Journal of the Mathematical Society of Japan Vol. 11, No. 2, April, 1959

Norm of units of quadratic fields.

By Yoshiomi FURUTA

(Received Nov. 13, 1958)

Let P be the rational number field and $\Omega=P(\sqrt{d})$ a real quadratic field, where d is a positive square free integer, different from 2. We denote by ε_0 a fundamental unit of Ω; by ε an arbitrary unit of Ω; by N the absolute norm; and by small Roman letters $a, b, \cdots, m, \cdots$ rational integers.

In this paper, we shall be concerned with the following problem:

"*For what pair of integers d, m does there exist in Ω a ring unit*[1] ε mod. m *with a negative norm*: $N\varepsilon=-1$?"

Dirichlet gave some criteria on the question by means of power residue symbols. More recently it was investigated by A. Scholz, L. Rédei and others. In particular, Rédei [**6**], [**7**] etc.[2], discussed it in detail by using the quadratic residue symbol and the fourth power residue symbol of Dirichlet, and finally Rédei [**9**] solved it completely as a problem related to the ideal class group of quadratic fields. On the other hand, Kuroda [**5**] and Furuta [**1**], [**2**] used the power residue symbol of Dirichlet and a generalized symbol to express the decomposition law of primes in some meta-abelian extensions, and also Tsunekawa [**10**] proved an interesting result concerning our problem. In the present paper, we shall give relationships between the norm of units of real quadratic fields and meta-abelian extensions, from which various results on our problem, in particular some of Rédei's results and Tsunekawa's theorem in a stronger from, can be deduced.

§ 1. Restricted power residue symbol.

Let Δ be an algebraic number field of finite degree, $\mathfrak{p}$ a prime ideal of Δ prime to 2 and α a number of Δ, prime to $\mathfrak{p}$. Then for a non-negative rational integer n the *restricted 2^n-th power residue symbol* $[\alpha/\mathfrak{p}]_n$ is defined as follows[3]. For $n=0$ we set always $[\alpha/\mathfrak{p}]_n=1$. For $n\geqq 1$ $[\alpha/\mathfrak{p}]_n$ is defined only when we have $[\alpha/\mathfrak{p}]_{n-1}=1$, and if this is really the case we set $[\alpha/\mathfrak{p}]_n=(-1)^x$, where $\alpha^{(N\mathfrak{p}^h-1)/2^n}\equiv(-1)^x$ (mod. $\mathfrak{p}$), h being the smallest natural number with $2^n\,|\,N\mathfrak{p}^h-1$. For an ideal $\mathfrak{m}$ of Δ prime to both α and 2 with the

1) Namely, a unit ε such that ε is contained in the ring class mod. m.

2) See Rédei [**9**], in which the history and literatures of the subject is stated.

3) See Furuta [**2**]. If Δ containes all the l-th roots of unity for a fixed rational prime l, we shall have analogous results to this § 1 by using l instead of 2.

prime ideal decomposition $\mathfrak{m}=\mathfrak{p}_1^{e_1}\cdots\mathfrak{p}_t^{e_t}$ we set $[\alpha/\mathfrak{m}]_n=[\alpha/\mathfrak{p}_1]_n^{e_1}\cdots[\alpha/\mathfrak{p}_t]_n^{e_t}$, when each $[\alpha/\mathfrak{p}_i]_n$ $(i=1,\cdots,t)$ is defined. From the definition follows the following lemma in an analogous manner[4] as in the case of the ordinary power residue symbol

LEMMA 1. *If* $2^n\mid N\mathfrak{p}-1$ *and* $[\alpha/\mathfrak{p}]_n=1$, *then* $\alpha\underset{[n]}{\equiv}1 \pmod{\mathfrak{p}}$[5].

Furthermore, we can prove

LEMMA 2. *If* $2^r\parallel N\mathfrak{p}-1$[6] *and* $[\alpha/\mathfrak{p}]_r=1$, *then* $[\alpha/\mathfrak{p}]_n=1$ *for all* n.

