Ann. Inst. Fourier, Grenoble
30, 2 (1980). 1-15.

PURE FIELDS OF DEGREE 9 WITH CLASS NUMBER PRIME TO 3

by Colin D. WALTER

In a well-known paper, Honda [5] found the precise rational conditions on $n \in \mathbf{Z}$ which determine when $\mathbf{Q}(\sqrt[3]{n})$ has class number divisible by 3. More recently, Endô [3] has tackled this problem for $\mathbf{Q}(\sqrt[9]{n})$ using the same techniques: a class number relation and the calculation of an ambiguous class number by norm residue symbols. His results are incomplete, although most of the residue symbols required to solve the problem are given by him. Here the main theorem (5.5) extends his work so that with only a few possible exceptions the necessary and sufficient rational conditions are now known for $\mathbf{Q}(\sqrt[9]{n})$ to have class number prime to 3 .

1. Class number relations.

Let M_2/K_0 be a normal extension of number fields whose Galois group is

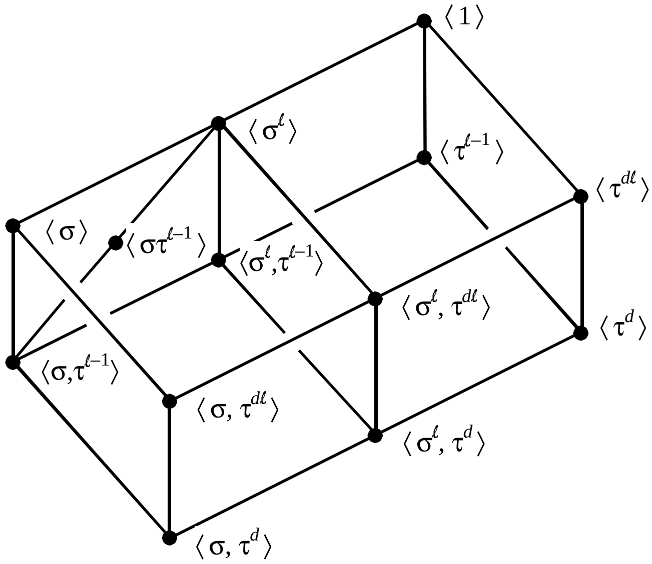
$$G = \langle \sigma, \tau \mid \sigma^{\ell^2} = \tau^{\ell(\ell-1)} = 1, \sigma\tau = \tau\sigma^r \rangle$$

where ℓ is an odd prime and r is an integer of order $\ell(\ell-1)$ modulo ℓ^2. R. Brauer [2] has shown that a class number relation can be obtained from any relation between the characters of G induced from the unit characters of its subgroups. To find all such relationships it is necessary to specify the conjugacy classes of subgroups.

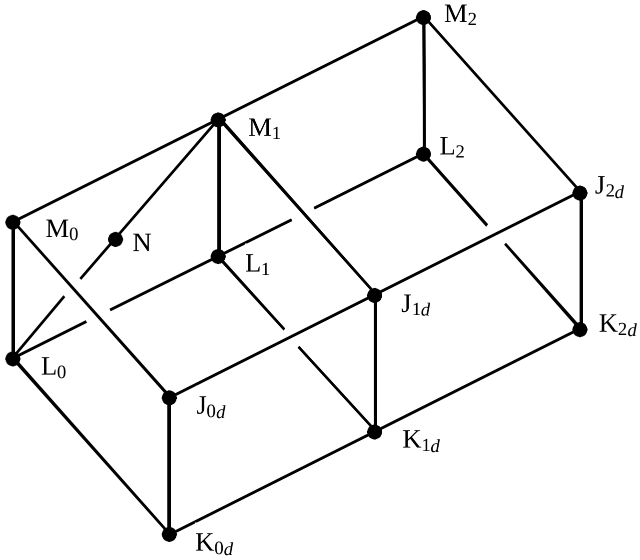
A Sylow ℓ-subgroup of any subgroup of G is contained in the normal Sylow ℓ-subgroup $G_\ell = \langle\sigma,\tau^{\ell-1}\rangle$ of G. The cyclic subgroups of G_ℓ with order ℓ^2 are $\langle\sigma\rangle \lhd G$ and $\langle\sigma\tau^{(\ell-1)i}\rangle$ for $0 < i < \ell$. The latter subgroups are conjugate under powers of τ. The ℓ^2 elements of G_ℓ which are not of order ℓ^2 form the unique non-cyclic subgroup of G with order ℓ^2, *viz.* $\langle\sigma^\ell, \tau^{\ell-1}\rangle \lhd G$. Hence the subgroups of order ℓ lie in $\langle\sigma^\ell, \tau^{\ell-1}\rangle$ and are $\langle\sigma^\ell\rangle \lhd G$ and $\langle\sigma^{\ell i}\tau^{\ell-1}\rangle$ for $0 \le i < \ell$. The latter subgroups are conjugate under powers of τ. Because the image of a subgroup in G/G_ℓ is cyclic, the subgroup is generated from one of the above ℓ-groups together with an element of order dividing $\ell-1$ which normalises the ℓ-group. The only such elements have the form $\sigma^i\tau^{d\ell}$ for $0 < d < \ell-1$ or 1 itself. Replacing $\sigma^i\tau^{d\ell}$

