Halter-Koch, F. and Ishii, N.
Osaka J. Math.
26 (1989), 625–646

RING CLASS FIELDS MODULO 8 OF $Q(\sqrt{-m})$ AND THE QUARTIC CHARACTER OF UNITS OF $Q(\sqrt{m})$ FOR $m \equiv 1$ MOD 8

FRANZ HALTER-KOCH AND NOBURO ISHII

(Received March 8, 1988)

1. Introduction

For a positive squarefree rational integer m let ε_m be the fundamental unit of $\boldsymbol{Q}(\sqrt{m})$ and suppose $N_{\boldsymbol{Q}(\sqrt{m})/\boldsymbol{Q}}(\varepsilon_m)=-1$. Then, for $s\geq 1$ and any prime ideal $\boldsymbol{P}$ of $\boldsymbol{Q}(\sqrt{m})$ with $N(\boldsymbol{P})\equiv 1 \bmod 2^s$, the 2^s-th power residue symbol $\left(\frac{\varepsilon_m}{\boldsymbol{P}}\right)_{2^s}$ is defined and has value ± 1 provided that ε_m is a 2^{s-1}-th power residue modulo $\boldsymbol{P}$, i.e. $\left(\frac{\varepsilon_m}{\boldsymbol{P}}\right)_{2^{s-1}}=1$. Especially, if p is a rational prime with $p\equiv 1 \bmod 2^{s+1}$ and $\left(\frac{m}{p}\right)=1$, the symbol $\left(\frac{\varepsilon_m}{\boldsymbol{P}}\right)_{2^s}$ for $\boldsymbol{P}\mid p$ depends only on p and is denoted by $\left(\frac{\varepsilon_m}{p}\right)_{2^s}$. Concerning this latter case, explicit criteria for $\left(\frac{\varepsilon_m}{p}\right)_{2^s}=1$ in terms of representations of powers of p by binary quadratic forms have been given in the following cases ([13], [6], [2]):

A. $m\equiv 5 \bmod 8$ or $m\equiv 2 \bmod 4$, and the ideal class group of $\boldsymbol{Q}(\sqrt{-m})$ has no invariant divisible by 4; $s=1$ and $s=2$.

B. $m\equiv 1 \bmod 8$, and the ideal class group of $\boldsymbol{Q}(\sqrt{-m})$ has only one invariant divisible by 4; $s=1$.

In this paper we treat the case $s=2$ for ***B.*** which could not be settled up to now (§5); in this case we also determine the quartic residue symbol $\left(\frac{\varepsilon_m}{\boldsymbol{P}}\right)_4$, where $\boldsymbol{P}$ is a prime divisor in $\boldsymbol{Q}(\sqrt{m})$ of a prime p with $\left(\frac{-1}{p}\right)=\left(\frac{m}{p}\right)=1$ (if $p\equiv 5 \bmod 8$, this symbol depends on $\boldsymbol{P}$ and not only on p). Further we derive criteria for $\left(\frac{\varepsilon_m}{\boldsymbol{P}}\right)_{2^s}=1$ $(s=1, 2)$ for inert prime ideals $\boldsymbol{P}$ of $\boldsymbol{Q}(\sqrt{m})$ under quite general assumptions (§3) and criteria for $\left(\frac{\varepsilon_m}{\boldsymbol{q}}\right)_{2^s}=1$ $(s=1, 2)$ in the case where $m=q$ is a prime and $\boldsymbol{q}=(\sqrt{q})$ (§6). The proofs depend on the generation of suitable subfields of the ring class field modulo 8 of $\boldsymbol{Q}(\sqrt{-m})$ by radicals (§4).

There is a similar and even more complete series of results including octic residuacity in the case $N_{Q(\sqrt{m})/Q}(\varepsilon_m)=1$ (see [13], [6], [7] and [11]).

2. Notation

Throughout this paper we keep the following notation:
$m>1$ is a squarefree rational integer;

$$F = \boldsymbol{Q}(\sqrt{m}),\ k = \boldsymbol{Q}(\sqrt{-m});$$
$$K = F\cdot k = \boldsymbol{Q}(\sqrt{m}, \sqrt{-m}) = F(i) = k(i)\,, \text{ where}$$
$$i = \sqrt{-1};$$

h is the odd part of the class number of k;
$\varepsilon=U+V\sqrt{m}$ is the fundamental unit of $\boldsymbol{Z}[\sqrt{m}]$ with

$$U,\ V\in\boldsymbol{N}, \text{ so } \varepsilon>1\,,$$
$$N_{Q(\sqrt{m})/Q}(\varepsilon) = U^2-mV^2 = -1\,.$$

If ε_m is the fundamental unit of $\boldsymbol{Q}(\sqrt{m})$ then either $\varepsilon=\varepsilon_m$ or $\varepsilon=\varepsilon_m^3$ where the latter case can only occur if $m\equiv5 \bmod 8$. In any case, ε and ε_m have the same 2^s-th power residue properties and we shall prefer to work with ε instead of ε_m.

3. Residuacity criteria for inert primes

We start with two simple lemmas; the first concerns Galois theory, the second quadratic reciprocity.

Lemma 1. *$K(\sqrt[4]{2\varepsilon})/k$ is a cyclic extension of degree 8, and $K(\sqrt[4]{2\varepsilon})/\boldsymbol{Q}$ is normal with a dihedral group of order 16 as Galois group.*

Proof. As $N_{K/k}(2\varepsilon)=-4$ we deduce from [6; Satz 1] that $K(\sqrt[4]{2\varepsilon})/k$ is cyclic of degree 8. If σ_0 generates the Galois group of K/k, then $\sigma_0(2\varepsilon)=\dfrac{(1-i)^4}{2\varepsilon}$, and thus a generator σ of the Galois group of $K(\sqrt[4]{2\varepsilon})/k$ is given by

$$\sigma(\sqrt[4]{2\varepsilon}) = \frac{1-i}{\sqrt[4]{2\varepsilon}}\,.$$

Let τ_0 be the generator of the Galois group of K/F; then $\tau_0(2\varepsilon)=2\varepsilon$ and thus τ_0 has an extension τ to $K(\sqrt[4]{2\varepsilon})$ defined by

$$\tau(\sqrt[4]{2\varepsilon}) = \sqrt[4]{2\varepsilon}\,.$$

But $\tau_0|k$ generates the Galois group of $k/\boldsymbol{Q}$, and therefore $K(\sqrt[4]{2\varepsilon})/\boldsymbol{Q}$ is normal with Galois group generated by σ and τ. Now we can check the relations

$$\sigma^8=\tau^2=id\,,\quad \sigma\tau=\tau\sigma^{-1}$$

by applying the automorphisms to $\sqrt[4]{2\varepsilon}$ and i; this proves the assertion. ■

Lemma 2. *Let E be a quadratic number field, p an odd rational prime which is inert in E and $\boldsymbol{P}=(p)$ the prime divisor of p in E. Then, for any rational integer r, prime to p, we have* $\left(\frac{r}{\boldsymbol{P}}\right)=1$ *and*

$$\left(\frac{r}{\boldsymbol{P}}\right)_4=\begin{cases}1, & \text{if } p\equiv -1 \bmod 4\,,\\ \left(\frac{r}{p}\right), & \text{if } p\equiv 1 \bmod 4\,.\end{cases}$$

Proof. By Euler's criterion, we have

$$\left(\frac{r}{\boldsymbol{P}}\right)\equiv r^{(p^2-1)/2} \bmod \boldsymbol{P}\,,$$

as $N(\boldsymbol{P})=p^2$, thus $\left(\frac{r}{\boldsymbol{P}}\right)=1$ since $r^{(p^2-1)/2}=(r^{p-1})^{(p+1)/2}\equiv 1 \bmod p$. In the same way,

$$\left(\frac{r}{\boldsymbol{P}}\right)_4\equiv r^{(p^2-1)/4} \bmod \boldsymbol{P}\,,$$

and if $p\equiv -1 \bmod 4$, $r^{(p^2-1)/4}=(r^{p-1})^{(p+1)/4}\equiv 1 \bmod p$ implies $\left(\frac{r}{\boldsymbol{P}}\right)_4=1$. If $p\equiv 1 \bmod 4$, $\frac{p+1}{2}$ is odd and the decomposition $\frac{p^2-1}{4}=\frac{p-1}{2}\cdot\frac{p+1}{2}$ shows that $r^{(p^2-1)/4}\equiv 1 \bmod \boldsymbol{P}$ if and only if $r^{(p-1)/2}\equiv 1 \bmod p$, i.e., $\left(\frac{r}{p}\right)=1$. ■

REMARK. Lemma 2 is a very special case of a general formula for the power residue symbol, see [5; §14, IV.].