PROOF. For $n\leqq r$ we have trivially $[\alpha/\mathfrak{p}]_n=1$ by the definition. Let $n>r$ and $2^n\mid N\mathfrak{p}^h-1$, h being as before. Let $(N\mathfrak{p}^h-1)/2^n=k(N\mathfrak{p}-1)/2^r$, where k is an integer. Then, since $\alpha^{(N\mathfrak{p}-1)/2^r}\equiv 1 \pmod{\mathfrak{p}}$ by assumption, we have $\alpha^{(N\mathfrak{p}^h-1)/2^n}\equiv\alpha^{k(N\mathfrak{p}-1)/2^r}\equiv 1 \pmod{\mathfrak{p}}$.

The next two lemmas follow immediately from Lemma 2 and the definition.

LEMMA 3. *If both* $[\alpha/\mathfrak{p}]_n$ *and* $[\beta/\mathfrak{p}]_n$ *are defined, then* $[\alpha\beta/\mathfrak{p}]_n$ *is also defined, and we have* $[\alpha/\mathfrak{p}]_n[\beta/\mathfrak{p}]_n=[\alpha\beta/\mathfrak{p}]_n$.

LEMMA 4. *If* $[\alpha^k/\mathfrak{p}]_n$ *is defined for some odd rational integer* k, *then* $[\alpha/\mathfrak{p}]_n$ *is also defined, and we have* $[\alpha^k/\mathfrak{p}]_n=[\alpha/\mathfrak{p}]_n^k=[\alpha/\mathfrak{p}]_n$.

LEMMA 5. *For any prime ideal* $\mathfrak{p}$ *prime to* 2 *and for any natural number* s, *the next two relations* $\alpha\underset{[n]}{\equiv}1 \pmod{\mathfrak{p}}$ *and* $\alpha\underset{[n]}{\equiv}1 \pmod{\mathfrak{p}^s}$ *are equivalent.*

PROOF. If $\alpha\underset{[n]}{\equiv}1 \pmod{\mathfrak{p}^s}$, then trivially $\alpha\underset{[n]}{\equiv}1 \pmod{\mathfrak{p}}$. Conversely suppose that $\alpha\underset{[n]}{\equiv}1 \pmod{\mathfrak{p}}$, namely $\alpha=\beta^{2^n}\gamma$, $\gamma\equiv 1 \pmod{\mathfrak{p}}$ for some $\beta,\gamma\in\Delta$. Denoting by $S(\mathfrak{p}^s)$ the group of all $x\in\Delta$ such that $x\equiv 1 \pmod{\mathfrak{p}^s}$, we see that the order of the factor group $S(\mathfrak{p})/S(\mathfrak{p}^s)$ is equal to $\varphi(\mathfrak{p}^s)/\varphi(\mathfrak{p})=p^k$ where $k=f(s-1)$, $N\mathfrak{p}=p^f$. Therefore $\gamma^{p^k}\equiv 1 \pmod{p^s}$, whence $\alpha^{p^k}\underset{[n]}{\equiv}1 \pmod{\mathfrak{p}^s}$. Since p is odd, we have $\alpha\underset{[n]}{\equiv}1 \pmod{\mathfrak{p}^s}$.

Now we have the following

LEMMA 6. *We have* $[\alpha/\mathfrak{p}]_n=1$ *for all*[7] n *if and only if we have* $\alpha^k\equiv 1$ $\pmod{\mathfrak{p}^s}$ *for a natural number* s *and for an odd rational integer* k.

PROOF. From $\alpha^k\equiv 1 \pmod{\mathfrak{p}^s}$ follows $\alpha^k\equiv 1 \pmod{p}$, hence $[\alpha^k/\mathfrak{p}]_n=1$ for all n, and by Lemma 4 we have $[\alpha/\mathfrak{p}]_n=1$ for all n since k is odd. Conversely, suppose that $[\alpha/\mathfrak{p}]_n=1$ for all n. If $2^r\parallel N\mathfrak{p}-1$, then by Lemma 1 $\alpha\underset{[r]}{\equiv}1 \pmod{\mathfrak{p}^s}$, i.e. $\alpha=\beta^{2^r}\gamma$, $\gamma\equiv 1 \pmod{\mathfrak{p}^s}$ for some $\beta,\gamma\in\Delta$. If we set $k=\varphi(\mathfrak{p}^s)/2^r$, then k is odd and we see that $\beta^{k2^r}=\beta^{\varphi(\mathfrak{p}^s)}\equiv 1 \pmod{\mathfrak{p}^s}$. Hence we

4) For instance, see Hasse, Bericht über neuere Untersuchungen und Probleme aus der Theorie der algebraischen Zahlkörper II (1926), p. 10.

