \nmid r \) imply \( (r, p-1) = 1 \) and hence \( (r, w(p-1)) = 1 \). Then \( ur = w(p-1) \) \( (p^2+p+1)/n \in \mathbb{Z} \) yields \( r \mid (p^2+p+1)/n \), which induces the desired equation \( 2I((p))/(n(p-1)) = (p^2+p+1)/(nr) \in \mathbb{Z} \).

In case of \((\#E((p)), p-1) = 6 \), we assume \( 3 \nmid n \) moreover. By virtue of \((2r, p-1) = 6 \), we set \( r = 3r' \) and then \((r', (p-1)/3) = 1 \) and similarly to the above, \( ur' = w(p-1)/3 \cdot (p^2+p+1)/n \) yields \( r' \mid (p^2+p+1)/n \). Hence \( 6I((p))/(p-1) = (p^2+p+1)/(nr') \) \( \in \mathbb{Z} \) holds. Thus we have \( n(p-1)/6 \mid I((p)) \). To show \( n(p-1)/2 \mid I((p)) \), we have only to see \( \text{ord}_3(n(p-1)/2) \leq \text{ord}_3(I((p))) \).

by virtue of Lemma 4.1. Thus we have completed the proof.

Remark. An integer \( n \) which satisfies the condition (i) is odd.

Proposition 4.1. Let \( n \) be a positive integer and let \( p \) be an odd prime number such that \( p \) is unramified in \( K(n) \). Then the following (i), (ii) are equivalent:
(i) \( p \) remains a prime ideal in \( F \) and \( n(p-1)/2 \mid I((p)) \).

(ii) Let \( \mathfrak{P} \) be a prime ideal of \( K(n) \) lying above \( p \) and set \( \rho := ((K(n)/Q)/\mathfrak{P}) \). Then we have

(ii.1) \( \rho^3 = id. \),

(ii.2) \( \rho_{\mathfrak{P} \cap F} \neq id. \),

(ii.3) \( \rho(\zeta_n) = \zeta_n^a \) for an integer \( a \) satisfying \( a^2 + a + 1 \equiv 0 \mod n \),

(ii.4) if \( 3 \mid n \), then \( \rho(\Omega) = \Omega \) holds, where \( \Omega := (1 + \varepsilon e + e) \sqrt[3]{\varepsilon} \).

Proof. (i) \( \Rightarrow \) (ii). Since \( p \) remains prime in \( F \), the degree of \( \mathfrak{P} \cap F \) is three and hence the order of \( \rho_{\mathfrak{P} \cap F} \) is three and then (ii.2) holds. By Lemma 4.5, we have \( p^3 + p + 1 \equiv 0 \mod n \), which implies (ii.3) for \( a = p \).

Since \( p^3 \equiv 1 \mod n \), we find that the order of \( \rho_{\mathfrak{P} \cap F} \) is three. By Lemma 4.5, \( \mathfrak{P} \cap K(n)/F \) is completely decomposable in \( K(n)/F \) and hence the degree of \( \mathfrak{P} \) is three and then the order of \( \rho \) is also three, which yields (ii.1). Suppose \( 3 \mid n \); then \( (#E((p)), p−1) = 2 \) occurs by virtue of Lemma 4.5. If \( p \equiv 2 \mod 3 \), then \( \rho(\zeta_3) = \zeta_3^{-1} \) holds, which contradicts (ii.3). Therefore we have \( p \equiv 1 \mod 3 \), and then Lemma 4.4 yields \( \rho(\Omega) = \Omega \), i.e., (ii.4).

(ii) \( \Rightarrow \) (i). We assume the condition (ii). (ii.3) and \( \rho(\zeta_n) = \zeta_n^a \) implies \( a \equiv p \mod n \) and hence \( p^2 + p + 1 \equiv 0 \mod n \). The conditions (ii.1) and (ii.2) yield that \( p \) remains prime in \( F \), and in \( K(n)/F \) the prime ideals lying above \( p \) are completely decomposable. If, hence \( (#E((p)), p−1) = 2 \), then Lemma 4.5 implies \( n(p−1)/2 \mid I((p)) \). Suppose \( (#E((p)), p−1) = 6 \). Since \( p \equiv 1 \mod 3 \), the supposition yields \( \rho(\Omega) \neq \Omega \) by Lemma 4.4. The condition (ii.4) implies \( 3 \nmid n \) and \( n(p−1)/2 \mid I((p)) \) by virtue of Lemma 4.5.