Now we are well prepared to prove the reciprocity criteria for inert primes:

Theorem 1. *Let p be an odd rational prime inert in F, i.e.* $\left(\frac{m}{p}\right)=-1$, *and let $\boldsymbol{P}=(p)$ be the prime divisor of p in F. Then:*

a) $\left(\frac{\varepsilon}{\boldsymbol{P}}\right)=\left(\frac{-1}{p}\right)$.

b) *If* $p\equiv 1 \bmod 4$, $\left(\frac{\varepsilon}{\boldsymbol{P}}\right)_4=\left(\frac{2}{p}\right)$.

Proof. Let $\boldsymbol{p}_k$ resp. $\boldsymbol{p}_K$ be a prime divisor of p in k resp. K; then $\boldsymbol{p}_K$ is a prime divisor of $\boldsymbol{P}$ of relative degree 1 and the prime residue class groups modulo $\boldsymbol{P}$ and $\boldsymbol{p}_K$ coincide.

If $p\equiv -1 \bmod 4$, $\boldsymbol{p}_k$ is inert in K, and as $K(\sqrt{2\varepsilon})/k$ is cyclic, $\boldsymbol{p}_k$ remains inert in $K(\sqrt{2\varepsilon})$. Thus $\boldsymbol{p}_K$ is inert in $K(\sqrt{2\varepsilon})$ too, and we obtain

$$-1=\left(\frac{2\varepsilon}{\boldsymbol{p}_K}\right)=\left(\frac{2\varepsilon}{\boldsymbol{P}}\right)=\left(\frac{2}{\boldsymbol{P}}\right)\cdot\left(\frac{\varepsilon}{\boldsymbol{P}}\right)=\left(\frac{\varepsilon}{\boldsymbol{P}}\right)$$

using lemma 2.

If $p\equiv 1 \bmod 4$, p is inert in k and therefore $\boldsymbol{p}_k$ splits completely in $K(\sqrt[4]{2\varepsilon})$ by [9; Satz 25] and lemma 1. Thus $\boldsymbol{p}_K$ splits completely in $K(\sqrt[4]{2\varepsilon})$ too, and we obtain

$$1=\left(\frac{2\varepsilon}{\boldsymbol{p}_K}\right)_4=\left(\frac{2\varepsilon}{\boldsymbol{P}}\right)_4=\left(\frac{2}{\boldsymbol{P}}\right)_4\cdot\left(\frac{\varepsilon}{\boldsymbol{P}}\right)_4=\left(\frac{2}{p}\right)\cdot\left(\frac{\varepsilon}{\boldsymbol{P}}\right)_4$$

by lemma 2, which is the assertion. ■

4. The ring class groups and ring class fields involved

In this section we study the subfields of the ring class field modulo 8 of $\boldsymbol{Q}(\sqrt{-m})$ which can be generated by radicals; the arithmetic of these fields is used in the next section to derive the announced power residue criteria.

From now on, we will assume that

$$m=q_1\cdot\cdots\cdot q_d$$

is the product of $d\geq 1$ different primes $q_1, \cdots, q_d$ with

$$q_1\equiv q_2\equiv\cdots\equiv q_d\equiv 1 \bmod 8\,.$$

For $s\geq 0$ let $R(s)$ be the ring class group modulo 2^s of k and $R(s)'$ the 2-component of $R(s)$; especially, $R(0)$ is the ideal class group and $R(0)'$ is the 2-class group of k. For an integral ideal $\boldsymbol{a}$ of k (prime to 2 if $s\geq 1$) let $[\boldsymbol{a}]_s\in R(s)$ be the ring class which contains $\boldsymbol{a}$.

Let $C_1, \cdots, C_d$ be a basis of $R(0)'$, $2^{t_j}>1$ the order of C_j, and $\boldsymbol{m}_j$ a primitive ambiguous ideal of k in $C_j^{2^{t_j-1}}$ (see [4; §29]). If $m_j=N(\boldsymbol{m}_j)$, then $m_j\,|\,2m$ for $j=1, \cdots, d$, and we may assume that $m_1=2m_1'$ and that $m_1', m_2, \cdots, m_d$ divide m (especially $m_1'\equiv m_2\equiv\cdots\equiv m_d\equiv 1 \bmod 8$). As m has only prime factors $q_j\equiv 1 \bmod 8$, the prime divisor of 2 lies in the principal genus of k [4, §26] and thus we have $t_1\geq 2$. Let $\boldsymbol{t}_j\in C_j$ be integral ideals prime to 2, $\boldsymbol{t}_j=\boldsymbol{m}_j$ in case $t_j=1$. Set

$$\boldsymbol{t}_j^{2^{t_j}}=(\mu_j)$$

with integral $\mu_j\in k (j=1, \cdots, d)$. Then we obtain:

Lemma 3. *There exist rational integers* $r_1, \cdots, r_d$ *such that* $\mu_1\equiv r_1\sqrt{-m}$ mod 8 *and* $\mu_j\equiv r_j$ mod 8 *for* $j=2, \cdots, d$.

Proof. As $\boldsymbol{t}_j^{2^{t_j-1}}$ and $\boldsymbol{m}_j$ are both contained in $C_j^{2^{t_j-1}}$ we have

$$t_j^{2^{t_j-1}} = m_j \cdot (\gamma_j)$$

with

$$\gamma_j = \frac{x_j + y_j\sqrt{-m}}{z_j} \in k,\ x_j, y_j, z_j \in \boldsymbol{Z},\ (x_j, y_j, z_j) = 1$$

and

$$N(t_j^{2^{t_j-1}}) = m_j \cdot \frac{x_j^2 + my_j^2}{z_j^2}\,.$$

$N(t_j^{2^{t_j-1}})$ is integral and congruent to 1 modulo 8, if $t_j \geq 2$.

As $t_1 \geq 2$, we have $z_1 = 2z_1'$ and $x_1 \equiv y_1 \equiv z_1' \equiv 1 \bmod 2$; therefore

$$\begin{aligned} \pm\mu = m_1\gamma_1^2 &= m_1 \cdot \frac{x_1^2 + my_1^2}{z_1^2} - \frac{m_1' my_1^2}{z_1'^2} + \frac{m_1' x_1 y_1}{z_1'^2} \cdot \sqrt{-m} \\ &\equiv x_1 y_1 \sqrt{-m} \bmod 8\,. \end{aligned}$$

If in the case $j \geq 2$ we have $t_j = 1$ then $\boldsymbol{t}_j = \boldsymbol{m}_j$, $\mu_j = \pm m_j$ and we are done.

If $j \geq 2$ and $t_j \geq 2$ then z_j is odd and either x_j or y_j is divisible by 4; therefore

$$\pm\mu_j = m_j\gamma_j^2 = m_j \cdot \frac{x_j^2 + my_j^2}{z_j^2} - \frac{2m_j my_j^2}{z_j^2} + \frac{2x_j y_j}{z_j^2} \cdot \sqrt{-m}\,,$$

and the assertion follows from $2x_j y_j \equiv 0 \bmod 8$. ■

Now we are in position to determine the structure of the group $R(s)'$ in our special situation, at least for $s \leq 3$ (compare [6; §7] where this was done under somewhat different assumptions).