5) $\alpha\underset{[n]}{\equiv}1 \pmod{\mathfrak{p}}$ means that $\alpha\equiv\beta^{2^n} \pmod{\mathfrak{p}}$ for some $\beta\in\Delta$.

6) $2^r\parallel N\mathfrak{p}-1$ means that $2^r\mid N\mathfrak{p}-1$ and $2^{r+1}\nmid N\mathfrak{p}-1$.

7) By Lemma 2 we may write "for n such that $2^n\parallel N\mathfrak{p}-1$" instead of "for all n".

have $\alpha^k \equiv 1$ (mod. $\mathfrak{p}^s$) for an odd k.

§ 2. Norm of ring units of real quadratic fields.

We denote hereafter by small Greek letters $\alpha, \beta, \cdots$ integers of the quadratic field Ω, and by $\alpha', \beta', \cdots$ their conjugates with regard to Ω/P. Let $d = q_1 \cdots q_t$ be the prime number decomposition of d in P, and $\mathfrak{q}_1, \cdots, \mathfrak{q}_t$ be all the prime divisors of $q_1, \cdots, q_t$ in Ω respectively. Further, assume hereafter that m is odd.

LEMMA 7. *Let* $m = \prod_{i=1}^{s} \mathfrak{p}_i^{e_i} \prod_{j=1}^{t} \mathfrak{q}_j^{e_j}$ *be the prime ideal decomposition of* m *in* Ω *where* $(\mathfrak{p}_i, d) = 1$, $1 \leqq e_i$ *and* $0 \leqq e_j$. *Then* α *is contained in the ring class* mod. m *of* Ω *if and only if*

$$\begin{cases} \alpha \equiv \alpha' & (\text{mod. } \mathfrak{p}_i^{e_i}) \quad i = 1, \cdots, s, \\ \alpha \equiv \alpha' & (\text{mod. } \mathfrak{q}_j^{2e_j+1}) \quad j = 1, \cdots, t. \end{cases}$$

PROOF. Since we have $\alpha - \alpha' = b\sqrt{d}$ or $\alpha - \alpha' = 2b\sqrt{d}$ with some b according as $d \equiv 1$ (mod. 4) or $d \equiv 2, 3$ (mod. 4), the lemma is clear.

THEOREM 1. *In order that* $N\varepsilon_0 = 1$ *resp.* -1 *it is necessary and sufficient that* $[\varepsilon_0^2/\mathfrak{q}]_n = 1$ *resp.* $[-\varepsilon_0^2/\mathfrak{q}]_n = 1$ *for all* n[7] *and for one of the prime divisors* $\mathfrak{q}$ *prime to* 2 *of* d.

PROOF. i) Since $\varepsilon_0 \equiv \varepsilon_0'$ (mod. $\sqrt{d}$), we have $N\varepsilon_0 \equiv \varepsilon_0^2$ (mod. $\sqrt{d}$), namely $\varepsilon_0^2 \equiv 1$ or -1 (mod. $\sqrt{d}$) according as $N\varepsilon_0 = 1$ or -1. Hence, it follows from Lemma 6 that we have $[\varepsilon_0^2/\mathfrak{q}]_n = 1$ or $[-\varepsilon_0^2/\mathfrak{q}]_n = 1$ for all $\mathfrak{q}$ prime to 2 according as $N\varepsilon_0 = 1$ or -1.

ii) Suppose that $[-\varepsilon_0^2/\mathfrak{q}]_n = 1$ for one of $\mathfrak{q} | d$ prime to 2 and for all n. Then by Lemma 6 we have $\varepsilon_0^{2k} \equiv -1$ (mod. $\mathfrak{q}$) for some odd k, hence $(N\varepsilon_0)^k \equiv -1$ (mod. $\mathfrak{q}$), owing to $N\varepsilon_0 \equiv \varepsilon_0^2$ (mod. $\mathfrak{q}$). Since k is odd, we have $N\varepsilon_0 \equiv -1$ (mod. $\mathfrak{q}$), which means that $N\varepsilon_0 = -1$, because $\mathfrak{q}$ is prime to 2.