Lemma 4.6. If \( F \) is not pure cubic, there exist infinitely many prime numbers \( p \) such that \( p \) remains a prime ideal in \( F \) and \( 3(p−1)/2 \mid I((p)) \).

Proof. Suppose that \( F \) is not pure cubic. Since \( F_0 \) does not contain \( \sqrt[3]{−3} \), there is an element \( \rho \) of \( \text{Gal}(F_0(\sqrt[3]{−3})/Q) \) such that \( \rho_{\mathfrak{P} \cap F_0} \neq id. \) and the order of \( \rho_{\mathfrak{P} \cap F_0} \) is three. Let \( \mathfrak{P} \) be a prime ideal of \( F_0(\sqrt[3]{−3}) \) whose Frobenius automorphism is \( \rho \). Then the degree of \( \mathfrak{P} \cap F_0 \) (resp. \( \mathfrak{P} \cap Q(\sqrt[3]{−3}) \)) is three (resp. two) and hence the prime number lying below \( \mathfrak{P} \) remains a prime ideal in \( F \) and \( Q(\sqrt[3]{−3}) \). Hence we have \( p \equiv 2 \mod 3 \) and

\[
\frac{2(p^2 + p + 1)}{I((p))/((p−1)/2)} = #E((p)) \in \mathbb{Z}.
\]

Since \( I((p))/((p−1)/2) \) is an integer by Lemma 4.1, it divides \( 2(p^2 + p + 1) \). On the other hand, \( p \equiv 2 \mod 3 \) implies \( p^2 + p + 1 \not\equiv 0 \mod 3 \) and hence 3 does not divide \( I((p))/((p−1)/2) \).
Lemma 4.7. If \( F \) is pure cubic and \( F_0(\sqrt[3]{\alpha})/\mathbb{Q} \) is a Galois extension, then a prime ideal of \( F_0 \) of degree 3 decomposes completely in \( F_0(\sqrt[3]{\alpha}) \).

Proof. Since \([F_0(\sqrt[3]{\alpha}) : \mathbb{Q}] = 18\), the 3-Sylow subgroup of \( \text{Gal}(F_0(\sqrt[3]{\alpha})/\mathbb{Q}) \) is isomorphic to \((\mathbb{Z}/3\mathbb{Z})^2 \) or \( \mathbb{Z}/9\mathbb{Z}\). We show \((\mathbb{Z}/3\mathbb{Z})^2\) is valid. To do it, suppose that the subgroup is cyclic; then there exists an automorphism \( \rho \in \text{Gal}(F_0(\sqrt[3]{\alpha})) \) whose order is 9. Hence the order of \( \rho_{\alpha_3} \) is three. Taking a conjugate of \( \rho \) if necessary, we may assume \( \rho(\alpha) = \alpha' \), \( \rho^2(\alpha) = \alpha'' \). Fix third roots \( \sqrt[3]{\alpha}, \sqrt[3]{\alpha'}, \sqrt[3]{\alpha''} \) so that \( \sqrt[3]{\alpha} \sqrt[3]{\alpha'} \sqrt[3]{\alpha''} = 1 \), we set \( \rho(\sqrt[3]{\alpha}) = \eta_1 \sqrt[3]{\alpha'}, \rho(\sqrt[3]{\alpha'}) = \eta_2 \sqrt[3]{\alpha'} \), \( \rho(\sqrt[3]{\alpha''}) = \eta_2 \sqrt[3]{\alpha''} \) for third roots \( \eta_1, \eta_2 \) of unity. Since \( \rho(\zeta_3) = \zeta_3 \), we have

\[
\rho^2(\sqrt[3]{\alpha}) = \rho(\eta_1 \sqrt[3]{\alpha'}) = \eta_1 \eta_2 \sqrt[3]{\alpha'} = \eta_1 \eta_2 \sqrt[3]{\alpha} \sqrt[3]{\alpha'}^{-1}, \\
\rho^3(\sqrt[3]{\alpha}) = \eta_1 \eta_2(\eta_1 \sqrt[3]{\alpha'} \eta_2 \sqrt[3]{\alpha''}^{-1} = \sqrt[3]{\alpha},
\]

which yields a contradiction that the order of \( \rho \) is three. Let \( p \) be a prime ideal of \( F_0 \) of degree 3, and \( \Psi \) a prime ideal of \( F_0(\sqrt[3]{\alpha}) \) lying above \( p \). The degree of \( \Psi \) is 3 or 9. The Frobenius automorphism \( \rho \) corresponding to \( \Psi \) has order 3 by what we have shown. It means that the order of \( \Psi \) is three and hence \( p \) is completely decomposable. \[\blacksquare\]

Proposition 4.2. The following are equivalent.