Proposition 1. *Let m be a product of $d \geq 1$ different primes $q_j \equiv 1 \bmod 8$ and keep all the notation introduced above. Then*:

a) *For $s \in \{0, 1\}$, $R(s)'$ is of type*

$$(2^{t_1+s}, 2^{t_2}, \cdots, 2^{t_d})$$

with basis

$$([\boldsymbol{t}_1]_s, [\boldsymbol{t}_2]_s, \cdots, [\boldsymbol{t}_d]_s)\,.$$

b) *For $s \in \{2, 3\}$, $R(s)'$ of is type*

$$(2^{s-1}, 2^{t_1+1}, 2^{t_2}, \cdots, 2^{t_d})$$

with basis

$$([(-1+2\sqrt{-m})]_s, [\boldsymbol{t}_1]_s, [\boldsymbol{t}_2]_s, \cdots, [\boldsymbol{t}_d]_s)\,.$$

c) *For $s \geq 4$, $R(s)'$ is generated by $[(-1+2\sqrt{-m})]_s$, $[\boldsymbol{t}_1]_s, \cdots, [\boldsymbol{t}_d]_s$ (but these elements do not necessarily form a basis).*

Proof. Let $P(s)$ be the prime residue class group modulo 2^s in k and $P_0(s) \subset P(s)$ the subgroup generated by those prime residue classes modulo 2^s which contain rational numbers. For an integral $\alpha \in k$, prime to 2, let $\{\alpha\}_s \in P(s)/P_0(s)$ be the class determined by α. Then we see from [8]:

$$P(0) = P_0(1) = 1\,,$$
$$P(1) = P(1)/P_0(1) \quad \text{is of order 2, generated by } \{\sqrt{-m}\}_1\,,$$

and for $s \geq 2$

$$P(s)/P_0(s) \quad \text{is of type } (2^{s-1}, 2) \text{ with basis } (\{-1+2\sqrt{-m}\}_s, \{\sqrt{-m}\}_s)\,.$$

Now $R(s)$ is determined by the exact sequence

$$1 \to P(s)/P_0(s) \xrightarrow{\varphi} R(s) \xrightarrow{\psi} R(0) \to 1$$

with $\varphi(\{\alpha\}_s) = [(\alpha)]_s$ and $\psi([\boldsymbol{a}]_s) = [\boldsymbol{a}]_0$. Obviously, $im(\varphi) \subset R(s)'$, and we get the exact sequence

$$1 \to P(s)/P_0(s) \to R(s)' \to R(0)' \to 1$$

which determines $R(s)'$ as follows:

$R(s)'$ is generated by $im(\varphi)$, $[\boldsymbol{t}_1]_s, \cdots, [\boldsymbol{t}_d]_s$. This, together with lemma 3, proves the proposition. ∎

Now let, for $s \geq 0$, $k(s)$ be the ring class field modulo 2^s over k and $k(s)'$ the maximal 2-extension contained in $k(s)$. Then $k(s)/k$ is abelian, and the Artin map gives isomorphisms

$$\phi(s) \colon R(s) \to Gal(k(s)/k)$$

with $\phi(s)(R(s)') = Gal(k(s)'/k)$. The decomposition law for rational primes in $k(s)$ can be described using binary quadratic forms as follows:

Let $C(s)$ be the composition class group of integral primitive binary quadratic forms $f = aX^2 + bXY + cY^2 \in \boldsymbol{Z}[X, Y]$ with discriminant $D(f) = b^2 - 4ac = -4^s \cdot 4m$; then there is an isomorphism

$$\lambda_s \colon R(s) \xrightarrow{\sim} C(s)$$

(called canonical) such that for each positive rational integer a with $(a, 2m) = 1$ and each class $Q \in C(s)$ the following holds:

Q represents properly a if and only if $a = N(\boldsymbol{a})$ for some integral primitive ideal $\boldsymbol{a}$ with $Q = \lambda_s([\boldsymbol{a}]_s)$.

Concerning the structure of the fields $k(s)$ we will have to use the following corollary to proposition 1:

Corollary 1. *Let L/k be a cyclic extension of degree 4 and suppose $L\subset k(s)$ for some $s\geq 0$; then $L\subset k(3)$.*

Proof. Actually we have $L\subset k(s)'$ for some $s\geq 3$. Let χ: $R(s)'\rightarrow \boldsymbol{C}^{\times}$ be the character of degree 4 defining L, and let ϑ: $R(s)'\rightarrow R(3)'$ be the natural epimorphism defined by $\vartheta([\boldsymbol{a}]_s)=[\boldsymbol{a}]_3$. Then we have to show that there is a factorization $\chi=\chi_0\circ\vartheta$ for some character χ_0: $R(3)'\rightarrow\boldsymbol{C}^{\times}$, but this is equivalent to

$$\mathit{ker}(\vartheta)\subset \mathit{ker}(\chi)\,.$$

Suppose $C\in \mathit{ker}(\vartheta)$; then by proposition 1, **c)**

$$C=[(-1+\sqrt{-m})]_s^{a_0}\cdot\textstyle\prod_{j=1}^d[\boldsymbol{t}_j]_s^{a_j}$$

with $a_0, a_1, \cdots, a_d\in\boldsymbol{N}_0$, and as $\vartheta(C)=1$ we deduce from proposition 1, **b)**

$$\begin{aligned}&a_0\equiv a_1\equiv 0 \mod 4\,,\\ &a_j\equiv 0 \mod 4 \text{ if } j\geq 2 \quad\text{and}\quad t_j\geq 2\,,\\ &a_j\equiv 0 \mod 2 \text{ if } j\geq 2 \quad\text{and}\quad t_j=1\,.\end{aligned}$$

Then

$$\chi(C)=\prod_{\substack{j=1\\ t_j=1}}^{d}\chi([\boldsymbol{t}_j]_s)^{a_j}\,;$$

but if $t_j=1$, $[\boldsymbol{t}_j]_s^2=[(m_j)]_s=1$ and thus $\chi([\boldsymbol{t}_j]_s)^2=1$, which implies $\chi(C)=1$. ■

Now we are well prepared to study the Galois theory and the ramification of those fields, which control the quartic character of ε.

If m is a product of different primes congruent to 1 modulo 8, then the prime divisor of 2 in k lies in the principal genus and therefore there are rational integers $a, b, u\in\boldsymbol{Z}$ such that

$$u>0,\; a+b\sqrt{m}>0,\; 2\nmid u,\; ab\equiv 3 \mod 4$$

and

$$a^2+mb^2=2u^2\,;$$

we fix such a triple (a, b, u) in the sequel and consider the algebraic integer

$$\delta=a+b\sqrt{-m}\in k\,;$$

it has the ideal decomposition

$$(\delta)=\boldsymbol{w}\cdot\boldsymbol{u}^2$$

where $\boldsymbol{w}$ is the prime divisor of 2 in k and $\boldsymbol{u}$ is a primitive integral ideal of k with $N(\boldsymbol{u})=u$.

Proposition 2.

a) *$K(\sqrt[4]{\varepsilon\delta^2(1-i)^2})/k$ is a cyclic extension of degree* 8, *$K(\sqrt[4]{\varepsilon\delta^2(1-i)^2})/\boldsymbol{Q}$ is normal with a dihedral group of order* 16 *as Galois group, and $K(\sqrt[4]{\varepsilon\delta^2(1-i)^2})\subset k(1)$.*

b) *$k(\sqrt{(2+\sqrt{2})\,\delta})/k$ is a cyclic extension of degree* 4, *$k(\sqrt{(2+\sqrt{2})\,\delta})/\boldsymbol{Q}$ is normal with a dihedral group of order* 8 *as Galois group, and $k(\sqrt{(2+\sqrt{2})\,\delta})\subset k(3)$.*

c) *$K(\sqrt[4]{2\varepsilon})/k$ is a cyclic extension of degree* 8, *$K(\sqrt[4]{2\varepsilon})/\boldsymbol{Q}$ is normal with a dihedral group of order* 16 *as Galois group, and $K(\sqrt[4]{2\varepsilon})\subset K(\sqrt[4]{\varepsilon\delta^2(1-i)^2})\cdot k(\sqrt{(2+\sqrt{2})\,\delta})\subset k(3)$, but $K(\sqrt[4]{2\varepsilon})\not\subset k(2)$.*

Proof.

a) We set

$$\eta = \sqrt[4]{\varepsilon\delta^2(1-i)^2}\ ;$$

then $N_{K/k}(\eta^4)=-4\delta^4$, and from [6; Satz 1] we deduce that $K(\eta)/k$ is cyclic of degree 8. Let σ_0 be the generator of the Galois group of K/k; then $\sigma_0(\eta^4)=\varepsilon^{-2}\,\eta^4$, and thus we may fix an extension σ of σ_0 to $K(\eta)$ by setting

$$\sigma(\eta)=\frac{1}{\sqrt{\varepsilon}}\cdot\eta\,,$$

and σ generates the Galois group of $K(\eta)/k$. Let τ_0 be the generator of the Galois group of K/F; then $\tau_0(\eta^4)=[(1-i)\,u\delta^{-1}]^4\cdot\eta^4$ and thus τ_0 has an extension to an automorphism τ of $K(\eta)$ satisfying

$$\tau(\eta)=(1-i)\,u\delta^{-1}\cdot\eta\,.$$

As $\tau_0|k$ generates the Galois group of $k/\boldsymbol{Q}$ we deduce that $K(\eta)/\boldsymbol{Q}$ is normal with Galois group generated by σ and τ. Now we can check the relation

$$\sigma^8=\tau^2=id\,,\quad \sigma\tau=\tau\sigma^{-1}$$

by applying the automorphisms to ε, i and η. Thus the Galois group of $K(\eta)/\boldsymbol{Q}$ is a dihedral group of order 16, and $K(\eta)$ is contained in a ring class field over k by [9; Satz 11].