Now we prove the following[8]

THEOREM 2[9] *In order that there exists in* Ω *a ring unit* ε *mod.* m *such that* $N\varepsilon = -1$, *it is necessary and sufficient that we have* $[-\varepsilon_0^2/\mathfrak{q}]_n = 1$ *for all* n[7] *and for one of the prime divisors* $\mathfrak{q}$, *prime to* 2, *of* d *and* $[-\varepsilon_0^2/\mathfrak{p}]_n = 1$ *for all* n[7] *and for all prime divisors* $\mathfrak{p}$ *of* m.

---

8) Theorem 2 is a result stronger than that of Tsunekawa [**10**], i. e. we drop his assumption $N\varepsilon_0 = -1$.

9) In the excluding cases where $d = 2$ or m is even, we can show easily the following facts: In case of $d = 2$ we have $N\varepsilon_0 = -1$. In case of m being even, if $d \equiv 1$ (mod. 4) and $N\varepsilon_0 = -1$ then $\varepsilon = \varepsilon_0^{\varphi(2)}$ is a ring unit mod. 2 such that $N\varepsilon = -1$, where φ is Euler's function in Ω; if $2 | d$, then there is no ring unit ε mod. 2 such that $N\varepsilon = -1$; finally, if $d \not\equiv 1$ (mod. 4) and $2 \nmid d$, then always $N\varepsilon_0 = -1$.

PROOF. $N\varepsilon=-1$ if and only if $N\varepsilon_0=-1$ and $\varepsilon=\varepsilon_0^k$ for some odd k. On the other hand, by Lemma 7, ε is a ring unit mod. $\mathfrak{m}$ if and only if $N\varepsilon\equiv\varepsilon^2$ (mod. $\mathfrak{p}_i^{e_i}$ and $\mathfrak{q}_j^{2e_j+1}$) $(i=1,\cdots,s;j=1,\cdots,t)$. Hence it is necessary and sufficient for ε to be a ring unit mod. $\mathfrak{m}$ that we have $N\varepsilon_0=-1$ and $(-\varepsilon_0^2)^k\equiv 1$ (mod. $\mathfrak{p}_i^{e_i}$ and $\mathfrak{q}_j^{2e_j+1}$) for some odd k $(i=1,\cdots,s;j=1,\cdots,t)$. The theorem follows immediately from Lemma 6 and Theorem 1.

§ 3. Fields $\Omega(\sqrt{\varepsilon_0})$.

LEMMA 8. *We have* $N\varepsilon_0=1$ *if and only if* $\Omega(\sqrt{\varepsilon_0})/P$ *is a non-cyclic extension of degree* 4.

We have $N\varepsilon_0=-1$ *if and only if* $\Omega(\sqrt{\sqrt{d}\,\varepsilon_0})/P$ *is a cyclic extension of degree* 4.