by a suitable power and a conjugate ensures that all subgroups are obtained by adjoining $\tau^{d\ell}$ where $d \mid (\ell - 1)$ and taking all conjugates of the resulting subgroups.

So for $d \mid \ell - 1$ the unique subgroup of order $\ell^3(\ell - 1)/d$ is $\langle\sigma, \tau^d\rangle \lhd G$; the subgroups of order $\ell^2(\ell - 1)/d$ are $\langle\sigma, \tau^{d\ell}\rangle \lhd G$, the $\ell - 1$ conjugates of $\langle\sigma\tau^{\ell-1}\rangle$ when $d = \ell - 1$ and the 1 or ℓ conjugates of $\langle\sigma^\ell, \tau^d\rangle$; the subgroups of order $\ell(\ell - 1)/d$ are the 1 or ℓ conjugates of $\langle\sigma^\ell, \tau^{d\ell}\rangle$ and the ℓ or ℓ^2 conjugates of $\langle\tau^d\rangle$; and the subgroups of order $(\ell - 1)/d$ are the ℓ or ℓ^2 conjugates of $\langle\tau^{d\ell}\rangle$. Each conjugacy class is represented in the following diagram as d varies over proper divisors of $\ell - 1$:



The corresponding subfields can be named thus :



and the subscript d will be omitted when $d = 1$.

The total number of classes is $6t + 1$ where t is the number of divisors of $\ell - 1$, and of these $2t + 3$ are cyclic. This means there are $4t - 2$ independent relations between the induced unit characters $\chi(\Omega)$ from the subgroup fixing Ω. They can be expressed in the following way and are easily verified :

(1.1) $\quad d'\chi(K_{1d}) - d'\chi(K_{0d}) = \chi(L_1) - \chi(L_0)$

(1.2) $\quad d'\chi(K_{2d}) - d'\chi(K_{1d}) = \chi(L_2) - \chi(L_1)$

(1.3) $\quad d'\chi(J_{1d}) - d'\chi(J_{0d}) = \chi(M_1) - \chi(M_0)$

(1.4) $\quad d'\chi(J_{2d}) - d'\chi(J_{1d}) = \chi(M_2) - \chi(M_1)$.