It remains to show that the conductor $\boldsymbol{f}$ of $K(\eta)/k$ devides 2. By [6; Satz 13] the extension $K(\sqrt{\varepsilon})/k$ is urnamified; thus, if $\boldsymbol{d}$ and $\boldsymbol{d}^*$ denote the relative discriminants of $K(\eta)/K(\sqrt{\varepsilon})$ and $K(\eta)/k$, we have

$$\boldsymbol{d}^*=N_{K(\sqrt{\varepsilon})/k}(\boldsymbol{d})\,.$$

Let χ be a generating character of $K(\eta)/k$ and $\boldsymbol{f}(\chi^j)$ be the conductor of χ^j $(j=0, 1, \cdots, 7)$. Then, by [14; §4], we have the following relations:

$$\boldsymbol{f} = \boldsymbol{f}(\chi^j) \quad \text{for} \quad j \equiv 1 \mod 2\,,$$
$$\boldsymbol{f}(\chi^j) = 1 \quad \text{for} \quad j \equiv 0 \mod 2$$

and

$$\boldsymbol{d}^* = \prod_{j=0}^{7} \boldsymbol{f}(\chi^j) = \boldsymbol{f}^4\,.$$

From these we see that in order to prove $\boldsymbol{f}\,|\,2$ it is sufficient to show $\boldsymbol{d}\,|\,2$; but this demands a careful analysis of the relative quadratic extension $K(\eta)/K(\sqrt{\varepsilon})$. Setting

$$\alpha = \frac{\sqrt{\varepsilon}\cdot\delta}{1-i}\,,$$

we have $K(\eta) = K(\sqrt{\varepsilon})(\sqrt{\alpha})$ and the ideal decomposition of δ shows that $K(\eta)/K(\sqrt{\varepsilon})$ is unramified outside 2. Let $\boldsymbol{w}$ be a prime divisor of 2 in $K(\sqrt{\varepsilon})$; then $ord_{\boldsymbol{w}}(2) = 2$, and thus it is sufficient to show $ord_{\boldsymbol{w}}(\boldsymbol{d}) \leq 2$, which, by [3; §11] is equivalent to:

$$\alpha \text{ is a quadratic residue} \quad \mathrm{mod}^{\times}\ \boldsymbol{w}^3\,.$$

We have

$$\alpha^2(1-i)^2 = \varepsilon\delta^2 = (U+V\sqrt{m})\,(a^2-mb^2+2ab\sqrt{-m})\,;$$

by [6; Satz 13]

$$U \equiv 0 \mod 4\,, \quad V \equiv 1 \mod 4$$

which, together with $ab \equiv 3 \mod 4$ and $a^2-mb^2 \equiv 0 \mod 8$ implies $\alpha^2(1-i)^2 \equiv (1-i)^2 \mod 8$ and thus

$$\alpha^2 \equiv 1 \mod 4\,.$$

Therefore $\dfrac{1+\alpha}{2}$ is an algebraic integer, i.e.

$$\alpha \equiv 1 \mod 2\,.$$

Let $\pi \in K(\sqrt{\varepsilon})$ be an element with $ord_{\boldsymbol{w}}(\pi) = 1$; then

$$\alpha \equiv 1 + \omega\pi^2 \mod \boldsymbol{w}^3$$

for some $\omega \in K(\sqrt{\varepsilon})$. As the prime residue class group modulo $\boldsymbol{w}$ is of odd order, $\omega \equiv \omega_0^2 \mod \boldsymbol{w}$ for some $\omega_0 \in K(\sqrt{\varepsilon})$, and then

$$\alpha \equiv (1+\omega_0\pi)^2 \mod \boldsymbol{w}^3$$

as asserted.

b) We consider the field

$$M = \boldsymbol{Q}(\sqrt{2})(\sqrt{\gamma})$$

with

$$\gamma = (a+u\sqrt{2})(2+\sqrt{2}) \in \boldsymbol{Q}(\sqrt{2})$$

As $N_{\boldsymbol{Q}(\sqrt{2})/\boldsymbol{Q}}(\gamma)=2(a^2-2u^2)=-2mb^2$, $M/\boldsymbol{Q}$ is not normal, its normal closure

$$L = \boldsymbol{Q}(\sqrt{2}, \sqrt{-2m}, \sqrt{\gamma})$$

is cyclic of degree 4 over k, and the Galois group of $L/\boldsymbol{Q}$ is a dihedral group of order 8 [9; Satz 1, 2]. Finally, the identity

$$a+u\sqrt{2} = \delta\cdot\left(\frac{1}{\sqrt{2}}+\frac{u}{\delta}\right)^2$$

shows that

$$L = k(\sqrt{(2+\sqrt{2})\,\delta})\,.$$

The prime ideal decomposition of δ shows that L/k is unramified outside 2, and by [9; Satz 11] $L\subset k(s)$ for some $s\geq 0$, so $L\subset k(3)$ by corollary 1.

c) The Galois theoretic assertion comes from lemma 1. The asserted inclusion of fields follows from the identities

$$(2+\sqrt{2})\cdot\delta\cdot(\zeta-i)^2 = \sqrt{2}\,\delta(1-i)$$

and

$$\sqrt[4]{2\varepsilon} = \sqrt{\sqrt{2}\,\delta(1-i)}\cdot\sqrt{\sqrt{\varepsilon}\,\delta(1-i)}\cdot[\delta(1-i)]^{-1}$$

with

$$\zeta = \frac{1+i}{\sqrt{2}} \in K(\sqrt[4]{\varepsilon\delta^2(1-i)^2})\cdot k(\sqrt{(2+\sqrt{2})\,\delta})\,.$$

Now suppose we have $K(\sqrt[4]{2\varepsilon})\subset k(2)$. By lemma 1, $K(\sqrt[4]{2\varepsilon})/k$ is cyclic of degree 8; let χ: $R(2)\to\boldsymbol{C}^\times$ be a generating character of $K(\sqrt[4]{2\varepsilon})$. Then, by proposition 1, $\chi^2=\psi\circ\theta$ where θ: $R(2)\to R(0)$ is the natural epimorphism defined by $\theta([\boldsymbol{a}]_2)=[\boldsymbol{a}]_0$ and ψ is a character on $R(0)$ of degree 4. Thus, $K(\sqrt{2\varepsilon})/k$ is defined by χ^2 and also by ψ and therefore unramified, a contradiction. ■

Remark. Proposition 2 **a)** generalizes [6; Satz 14, a]; the Galois theoretic assertion in **c)** could equally be deduced from [2; Proposition 1].

Proposition 3. *Suppose $M=K(\sqrt{\delta(1-i)})$; let p be a rational prime with* $p\equiv 1 \bmod 4$, $\left(\frac{q_j}{p}\right)=1$ *for $j=1, \cdots, d$, and let $\boldsymbol{P}$ be a prime divisor of p in F.*

Then there exist $w, r, s \in \boldsymbol{Z}$ *with*

$$(r, s) = 1,\ r-s \equiv 1 \bmod 4,\ 2 \nmid w\,,$$
$$w^2 p = r^2 - ms^2$$

and

$$r + s\sqrt{m} \in \boldsymbol{P}\,.$$

If w, r, s *are as above then* $\boldsymbol{P}$ *splits in* M *if and only if*

$$r-s \equiv 1 \bmod 8\,.$$

If $p \equiv 1 \bmod 8$ *then* $s \equiv 0 \bmod 4$, *and the two prime divisors of* p *in* F *either both split in* M *or both do not; if* $p \equiv 5 \bmod 8$ *then* $s \equiv 2 \bmod 4$ *and exactly one of the prime divisors of* p *in* F *splits in* M.