(i) If an odd prime number \( p \) remains a prime ideal in \( F \) and is unramified in \( F_0(\sqrt[3]{\alpha}) \), then

\[3(p-1)/2 | I((p))\]

holds.

(ii) \( F \) is pure cubic and \( F_0(\sqrt[3]{\alpha})/\mathbb{Q} \) is a Galois extension.

Proof. (i) \(\Rightarrow\) (ii). By Lemma 4.6, \( F \) is pure cubic. Suppose that \( F_0(\sqrt[3]{\alpha})/\mathbb{Q} \) is not a Galois extension and then \( K(3)/F_0(\sqrt[3]{\alpha}) \) is a cubic extension. Let \( \rho_0 \) be an automorphism in \( \text{Gal}(F_0/\mathbb{Q}) \) such that \( \rho_0(\alpha) = \alpha' \) (and hence \( \rho_0^2(\alpha) = \alpha'' \)). Then \( \rho_0 \) is the identity on \( \mathbb{Q}(\sqrt[3]{\alpha}) = \mathbb{Q}(\zeta_3) \). Since \( K(3)/F_0 \) is a Kummer extension with \( \text{Gal}(K(3)/F_0) \) being isomorphic to \((\mathbb{Z}/3\mathbb{Z})^2\) and \( \rho_0(\sqrt[3]{\alpha}) = \sqrt[3]{\alpha'} = e^{-3}(\sqrt[3]{\alpha})^{-2} \), there is an extension \( \rho \in \text{Gal}(K(3)/\mathbb{Q}) \) of \( \rho_0 \) such that for \( f = \sqrt[3]{\alpha} / \sqrt[3]{\alpha}, \rho(f) = w/e^2 \) for a nontrivial third root \( w \) of unity. By virtue of \( \rho(\zeta_3) = \zeta_3, w = e^2 \rho(f) \) does not
depend on the choice of the third root of \( e \) and hence we have for 
\[
f_1 := \rho(\sqrt[3]{e})/\sqrt[3]{e}, \quad w = \varepsilon f^3, \quad \rho(f_1) = \sqrt[3]{e} \rho(\sqrt[3]{e}) \rho^2(\sqrt[3]{e}).
\] 
Now we take an odd prime integer \( p \) and a prime ideal \( \mathfrak{P} \) of \( K(3) \) lying above \( p \) so that 
\[
\rho = ((K(3)/\mathbb{Q})/\mathfrak{P}). \quad \rho(\zeta) = \zeta_1 \text{ implies } p \equiv 1 \mod 3 \text{ and then Lemma 4.4}
\] 
and the remark after it yield (\( \#E((p)), p-1=6 \). Therefore \( 3 \mid \#E((p)) \) holds, which implies \( \text{ord}_p((I((p))/(p-1)/2)) = \text{ord}_p(2(p^2+p+1)/\#E((p))) \leq 0 \) because \( p \equiv 1 \mod 3 \) implies \( 3 \parallel p^2+p+1 \). Since \( I((p))/(p-1)/2 \) is an integer by Lemma 4.1, we obtain \( 3(p-1)/2 \mid I((p)) \). It contradicts the assumption.