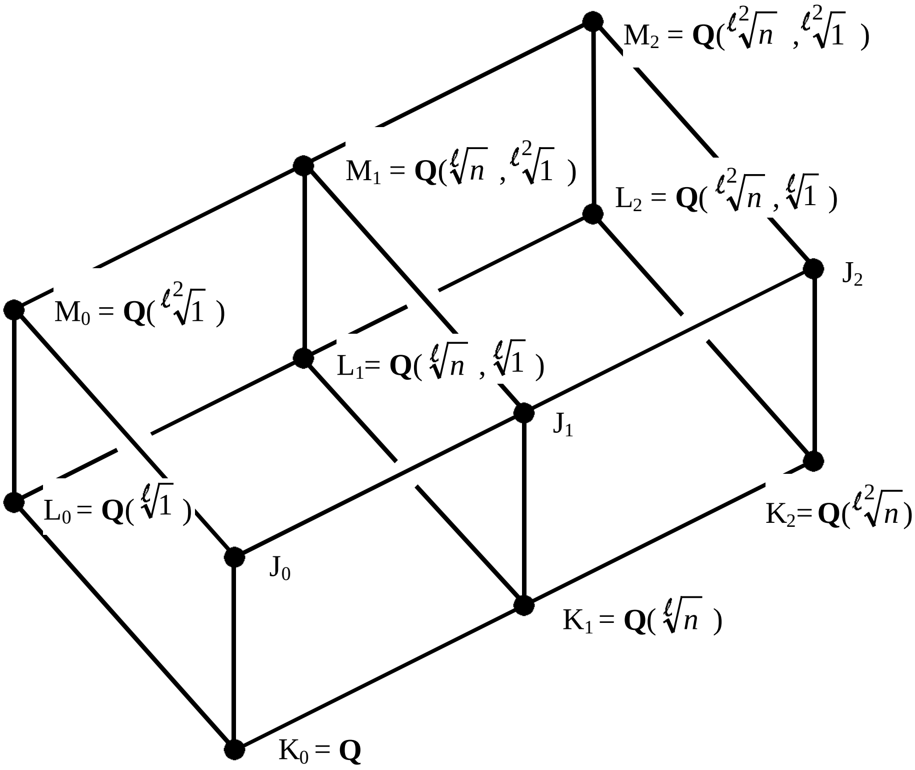
Here d' is defined by $dd' = \ell - 1$ and d is a proper divisor of $\ell - 1$. The remaining two independent relations are :

(1.5) $\quad \ell\chi(L_2) - \ell\chi(L_1) = \chi(M_2) - \chi(M_1)$

(1.6) $\quad (\ell-1)\chi(N) - (\ell-1)\chi(L_0) = \chi(M_1) - \chi(M_0)$.

Each of these relations is of standard type for which the corresponding class number relation is known. The first four are of Frobenius type (see [8]) and the last two are of Kuroda type (see [9]), whilst equations (1.3) and (1.4) add to give a further Frobenius type relation.

Suppose $n \in \mathbf{Z}$ is such that $K_2 = \mathbf{Q}(\sqrt[\ell^2]{n})$ has degree ℓ^2 over $\mathbf{Q}$. Then the normal extension $M_2/K_0 = \mathbf{Q}(\sqrt[\ell^2]{n}, \sqrt[\ell^2]{1})/\mathbf{Q}$ has G as its Galois group and its subfields for $d = 1$ are :



Let h_Ω be the class number and U_Ω the unit group of a field Ω. If

$$I(k_1/k_2) = (U_{k_1}/U_{k_2})_{\mathrm{tor}}$$

for an extension k_1/k_2 and $(k_1 : k_2) = \ell$ then $I(k_1/k_2) \neq 1$ implies $k_1 = k_2(\sqrt[\ell]{e})$ for some $e \in U_{k_2}$ (see [9] § 4). There is no such extension of $\mathbf{Q}$ and so $I(K_1/\mathbf{Q}) = 1$. If $K_2 = K_1(\sqrt[\ell]{e})$ for $e \in U_{K_1}$ then $\sqrt[\ell]{e} = e^i\alpha^\ell$ for some $\alpha \in K_1$ and i prime to ℓ. Hence $n = (\pm N_{K_1/\mathbf{Q}}\alpha)^\ell$, which is absurd. So $I(K_2/K_1) = 1$ also. This simplifies the relations given in [8], theorem 4.4, which correspond to the equations (1.1) and (1.2) :

$$(1.7)\qquad \frac{h_{L_1} h_{\mathbf{Q}}^{\ell-1}}{h_{L_0} h_{K_1}^{\ell-1}} = Q_1 \ell^{-(\ell^2-5)/4} \qquad \textit{for } Q_1 = [U_{L_1} : U_{L_0} \textstyle\prod_{K_1} U_{K_1}].$$

$$(1.8)\qquad \frac{h_{L_2} h_{K_1}^{\ell-1}}{h_{L_1} h_{K_2}^{\ell-1}} = Q_2 \ell^{-(\ell-1)^3/4 - (\ell-3)/2} \qquad \textit{for } Q_2 = [U_{L_2} : U_{L_1} \textstyle\prod_{K_2} U_{K_2}].$$

where the products extend over the conjugates of K_1 and K_2 over $\mathbf{Q}$ and K_1 respectively.