When showing proposition 3 we shall also prove the following congruence which has not been noticed hitherto:

Proposition 4. *We have*

$$\frac{U}{4} \equiv \frac{u-1}{2} \bmod 2\,.$$

Remark. If m is a prime a short proof of proposition 4 can be given as follows: The prime divisor $\boldsymbol{u}$ of u in k lies in an ideal class of order 4 and thus the class number of k is divisible by 8 if and only if $\boldsymbol{u}$ lies in the principal genus, i.e., $u \equiv 1 \bmod 4$. On the other hand, $U \equiv 0 \bmod 8$, if and only if 8 divides the class number of k [1].

P. Kaplan remarked that proposition 4 can also be deduced from [12] by appealing to theorem 1 and formula (2.6) of that paper (with $A = [2, 2, \frac{1+m}{2}]$ and a square root B_1 of A representing u).

Proof of propositions 3 and 4. The identity

$$\delta \cdot (1-i) \cdot \left\{ \frac{1}{2} + \frac{u}{\delta(1-i)} \right\}^2 = \frac{a + b\sqrt{m}}{2} + u$$

shows that

$$M = K \cdot F\left(\sqrt{\frac{a+b\sqrt{m}}{2} + u} \right),$$

and as $p \equiv 1 \bmod 4$, p splits completely in K. Thus $\boldsymbol{P}$ splits in M if and only if it splits in $F\left(\sqrt{\frac{a+b\sqrt{m}}{2} + u} \right)$.

As $a + b\sqrt{m} > 0$, $u > 0$ and

$$N_{F/Q}\left(\frac{a+b\sqrt{m}}{2}+u\right) = \frac{1}{2}(u+a)^2>0\,,$$

$\dfrac{a+b\sqrt{m}}{2}+u$ is totally positive in F, and $F\left(\sqrt{\dfrac{a+b\sqrt{m}}{2}+u}\right)/F$ is unramified at infinity. As the ideal $(\delta(1-i))$ is a square in K, M/F and thus also $F\left(\sqrt{\dfrac{a+b\sqrt{m}}{2}+u}\right)/F$ are unramified outside 2. Let z, z' be the prime divisors of 2 in F, normed such that

$$\sqrt{m}\equiv-1 \bmod z^2\,, \quad \sqrt{m}\equiv 1 \bmod z'^2\,.$$

Then we have $(1+\sqrt{m})^2=1+m+2\sqrt{m}\equiv 0 \bmod z^4$ and thus

$$\sqrt{m}\equiv-\frac{m+1}{2} \bmod z^3\,.$$

From

$$a^2+mb^2 = (a+b\sqrt{m})(a-b\sqrt{m})+2mb^2 = 2u^2$$

and

$$2mb^2\equiv 2u^2\equiv 2 \bmod 16$$

we deduce

$$(a+b\sqrt{m})(a-b\sqrt{m})\equiv 0 \bmod 16\,,$$

and $ab\equiv 3 \bmod 4$ implies

$$a-b\sqrt{m}\equiv a-b\equiv 2 \bmod z'^2\,;$$

consequently

$$a+b\sqrt{m}\equiv 0 \bmod z'^3\,.$$

This implies

$$\frac{a+b\sqrt{m}}{2}+u\equiv u \bmod z'^2\,;$$

as $N_{F/Q}\left(\dfrac{a+b\sqrt{m}}{2}+u\right)=\dfrac{1}{2}(a+u)^2$, $ord_z\left(\dfrac{a+b\sqrt{m}}{2}+u\right)\equiv 1 \bmod 2$.

Now let f be the conductor and φ the generating ideal character of $F\left(\sqrt{\dfrac{a+b\sqrt{m}}{2}+u}\right)/F$. It follows from [3; §11] that

$$f = z^3 z'^v$$

with

$$v=\begin{cases}0, & \text{if} \quad u\equiv 1 \mod 4\,, \\ 2, & \text{if} \quad u\equiv 3 \mod 4\,.\end{cases}$$

For an integral $\alpha\in F$ with $\alpha\equiv 1$ mod 4 we have in any case

$$\varphi((\alpha))=\begin{cases}1, & \text{if} \quad \alpha\equiv 1 \mod \boldsymbol{z}^3\,, \\ -1, & \text{if} \quad \alpha\equiv 5 \mod \boldsymbol{z}^3\,.\end{cases}$$

Now suppose $p\equiv 1$ mod 4, $\left(\frac{q_j}{p}\right)=1$ for $j=1, \cdots, d$, and let $\boldsymbol{P}$ be a prime divisor of p in F. Then $\boldsymbol{P}$ lies in the principal genus (in the narrow sense), so there is a primitive integral ideal $\boldsymbol{w}$ prime to $2p$ such that $\boldsymbol{w}^2\boldsymbol{P}$ is principal,

$$\boldsymbol{w}^2\boldsymbol{P}=\left(\frac{r'+s'\sqrt{m}}{2}\right)$$

with $r', s'\in \boldsymbol{Z}$, $(r', s')\,|\,2$, $r'\equiv s'$ mod 2 and

$$N(\boldsymbol{w}^2\boldsymbol{P})=w^2p=\frac{r'^2-ms'^2}{4}\,.$$

As $w^2p\equiv 1$ mod 4, we have $r'\equiv s'\equiv 0$ mod 2, $r'=2r$, $s'=2s$,

$$\boldsymbol{w}^2\boldsymbol{P}=(r+s\sqrt{m})\subset \boldsymbol{P}\,,$$
$$w^2p=r^2-ms^2\,,$$

and from $w^2p\equiv 1$ mod 4 we deduce $r\equiv 1$ mod 2, $s\equiv 0$ mod 2. By changing signs if necessary we may assume

$$r-s\equiv 1 \mod 4\,.$$

Then we obtain

$$r+s\sqrt{m}\equiv r+s\equiv r-s\equiv 1 \mod 4\,,$$

and as

$$r+s\sqrt{m}\equiv r-s \mod \boldsymbol{z}^3\,,$$

we deduce:

$$\varphi((r+s\sqrt{m}))=1 \quad \text{if and only if} \quad r-s\equiv 1 \mod 8\,.$$

Now $\boldsymbol{P}$ splits in $F\left(\sqrt{\frac{a+b\sqrt{m}}{2}+u}\right)$ if and only if $\varphi(\boldsymbol{P})=1$, but

$$\varphi(\boldsymbol{P})=\varphi((r+s\sqrt{m}))\,,$$

and this proves the first part of proposition 3; the second part is obvious.

To prove proposition 4, consider $\varepsilon=U+V\sqrt{m}$ and observe that

$$U \equiv 0 \bmod 4,\ V \equiv \frac{m+1}{2} \bmod 8$$

by [6; Satz 13], which implies

$$\varepsilon \equiv U - \left(\frac{1+m}{2}\right)^2 \equiv U-1 \bmod \mathfrak{z}^3,$$

whilst

$$\varepsilon \equiv \sqrt{m} \equiv 1 \bmod \mathfrak{z}'^2,$$

If now $v=0$, $F\left(\sqrt{\frac{a+b\sqrt{m}}{2}+u}\right)/F$ has conductor $\mathfrak{z}^3$ and thus there is no unit η in F with $\eta \equiv 1 \bmod \mathfrak{z}^2$, $\eta \not\equiv 1 \bmod \mathfrak{z}^3$. As $-\varepsilon \equiv 1 \bmod \mathfrak{z}^2$ we have $-\varepsilon \equiv 1-U \equiv 1 \bmod \mathfrak{z}^3$ which implies $U \equiv 0 \bmod 8$.
If $v=2$, $F\left(\sqrt{\frac{a+b\sqrt{m}}{2}+u}\right)/F$ has conductor $\mathfrak{z}^3\mathfrak{z}'^2$ and thus there is no unit η in F with $\eta \equiv 1 \bmod \mathfrak{z}^3$, $\eta \not\equiv 1 \bmod \mathfrak{z}^3\mathfrak{z}^{2\prime}$. As $-\varepsilon \not\equiv 1 \bmod \mathfrak{z}'^2$ we have $-\varepsilon \equiv 1-U \not\equiv 1 \bmod \mathfrak{z}^3$ which implies $U \equiv 4 \bmod 8$. ■

5. Residuacity criteria for splitting primes

Theorem 2. *Suppose $m=q_1\cdot\cdots\cdot q_d$ is a product of $d\geq 1$ different primes $q_j\equiv 1 \bmod 8$ and suppose that the ideal class group of k has only one invariant 2^t $(t\geq 2)$ divisible by 4; then the fundamental unit $\varepsilon=\varepsilon_m$ of F satisfies $N_{F/Q}(\varepsilon)=-1$.*

Let l be a prime satisfying $l\equiv 3 \bmod 4$ and $l^{2^t}=\xi^2+m\eta^2$ with $\xi, \eta\in \boldsymbol{Z}$, $(\xi, \eta)=1$.