PROOF. Let ω be equal to ε_0 or $\sqrt{d}\,\varepsilon_0$ according as $N\varepsilon_0=1$ or -1, and put $K=\Omega\,(\sqrt{\omega})$. Let σ and τ be the non-unit element of the Galois group of Ω/k and of K/Ω respectively, and let U_σ be a representative of σ in the Galois group of K/P. Since $\varepsilon_0^\sigma=\varepsilon_0^{-1}$ or $(\sqrt{d}\,\varepsilon_0)^\sigma=\sqrt{d}\,\varepsilon_0\cdot\varepsilon_0^{-2}$ according as $N\varepsilon_0=1$ or -1, K/P is a normal extension. On the other hand we have $\sqrt{\omega}^\tau=-\sqrt{\omega}$, $\sqrt{\omega}^{U_\sigma}=\sqrt{\omega}\,\gamma$ for some $\gamma\in\Omega$, hence $\sqrt{\omega}^{U_\sigma^2}=\sqrt{\omega}\,N\gamma$. First, let $N\varepsilon_0=1$. Then $\omega=\varepsilon_0$, $(\sqrt{\omega}^{U_\sigma})^2=\varepsilon_0^\sigma=\varepsilon_0^{-1}$ and $(\sqrt{\omega}^{U_\sigma})^2=(\sqrt{\omega}\,\gamma)=\varepsilon_0\cdot\gamma^2$. Therefore we have $\gamma=\pm\varepsilon_0$, $N\gamma=N\varepsilon_0=1$, hence $U_\sigma^2=1$, which means that K/P is a non-cyclic extension. Next, let $N\varepsilon_0=-1$. Then $\omega=\sqrt{d}\,\varepsilon_0$, $(\sqrt{\omega}^{U_\sigma})^2=(\sqrt{d}\,\varepsilon_0)^\sigma$ $=\sqrt{d}\,\varepsilon_0^{-1}$ and $(\sqrt{\omega}^{U_\sigma})^2=(\sqrt{\omega}\,\gamma)^2=\sqrt{d}\,\varepsilon_0\cdot\gamma^2$. Therefore we have $\gamma=\pm\varepsilon_0^{-1}$, $N\gamma$ $=N\varepsilon_0^{-1}=-1$, hence $U_\sigma^2=\tau$, which means that K/P is a cyclic extension.

Now, for a while, suppose that $N\varepsilon_0=-1$. Let $d=q_1\cdots q_t$ be, as before, the prime number decomposition of d in P. Then we see necessarily that $q_i=2$ or $q_i\equiv 1$ (mod. 4) $(i=1,\cdots,t)$. Let K_i $(i=1,\cdots,t)$ be a cyclic subfield of degree 4 of the 2^n-th cyclotomic extensions over P $(n\geqq 4)$ or the cyclic subfield of degree 4 of the ray class field mod. q over P according as $q_i=2$ or not. Moreover, let χ_i be a generating character of the Galois group of K_i/P $(i=1,\cdots,t)$. For $a\in P$ we put $\chi_i(a)=\chi_i\left(\left(\frac{K/P}{(a)}\right)\right)$ where $\left(\frac{K/P}{(a)}\right)$ is the Artin symbol. We set

$$(*)\qquad \chi=\chi_1^{n_1}\cdots\chi_t^{n_t},\ n_i=1,3\qquad(i=1,\cdots,t).$$

Then Ω is the field corresponding to χ^2. Denote by A the field corresponding to χ. Then all the divisors of d and only these are completely ramified in A/P, and conversely a cyclic extension A over P of degree 4 with this property corresponds to a character χ defined by $(*)$.

In the rational number field the symbol $[a/p]_n$ is defined for $p=2$ as follows[10]: $[a/2]_n$ is defined only when $a\equiv 1 \pmod{2^{n+1}}$ and if this is really the case $[a/2]_n$ is equal to 1 or -1 according as $a\equiv 1 \pmod{2^{n+2}}$ or not.

Now we have

THEOREM 3. *If* $N\varepsilon_0=-1$, *then* $\Omega(\sqrt{-1}, \sqrt{\varepsilon_0})/P$ *is a non-abelian extension, and, for some* χ *defined by* (*) *and for any rational prime* p *with* $p\equiv 1 \pmod 4$ *and* $(d/p)=1$[11], *we have*

$$(\varepsilon_0/\mathfrak{p})=\chi(p)[d/p]_2$$

where $\mathfrak{p}$ *is a prime divisor of* p *in* Ω, *and* $(\varepsilon_0/\mathfrak{p})$ *is the quadratic residue symbol in* $\Omega(\sqrt{-1})$.