(ii) \Rightarrow (i). Let \( p \) be an odd prime number such that \( p \) remains a prime ideal in \( F \) and unramified in \( F_0(\sqrt[3]{e}) \). For a prime ideal \( \mathfrak{P} \) of \( F_0(\sqrt[3]{e}) \) lying above \( p \), we set 
\[
\rho = ((F_0(\sqrt[3]{e})/\mathbb{Q})/\mathfrak{P}). \quad \rho = \rho(\zeta) \text{ implies } p \equiv 1 \mod 3 \text{ and hence the order of } \rho(\zeta) \text{ is three. By Lemma 4.7, the degree of } \mathfrak{P} \text{ and hence the order of } \rho \text{ is three, too. By virtue of Lemma 1.7, there is an element } f \in F_0 \text{ such that } f^3 = e'/e. \text{ Taking a conjugate of } \mathfrak{P}, \text{ we may assume } \rho(\zeta) = e'. \text{ For the complex conjugation } j, \text{ we have }
\]
\[
(ejf(f))^3 = e' \cdot e / e = 1
\]
and \( ejf(f) \) is real positive and so \( ejf(f) = 1 \). On the other hand, we see 
\[
(p(f) jpf(f))^3 = \rho(e'/e) jpf(e'/e) = e'/e \cdot e' / e = 1
\]
and hence \( p(f) jpf(f) = 1 \), since it is real positive. Now \( \rho^2 = jpf \) on \( F_0 \) implies 
\[
\rho^2(f) = jpf(f) = jpf(e' f) = j(e' \rho(f))^{-1} = \rho(f) / e'
\]
and hence \( e = \rho(e') = \rho(p(f) / \rho^2(f)) = \rho^2(f) / f \) holds. Therefore we have 
\[
e^{(p^2+p+1)/3} \equiv (f^{p-1})^{(p^2+p+1)/3} \mod \mathfrak{P} \equiv (e^{p^2+p+1})(p-1)/(p^2) \mod \mathfrak{P}
\]
by \( f^3 = e'/e \equiv e^{p-1} \mod \mathfrak{P} \). Here, noting \( 1 = N_{F/\mathbb{Q}}(e) = e\rho(e) \rho^2(e) \equiv e^{p^2+p+1} \mod \mathfrak{P} \), we get finally 
\[
e^{(p^2+p+1)/3} \equiv 1 \mod \mathfrak{P}
\]
and hence \( \#E((p)) \mid 2(p^2+p+1)/3 \). It implies 
\[
I((p)) \frac{2(p^2+p+1)/3}{3(p-1)/2} = \frac{\#E((p))}{\#E((p))} \in \mathbb{Z}.
\]
We define a union of conjugacy classes \( C(n) \) of \( \text{Gal}(K(n)/\mathbb{Q}) \) by

\[
C(n) := \left\{ r \in \text{Gal}(K(n)/\mathbb{Q}) \mid \text{ii.1), (ii.2), (ii.3) and (ii.4) in Proposition 4.1} \right\}.
\]

In this section, we denote by \( \mathcal{P}(x) \) the set of prime numbers \( p \) such that \( p \) remains a prime ideal in \( F \) and is unramified in \( F_0 \) and \( p \leq x \). \( I((p)) \) is divisible by \( \delta_F(p-1)/2 \). We set

\[
N(x) := \# \{ (p) \in \mathcal{P}(x) \mid I((p)) = \delta_F(p-1)/2 \},
\]
\[
N(x, \eta) := \# \{ (p) \in \mathcal{P}(x) \mid q^I((p))/\delta_F(p-1)/2 \text{ for } q \leq \eta \},
\]
\[
M(x, \eta_1, \eta_2) := \# \{ (p) \in \mathcal{P}(x) \mid q^I((p))/\delta_F(p-1)/2 \text{ for } \eta_1 < q \leq \eta_2 \},
\]
\[
P(x, n) := \# \{ (p) \in \mathcal{P}(x) \mid n^I((p))/\delta_F(p-1)/2 \},
\]

where \( q \) stands for prime numbers.

Then as before, we have

\[
N(x) = \sum_{n \mid \Omega(\zeta_1)} \mu(n) P(x, n) + O(M(x, \zeta_1, x)),
\]

and

\[
P(x, n) = \pi_{\mathbb{C}(\delta_n)}(x, K(\delta_n)/\mathbb{Q}) + O(\omega(n)).
\]

We conjecture

\[
N(x) = c_0 \text{Li}(x) + O\left( \frac{x \log \log x}{(\log x)^2} \right)
\]

where

\[
c_0 := \sum_{n \geq 1} \frac{\mu(n) \# C(\delta_n)}{[K(\delta_n) : \mathbb{Q}]}.
\]

But what we can do now is to show \( c_0 > 0 \). It means that the lower bound \( \delta_F(p-1)/2 \) for \( I((p)) \) is good. \( c_0 \) is a rational number times

\[
\prod_{p \equiv 1 \mod 3} \left\{ 1 - \frac{2}{p(p-1)} \right\}.
\]
Remark. Since
\[ P(x, 1) = \#P(x) \]
= the number of primes which is less than or equal to \( x \) and remains prime in \( F \)
= the number of primes which is less than or equal to \( x \) and decomposes a product of prime ideals of degree 3 in \( F_0 \)
\[ = \frac{1}{3} \cdot \text{Li}(x) + \text{error}, \]
\[ \#C(1)/[K(1) : \mathbb{Q}] \] should be 1/3.

REFERENCES


[H] T. Honda, Pure cubic fields whose class numbers are multiple of three, *J. Number Theory* 3 (1971), 7–12.