Let p be a prime such that $p\equiv 1 \bmod 4$ and $\left(\frac{q_j}{p}\right)=1$ for $j=1, \cdots, d$, and let $\boldsymbol{P}$ be a prime divisor of p in F; suppose

$$w^2p = r^2-ms^2$$

with $w, r, s\in\boldsymbol{Z}$ such that

$$(r, s) = 1,\ r-s\equiv 1 \bmod 4,\ 2\nmid w$$

and

$$r+s\sqrt{m}\in\boldsymbol{P}.$$

A. *There is a unique exponent $n\in\boldsymbol{N}_0$ satisfying $n\leq 2^{t-1}$ such that*

$$(*)\qquad l^{2n}p^h = X^2+4mY^2$$

with $X, Y\in\boldsymbol{Z}$, $(X, Y)=1$.

B. *The following assertions are equivalent:*

a) $\left(\frac{\varepsilon}{p}\right)=1$;

b) *In* $(*)$, *we have* $n\equiv 0 \bmod 2$;

c) p *is represented by a class* $Q\in C(0)$ *which is a 4-th power.*

d) $p^{2^{t-2}h}=x^2+my^2$ *with* $x, y\in \boldsymbol{Z}$, $(x, y)=1$.

e) p *is represented by a class* $Q\in C(1)$ *which is a 4-th power.*

f) $p^{2^{t-1}h}=x^2+4my^2$ *with* $x, y\in \boldsymbol{Z}$, $(x, y)=1$.

C. *Suppose* $\left(\frac{\varepsilon}{p}\right)=1$, *i.e.* $n\equiv 0 \bmod 2$ *in* $(*)$. *Then*

$$\left(\frac{\varepsilon}{\boldsymbol{P}}\right)_4=(-1)^{(n/2)+(r-s-1/4)}.$$

D. *Suppose* $\left(\frac{\varepsilon}{p}\right)=1$ *and* $p\equiv 1 \bmod 8$. *Then, in* $(*)$ *we have* $n\equiv Y\equiv 0 \bmod 2$, *and*

$$\left(\frac{2\varepsilon}{p}\right)_4=(-1)^{(n/2)+(Y/2)}.$$

E. *Suppose* $\left(\frac{\varepsilon}{p}\right)=1$ *and* $p\equiv 1 \bmod 8$; *let* $Q\in C(3)$ *represent* p. *Then either*

$$(I) \qquad p^{2^{t-2}h}=X^2+16mY^2$$

or

$$(II) \qquad p^{2^{t-2}h}=16X^2+mY^2$$

with $X, Y\in\boldsymbol{Z}$, $(X, Y)=1$, *and we obtain*:

$$\left(\frac{2\varepsilon}{p}\right)_4=1$$

if and only if

in case (I): Q *is an* 8*-th power*;

in case (II): Q *is no* 4*-th power.*

F. *Suppose* $p\equiv 1 \bmod 8$ *and* $p^h=16X^2+mY^2$ *with* $X, Y\in\boldsymbol{Z}$, $(X, Y)=1$. *Then* $\left(\frac{\varepsilon}{p}\right)=1$, *and we have*

$$\left(\frac{2\varepsilon}{p}\right)_4=(-1)^{2^{t-2}+X}.$$

Remark. 1. In theorem 2, l plays the role of an auxiliary parameter. If C is an absolute ideal class of k of order 2^t and $\boldsymbol{l}\in C$ is a prime ideal of degree 1 then the underlying prime l satisfies all requirements.

2. Criteria for the quadratic character of ε under more general conditions were proved in [6]; for a different approach see [2].

Proof. $N_{F/Q}(\varepsilon)=-1$ follows from [6; Satz 14]. The assumption concerning the ideal class group implies $t_1=t\geq 2$ and $t_j=1$ for $j=2, \cdots, d$ in the terminology of §4. Let $\mathfrak{p}$ be a prime divisor of p in k.

For $s\geq 0$, let $k(s)^*$ be the genus field of $k(s)$, i.e. the greatest absolutely abelian subfield of $k(s)$. Then, by [10],

$$k(s)^* = \begin{cases} k(\sqrt{q_1}, \cdots, \sqrt{q_{d-1}}, \sqrt{-1}), & \text{if } s\leq 1, \\ k(\sqrt{q_1}, \cdots, \sqrt{q_{d-1}}, \sqrt{-1}, \sqrt{2}), & \text{if } s\geq 2, \end{cases}$$

and $k(s)^*$ is the greatest multiquadratic extension of k inside $k(s)$.

As $p\equiv 1 \bmod 4$ and $\left(\frac{q_j}{p}\right)=1$ for $j=1, \cdots d$, p splits completely in $k(s)^*$ for $s\leq 1$; but this implies $\varphi([\mathfrak{p}]_s)=1$ for all quadratic characters φ of $R(s)$, i.e. $[\mathfrak{p}]_s$ is a square in $R(s)$ for $s\leq 1$. If, in addition, $p\equiv 1 \bmod 8$, then $[\mathfrak{p}]_s$ is a square in $R(s)$ also for $s\geq 2$.

By proposition 1, $R(3)'$ is of type $(4, 2^{t+1}, 2, \cdots, 2)$ with basis $([(-1+2\sqrt{-m})]_3, [\mathfrak{t}_1]_3, \cdots, [\mathfrak{t}_s]_3)$, and we set

$$C_0 = [(-1+2\sqrt{-m})]_3,\ C_1 = [\mathfrak{t}_1]_3\,.$$

For $s\leq 3$, let ω_s: $R(3)\rightarrow R(s)$ be the canonical epimorphism defined by $\omega_s([\mathfrak{a}]_3)=[\mathfrak{a}]_s$; then $ker(\omega_2)=\langle C_0^2\rangle$, $ker(\omega_1)=\langle C_0\rangle$ and $ker(\omega_0)=\langle C_0, C_1^{2^t}\rangle$. From $C_1^{2^t}=[(\sqrt{-m})]_3$ we see that, for $s\leq 3$, $\lambda_s\circ\omega_s(C_1^{2^t})$ contains the form $4^sX^2+mY^2$.

By proposition 2, $K(\sqrt[4]{\varepsilon\delta^2(1-i)^2})$ is a cyclic extension of k of degree 8 contained in $k(1)$. Let χ_1: $R(1)\rightarrow \boldsymbol{C}^\times$ be a generating character for $K(\sqrt[4]{\varepsilon\delta^2(1-i)^2})/k$; then (by raising χ_1 to an odd power if necessary) we may assume $\chi_1([\mathfrak{t}_1]_1)=\zeta$, where $\zeta=\frac{1+i}{\sqrt{2}}\in \boldsymbol{C}^\times$ is a primitive 8-th root of unity. Then $\chi=\chi_1\circ\omega_1$: $R(3)\rightarrow \boldsymbol{C}^\times$ also defines $K(\sqrt[4]{\varepsilon\delta^2(1-i)^2})$, χ^2 defines $K(\sqrt{\varepsilon})$, χ^4 defines K, and we have

$$\chi(C_0) = 1\,,\quad \chi(C_1) = \zeta\,.$$

As $[\mathfrak{p}]_1$ is a square in $R(1)$, we may set

$$[\mathfrak{p}]_3 = C_0^{a'}\cdot C_1^{2b}\cdot U$$

with $a', b\in \boldsymbol{N}_0$, $a'<4$, $b<2^t$ and a class $U\in R(3)$ of odd order.