PROOF. If we put $K=\Omega(\sqrt{\sqrt{d}\,\varepsilon_0})$ and $K'=\Omega(\sqrt{-\sqrt{d}\,\varepsilon_0})$, then by Lemma 8 K and K' are both cyclic extension over P of degree 4, in which all divisors of d are completely ramified. If we can show that at least in one of them only the divisors of d are ramified, then by what we have remarked above we see that $(\sqrt{d}\,\varepsilon_0/\mathfrak{p})=\chi(\mathfrak{p})$, and therefore[12] $(\varepsilon_0/\mathfrak{p})=\chi(p)[d/p]_2$, for some χ defined by (*) and for any rational prime p with $p\equiv 1 \pmod 4$ and $(d/p)=1$. Hence to prove the theorem we have only to show that at least in one of K and K' over P only the divisors of d are ramified. Since both in K and in K' over P only divisors of $2d$ can be ramified, it remains only to prove that if d is not even, then 2 is not ramified at least in one of K or K' over P. Let d be odd, and suppose that 2 is ramified in K. Denote by A, as before, the field corresponding to χ, and B the quadratic subfield of AK over Ω, distinct both from A and from K. Then, since A and K are both cyclic over P of degree 4, B is non-cyclic and biquadratic over P and only the divisors of 2 are ramified. Hence we have $B=\Omega(\sqrt{a})$ where $a=-1$ or 2. But $a=2$ does not occur, because otherwise we would have $A=\Omega(\sqrt{2\sqrt{d}\,\varepsilon_0})$, contrary to the fact that 2 is not ramified in A/P. Therefore we have $A=K'$, and our assertion is proved.

COROLLARY. *If we assume in Theorem* 2 *moreover that* $(p/q_i)=1$ *for all* $q_i\,|\,d$, *then we have*

$$(\varepsilon_0/\mathfrak{p})=[p/d]_2\,[d/p]_2\,.$$

PROOF. If $(p/q_i)=1$, then we have $\chi_i(p)=[p/q_i]_2$. Thus, our assertion follows from the theorem at once.

§ 4. Applications.

If Pell's equation $x^2-fy^2=-1$ is solvable, we call f *admissible.* Suppose

10) cf. Furuta [**1**, p. 50].
11) (d/p) is the quadratic residue symbol in P.
12) cf. Furuta [**2**, Lemma 1 and Lemma 2].

that $d(\neq 2)$ is squarefree and let $f=m^2d$. Then f is admissible if and only if there exists in $P(\sqrt{d})$ a ring unit ε mod. m such that $N\varepsilon=-1$. By Theorem 2 and Corollary to Theorem 3 the following result is easily obtained:

a) *Suppose that d is admissible and that m is divisible only by primes p with $p\equiv 5$ (mod. 8) and $(p/q)=1$ for all $q|d$. Then m^2d is addmissible if and only if we have $[p/d]_2[d/p]_2=-1$ for all $p|m$.*

b)[13] *Let d_1 and d_2 be two positive odd integers and put $d=d_1d_2$, $\Omega_1=P(\sqrt{d_1})$, $\Omega_2=P(\sqrt{d_2})$, $\Omega_3=P(\sqrt{d})$. Moreover, let ε_i be a fundamental unit of Ω_i and suppose that $N\varepsilon_i=-1$ $(i=1,2,3)$. Then $\sqrt{\varepsilon_1\varepsilon_2\varepsilon_3}$ is contained in $\Lambda=P(\sqrt{-1}, \sqrt{q_1},\cdots,\sqrt{q_t})$ where $q_1,\cdots,q_t$ are all divisors of d.*

PROOF. Let p be any rational prime which decomposes completely in Λ, i.e., $(p/q)=1$ for all $q|d$, and $\mathfrak{P}, \mathfrak{p}_1, \mathfrak{p}_2, \mathfrak{p}_3$ be prime divisors of p in $\Lambda, \Omega_1, \Omega_2, \Omega_3$ respectively. Then by Corollary to Theorem 3 $(\varepsilon_1\varepsilon_2\varepsilon_3/\mathfrak{P})=(\varepsilon_1/\mathfrak{p}_1)(\varepsilon_2/\mathfrak{p}_2)(\varepsilon_3/\mathfrak{p}_3)=[p/d_1]_2[d_1/p]_2[p/d_2]_2[d_2/p]_2[p/d]_2[d/p]_2=1$. Hence p also decomposes completely in $\Lambda(\sqrt{\varepsilon_1\varepsilon_2\varepsilon_3})$, i.e. $\sqrt{\varepsilon_1\varepsilon_2\varepsilon_3}\in\Lambda$.