Proof of **A**. As $l^{2^t}=r^2+ms^2$, $\left(\frac{-m}{l}\right)=1$, and $(l)=\mathfrak{l}_1\mathfrak{l}_2$ with different prime ideals $\mathfrak{l}_1$, $\mathfrak{l}_2$ of k which lie in ideal classes of even order. ω_0 induces an isomorphism of the odd parts of $R(3)$ and $R(0)$, and thus we have

$$[\mathfrak{l}_1]_3 = C_0^\nu C_1^\mu T,\ [\mathfrak{l}_2]_3 = C_0^{2-\nu} C_1^{2^t-\mu} T$$

with exponents ν, $\mu\in \boldsymbol{N}_0$, $\nu<2$, $\mu<2^t$ and a class $T\in R(3)$ with $T^2=1$. As $l\equiv 3 \bmod 4$, $\mathfrak{l}_1$ is inert in K, and thus $-1=\chi^4([\mathfrak{l}_1]_3)=(-1)^\mu$, i.e.

$$\mu \equiv 1 \mod 2 .$$

Now, for $n \in \boldsymbol{N}_0$ the integer $l^{2n} p^h$ is properly represented by the classes $\lambda_1([\boldsymbol{l}_1^{2n} \boldsymbol{p}^h]_1)$, $\lambda_1([\boldsymbol{l}_2^{2n} \boldsymbol{p}^h]_1)$ and their inverses in $C(1)$. So the existence of X, $Y \in \boldsymbol{Z}$ with $(X, Y)=1$ and $l^{2n} p^h = X^2 + 4mY^2$ is equivalent to $[\boldsymbol{l}_1^{2n} \boldsymbol{p}^h]_1 = 1$ or $[\boldsymbol{l}_2^{2n} \boldsymbol{p}^h]_1 = 1$, i.e. to $[\boldsymbol{l}_j^{2n} \boldsymbol{p}^h]_3 \in \langle C_0 \rangle$ for $j=1$ or $j=2$. From

$$[\boldsymbol{l}_1^{2n} \boldsymbol{p}^h]_3 = C_0^{a'h+2n\nu} \cdot C_1^{2bh+2n\mu} ,$$
$$[\boldsymbol{l}_2^{2n} \boldsymbol{p}^h]_3 = C_0^{a'h-2n\nu} \cdot C_1^{2bh-2n\mu}$$

we see that it is sufficient to show that there is a unique $n \in \boldsymbol{N}_0$ with $n \leq 2^{t-1}$ for which one of the congruences

$$2bh \pm 2n\mu \equiv 0 \mod 2^{t+1}$$

holds; but this is obvious.

Proof of **B.** As $p \equiv 1 \mod 4$, $\left(\frac{\varepsilon}{p}\right)$ is well defined, and as χ^2 defines $K(\sqrt{\varepsilon})$,

$$\left(\frac{\varepsilon}{p}\right) = 1, \quad \text{if and only if} \quad \chi^2([\boldsymbol{p}]_3) = 1 .$$

From the above we deduce

$$\left(\frac{\varepsilon}{p}\right) = \chi^2([\boldsymbol{p}]_3) = (-1)^b ,$$

and the congruence $2bh \pm 2n\mu \equiv 0 \mod 2^{t+1}$ together with $t \geq 2$ and $h \equiv \mu \equiv 1 \mod 2$ implies

$$b \equiv n \mod 2 ,$$

thus

$$\left(\frac{\varepsilon}{p}\right) = (-1)^n ,$$

which proves the equivalence of **a**) and **b**).

For $s \in \{0, 1\}$, p is represented by the class $\lambda_s \circ \omega_s([\boldsymbol{p}]_3) = \lambda_s([\boldsymbol{t}_1]_s)^{2b} \cdot \lambda_s \circ \omega_s(U)$ and its inverse in $C(s)$, and as $\lambda_s \circ \omega_s(U)$ is of odd order, p is represented by a 4-th power in $C(s)$ if and only if $b \equiv 0 \mod 2$; this proves the equivalence of **a**) with **c**) and **e**).

For $s \in \{0, 1\}$, $p^{2^{t+s-2}h}$ is properly represented by the class $\lambda_s([\boldsymbol{t}_1]_s)^{2^{t+s-2}bh}$, and this is the principal class if and only if $b \equiv 0 \mod 2$; this proves the equivalence of **a**) with **d**) and **f**).

Proof of **C**: If $\left(\frac{\varepsilon}{p}\right) = 1$, then by **B.** we have $n \equiv b \equiv 0 \mod 2$, and from $2bh \pm 2n\nu \equiv 0 \mod 2^{t+1}$, $t \geq 2$ and $h \equiv \mu \equiv 1 \mod 2$ we infer

$$\frac{b}{2} \equiv \frac{n}{2} \mod 2.$$

Now let $\boldsymbol{P}_K$ be a prime divisor of $\boldsymbol{P}$ in K; as $K(\sqrt[4]{\varepsilon\delta^2(1-i)^2})/\boldsymbol{Q}$ is normal, $\boldsymbol{P}_K$ splits in $K(\sqrt[4]{\varepsilon\delta^2(1-i)^2})$ if and only if p does; therefore, $\boldsymbol{P}_K$ splits in $K(\sqrt[4]{\varepsilon\delta^2(1-i)^2})$ if and only if $\boldsymbol{p}$ does, and as χ defines $K(\sqrt[4]{\varepsilon\delta^2(1-i)^2})$, this is equivalent to $\chi([\boldsymbol{p}]_3)=1$. As

$$\chi([\boldsymbol{p}]_3) = (-1)^{b/2} = (-1)^{n/2},$$

we obtain

$$(-1)^{n/2} = \left(\frac{\varepsilon\delta^2(1-i)^2}{\boldsymbol{P}_K}\right)_4 = \left(\frac{\varepsilon}{\boldsymbol{P}_K}\right)_4 \cdot \left(\frac{\delta(1-i)}{\boldsymbol{P}_K}\right).$$

The prime residue class groups of $\boldsymbol{P}$ and $\boldsymbol{P}_K$ coincide, thus we conclude

$$\left(\frac{\varepsilon}{\boldsymbol{P}_K}\right)_4 = \left(\frac{\varepsilon}{\boldsymbol{P}}\right)_4.$$

As $\left(\frac{\delta(1-i)}{\boldsymbol{P}_K}\right)=1$ if and only if $\boldsymbol{P}_K$ splits in $K(\sqrt{\delta(1-i)})$, it follows from proposition 3 that

$$\left(\frac{\delta(1-i)}{\boldsymbol{P}_K}\right) = (-1)^{(r-s-1)/4}.$$

Putting all together, we deduce

$$\left(\frac{\varepsilon}{\boldsymbol{P}}\right)_4 = (-1)^{(r-s-1)/4+\frac{n}{2}}.$$

Proof of **D**: Let ψ: $R(3)\to \boldsymbol{C}^\times$ be a generating character for $K(\sqrt[4]{2\varepsilon})/k$. By raising ψ to an odd power if necessary, we may assume that

$$\psi(C_1) = \zeta.$$

By proposition 2, $K(\sqrt[4]{2\varepsilon}) \not\subset k(2)$, thus $ker(\omega_2)=\langle C_0^2\rangle \not\subset ker(\psi)$ and consequently

$$\psi(C_0) = \pm i.$$

As $p\equiv 1 \bmod 8$, $[\boldsymbol{p}]_3 \in R(3)$ is a square, and thus $a'\equiv 0 \bmod 2$,

$$a' = 2a,\ 0\le a<2.$$

From $\left(\frac{\varepsilon}{p}\right)=1$ we deduce as in the proof of $\boldsymbol{C}$. $b\equiv n\equiv 0 \bmod 2$ and

$$\frac{b}{2} \equiv \frac{n}{2} \mod 2.$$

This implies

$$\left(\frac{2\varepsilon}{p}\right)_4 = \psi([p]_3) = (-1)^{(b/2)+a} = (-1)^{(n/2)+a}\,.$$

In (*), we have $Y\equiv 0 \bmod 4$ if and olny if $l^{2n}p^h$ is properly represented by the principal class of $C(3)$; but as $l^{2n}p^h$ is properly represented by the classes $\lambda_3([l_j^{2n}\,p^h]_3)$ $(j=1, 2)$ and their inverses in $C(3)$, $Y\equiv 0 \bmod 4$ is equivalent to

$$1=[l_j^{2n}\,p^h]_3 = C_0^{2ah}\cdot C_1^{2bh\pm 2n\mu}$$

for $j=1$ or $j=2$, i.e. for one choice of the sign in the exponent of C_1. As n was determined so that $2bh\pm 2n\mu\equiv 0 \bmod 2^{t+1}$ for one choice of the sign, $Y\equiv 0 \bmod 4$ is equivalent to $a\equiv 0 \bmod 2$, thus

$$a\equiv\frac{Y}{2} \bmod 2$$

and

$$\left(\frac{2\varepsilon}{p}\right)_4 = (-1)^{(n/2)+(Y/2)}\,.$$

Proof of **E**: As $\left(\frac{\varepsilon}{p}\right)=1$ and $p\equiv 1 \bmod 8$ we have $a'=2a$, $b\equiv n\equiv 0 \bmod 2$ and $\frac{b}{2}\equiv\frac{n}{2} \bmod 2$ as in the proof of ***C***. p is represented by the class $\lambda_3(C_0^{2a}\,C_1^{2b}\cdot U)$ and its inverse in $C(3)$. Thus, if $Q\in C(3)$ represents p, Q is a 4-th power if and only if $a\equiv 0 \bmod 2$.

As p^{2^t-2h} is properly represented by the ambiguous class $\lambda_2\circ\omega_2(C_1^{2^{t-1}b})\in C(2)$, we deduce

$$b\equiv 0 \bmod 4 \text{ in case (I)}\,,$$
$$b\equiv 2 \bmod 4 \text{ in case (II)}\,.$$

As in the proof of ***D***. we obtain

$$\left(\frac{2\varepsilon}{p}\right)_4 = (-1)^{(n/2)+a} = (-1)^{(b/2)+a}\,.$$

In case (I), $b\equiv 0 \bmod 4$ and thus $\left(\frac{2\varepsilon}{p}\right)_4=1$ if and only if $a\equiv 0 \bmod 2$, i.e. Q is an 8-th power. In case (II), $b\equiv 2 \bmod 4$ and thus $\left(\frac{2\varepsilon}{p}\right)_4=1$ if and only if $a\equiv 1 \bmod 2$, i.e. Q is not a 4-th power.

Proof of **F**: As $p\equiv 1 \bmod 8$, we have $a'\equiv 0 \bmod 2$, $a'=2a$, and p is represented by the classes $\lambda_3(C_0^{2a}\,C_1^{2b}U)^{\pm 1}\in C(3)$; thus p^h is properly represented by $\lambda_3(C_0^{2a}\,C_1^{2bh})^{\pm 1}\in C(3)$ and by $\lambda_2\circ\omega_2(C_0^{2a}\,C_1^{2bh})^{\pm 1}=\lambda_2\circ\omega_2(C_1^{\pm 2bh})\in C(2)$. As $p^h=16X^2+mY^2$ with $X, Y\in\boldsymbol{Z}$, $(X, Y)=1$, p^h is also properly represented by $\lambda_2\circ\omega_2(C_1^{2^t})$ and this implies

$$b = 2^{t-1}.$$

As in **B**. we have $b \equiv n \bmod 2$ and thus

$$\left(\frac{\varepsilon}{p}\right) = (-1)^b = 1.$$

Further, we have $X \equiv 0 \bmod 2$ if and only if p^h is properly represented by $\lambda_3(C_1^{2^t})$, and as p^h is properly represented by $\lambda_3(C_0^{2a}C_1^{2^t})$ this is equivalent to $a \equiv 0 \bmod 2$. This implies

$$a \equiv X \bmod 2$$

and

$$\left(\frac{2\varepsilon}{p}\right)_4 = (-1)^{(b/2)+a} = (-1)^{2^{t-2}+X}.$$

6. Residuacity criteria for ramified primes

In this final section we assume that m is a prime and consider ε_m modulo the prime dividing m.

Theorem 3. *Let* $m=q\equiv 1 \bmod 4$ *be a prime and* $\mathfrak{q}=(\sqrt{q})$ *the prime divisor of* q *in* F. *Then*:

a) *If* $q\equiv 5 \bmod 8$, $\left(\frac{\varepsilon_q}{\mathfrak{q}}\right)=-1$.

b) *If* $q\equiv 1 \bmod 8$, $\left(\frac{\varepsilon_q}{\mathfrak{q}}\right)=1$,

$$\left(\frac{\varepsilon_q}{\mathfrak{q}}\right)_4 = (-1)^{(q-1)/8} \quad \textit{and} \quad \left(\frac{2\varepsilon_q}{\mathfrak{q}}\right)_4 = (-1)^{2^{t-2}}.$$

Proof. $\varepsilon_q = U+V\sqrt{q}$, and $U^2-qV^2=-1$. Therefore we have $\varepsilon_q \equiv U \bmod \mathfrak{q}$,

$$\left(\frac{\varepsilon_q}{\mathfrak{q}}\right) = \left(\frac{U}{q}\right) = \left(\frac{U^2}{q}\right)_4 = \left(\frac{-1}{q}\right)_4 = (-1)^{(q-1)/4}$$

and, if $q\equiv 1 \bmod 8$,

$$\left(\frac{\varepsilon_q}{\mathfrak{q}}\right)_4 = \left(\frac{U}{q}\right)_4 = \left(\frac{U^2}{q}\right)_8 = \left(\frac{-1}{q}\right)_8 = (-1)^{(q-1)/8}.$$

To show $\left(\frac{2\varepsilon_q}{\mathfrak{q}}\right)_4=(-1)^{2^{t-2}}$ we adopt the terminology of the proof of theorem 2. Then

$$[\mathfrak{q}]_3 = [(\sqrt{-q})]_3 = C_1^{2^t}$$

and

$$\left(\frac{2\varepsilon_q}{q}\right)_4 = \psi([q]_3) = (-1)^{2^{t-2}}. \blacksquare$$

Corollary 3. *$t \geq 3$ if and only if* $\left(\frac{-4}{q}\right)_8 = 1$.

Proof. $(-1)^{2^{t-2}} = \left(\frac{2\varepsilon_q}{q}\right)_4 = \left(\frac{2}{q}\right)_4 \cdot \left(\frac{\varepsilon_q}{q}\right)_4 = \left(\frac{2}{q}\right)_4 \left(\frac{-1}{q}\right)_8 = \left(\frac{-4}{q}\right)_8$, by the theorem. ■

Remark. Corollary 3 was first proved in [1]; it is not surprising that an extensive study of the structure of the ring class fields as we have done in this paper delivers this basic fact too.

References

[1] P. Barrucand and H. Cohn: *Note on primes of type x^2+32y^2, class number and residuacity,* J. Reine Angew. Math. **238** (1969), 67–70.

[2] Y. Chuman and N. Ishii: *On the quartic residue of quadratic units of negative norm,* Math. Japonica **32** (1987), 389–420.

[3] H. Hasse: Bericht über neuere Untersuchungen und Probleme aus der Theorie der algebraischen Zahlkörper, Teil I a. Physica-Verlag, Würzburg 1965.

[4] H. Hasse: Number Theory. Springer 1980.

[5] H. Hasse: Bericht über neuere Untersuchungen und Probleme aus der Theorie der algebraischen Zahlkörper, Teil II. Physica-Verlag, Würzburg 1965.

[6] F. Halter-Koch: *Konstruktion von Klassenkörpern und Potenzrestkriterien für quadratische Einheiten,* Manuscripta Math. **54** (1986), 453–492.

[7] F. Halter-Koch: Quadratische Einheiten als 8. Potenzreste, Proc. Int. Conf. on Class Numbers and Fundamental Units, Katata, Japan, 1986.

[8] F. Halter-Koch: *Einseinheitengruppen und prime Restklassengruppen in quadratischen Zahlkörpern,* J. Number Theory **6** (1972), 70–77.

[9] F. Halter-Koch: *Arithmetische Theorie der Normalkörper von 2-Potenzgrad mit Diedergruppe,* J. Number Theory **3** (1971), 412–443.

[10] F. Halter-Koch: *Geschlechtertheorie der Ringklassenkörper,* J. Reine Angew. Math. **250**, (1971), 107–108.

[11] N. Ishii: *On the quartic residue symbol of totally positive quadratic units,* Tokyo J. of Math. **9** (1986), 53–65.

[12] P. Kaplan and K.S. Williams: *An Artin Character and Representations of Primes by Binary Quadratic Forms,* Manuscpipta Math. **33** (1981), 339–356.

[13] P.A. Leonard and K.S. Williams: *The quadratic and quartic character of certain quadratic units II,* Rocky Mountain J. Math. **9** (1979), 683–692.

[14] J.-P. Serre: Local Class Field Theory, in "Algebraic Number Theory", ed. by J.W.S. Cassels and A. Fröhlich. Academic Press 1967.

Franz Halter-Koch
Institut für Mathematik

der Karl-Franzens-Universität
Halbärthgasse 1/I,A-8010 Graz
Austria

Noburo Ishii
Department of Mathematics
University of Osaka Prefecture
Sakai, Osaka 591
Japan