c)[14] *Let d_1 and d_2 be two admissible odd integers prime to each other, and put $d=d_1d_2$. If $[p/d_2]_2[d_2/p]_2=-1$ for one of the prime divisors p of d_1, then d is non-admissible.*

PROOF. Notations being as in **b**), we have $N\varepsilon_1=N\varepsilon_2=-1$ by the assumption for d_1 and d_2. We now assume that $N\varepsilon_3=-1$. Then by **b**) the product $\varepsilon_1\varepsilon_2\varepsilon_3$ is a square number in Λ. Hence we have $(\varepsilon_3/\mathfrak{p}_3)=(\varepsilon_1/\mathfrak{p}_1)(\varepsilon_2/\mathfrak{p}_2)$ and by Theorem 1 $[-\varepsilon_1^2/\mathfrak{p}_1]_2=[-1/p]_2(\varepsilon_1/\mathfrak{p}_1)=1$. Therefore, we see by Corollary to Theorem 3 that $(\varepsilon_3/\mathfrak{p}_3)=[-1/\mathfrak{p}_1]_2(\varepsilon_2/\mathfrak{p}_2)=[-1/\mathfrak{p}_1]_2[p/d_2]_2[d_2/p]_2$, whence $(\varepsilon_3/\mathfrak{p}_3)=-[-1/\mathfrak{p}_1]_2=-[-1/p]_2$ by the assumption. On the other hand, we have $[-\varepsilon_3^2/\mathfrak{p}_3]_2=[-1/p]_2(\varepsilon_3/\mathfrak{p}_3)=1$ by Theorem 1, whence $(\varepsilon_3/\mathfrak{p}_3)=[-1/p]_2$, which is a contradiction. Thus our assertion is proved.

Mathematical Institute,
Nagoya University.

References

[1] Y. Furuta, A reciprocity law of the power residue symbol, J. Math. Soc. Japan, **10** (1958), 46-54.

[2] Y. Furuta, On meta-abelian fields of a certain type, Nagoya Math. J., **14** (1959), 193-199.

[3] T. Kubota, Über den bizyklischen biquadratischen Zahlkörper, Nagoya Math. J., **10** (1956), 65-85.

---

13) cf. Kuroda [**4**, Satz 11] and Kubota [**3**, Satz 1].

14) This criterion **c**) is somewhat different from that of Rédei [**7**].

[4] S. Kuroda, Über den Dirichletschen Körper, J. Fac. Sci. Imp. Univ. Tokyo, Sec., I, **4** (1943), 383-406.

[5] S. Kuroda, Über die Zerlegung rationaler Primzahlen in gewissen nicht-abelschen galoischen Körpern. J. Math. Soc. Japan, **3** (1951), 148-156.

[6] L. Rédei, Über die Grundeinheit und die durch 8 teilbaren Invarianten der absoluten Klassengruppe im quadratischen Zahlkörper. J. Reine Angew. Math., **171** (1934), 131-148.

[7] L. Rédei, Über die Pellsche Gleichung $t^2-du^2=-1$, J. Reine Angew. Math., **173** (1935), 193-211.

[8] L. Rédei, Bedingtes Artinsches Symbol mit Anwendung in der Klassenkörpertheorie, Acta Math. Acad. Sci. Hung., **4** (1953), 1-30.

[9] L. Rédei, Die 2-Ringklassengruppe des quadratischen Zahlkörpers und die Theorie den Pellschen Gleichung, ibid., 31-85.

[10] M. Tsunekawa, On the multiple solutions of $x^2-dy^2=-1$, Bull. Nagoya Inst. Technology, **8** (1956), 1-7 (Japanese).