Bounds are given in [8] theorem 3.6 for the indices Q_1 and Q_2. In the two cases the given indices I divide $I(L_1/L_0)$ and $I(L_2/L_1)$ respectively. If $L_1 = L_0(\sqrt[\ell]{e})$ for $e \in U_{L_0}$ then $n = e^i\alpha^\ell$ for some $\alpha \in L_0$ and i prime to ℓ. Hence $n^{\ell-1} = (\pm N_{L_0/\mathbf{Q}}\alpha)^\ell$ which is not possible. Thus $I(L_1/L_0) = 1$. Also, if $L_2 = L_1(\sqrt[\ell]{e})$ for $e \in U_{L_1}$ then $\sqrt[\ell]{n} = e^i\alpha^\ell$ for some $\alpha \in L_1$ and i prime to ℓ. Hence $n^{\ell-1} = (\pm N_{L_1/\mathbf{Q}}\alpha)^\ell$ which again is not possible. Therefore $I(L_2/L_1) = 1$. These remarks and [8] yield that :

$$(1.9)\qquad Q_1 \textit{ divides } \ell^{(\ell-1)(\ell-2)/2}$$

$$(1.10)\qquad Q_2 \textit{ divides } \ell^{\ell(\ell-1)(\ell-2)/2}.$$

The first of these bounds has already been obtained by Parry for $\ell = 5$ in [7]. The second sharpens and generalises that given by Endô in [3] Lemma 3. Formula (1.8) for $\ell = 3$ is due to Endô (*op. cit.* Lemma 2).

2. Prime ideals.

Take $\ell = 3$ in Section 1 .The aim is to establish which n give rise to a field $K_2 = \mathbf{Q}(\sqrt[9]{n})$ whose class number is prime to 3. Every subextension of $M_2/\mathbf{Q}$ is composed of extensions containing a totally ramified prime: either a divisor of (3) or a divisor of (n). Hence the class number of any field divides that of its extensions in M_2 (see [6]). In particular, h_{K_1} divides h_{K_2} and so it is necessary that $3\nmid h_{K_1}$. For the rest of this article the assumption is therefore made that n *is such that* 3 *does not divide the class number of* $\mathbf{Q}(\sqrt[3]{n})$. If $n = n_0 n_1^3$ where n_0 and n_1 are cube free then $K_1 = \mathbf{Q}(\sqrt[3]{n_0})$ and Honda [5] has described precisely the allowable integers n_0. Without loss of generality, it is assumed that n_0 is one of the following :

(2.1i) $n_0 = 3$

(2.1ii) $n_0 = p$ *where* $p \equiv -1 \bmod 9$.

(2.2i) $n_0 = 3^i p$ *where* $p \equiv 2$ *or* $5 \bmod 9$ *and* $i = 0, 1$ *or* 2.

(2.2ii) $n_0 = p^i q$ *where* $i = 1$ *or* 2 *and*
$p, q \equiv 2$ *or* $5 \bmod 9$ *satisfy* $n_0 \equiv \pm 1 \bmod 9$.

Here p and q denote distinct rational primes.

In (2.1) there is just one prime ramified in $K_1/\mathbf{Q}$ and $\zeta = \sqrt[3]{1}$ is a norm in L_1/L_0. However, in (2.2) there are two primes ramified in $K_1/\mathbf{Q}$ but ζ is no longer a norm in L_1/L_0. It will be convenient to assume that K_2 is contained in $\mathbf{R}$ under an embedding of M_2 into $\mathbf{C}$ which is fixed from now on; and K_1 will be the conjugate contained in K_2. With this convention τ^3 represents complex conjugacy on M_2 and τ induces complex conjugacy on L_2.

Because $h_{\mathbf{Q}}$, h_{L_0} and h_{K_1} are all prime to 3 the class number relation (1.7) and the bound (1.9) show that h_{L_1} is prime to 3 and that $Q_1 = 3$. From (1.8) the 3-components h'_Ω of h_Ω satisfy

$$(2.3) \qquad h'_{L_2} h'^{-2}_{K_2} = Q_2 3^{-2}$$

with Q_2 dividing 3^3 by (1.10). Thus :

(2.4) LEMMA. – *If* $3^2 \mid h_{L_2}$ *then* $3 \mid h_{K_2}$.

The main technique used to discard unsuitable n is the calculation of the ambiguous class number $\mathscr{A}$ of L_2/L_1. From (2.4) and [6] one has :

(2.5) LEMMA. – i) *If* $3^2 \mid \mathscr{A}$ *then* $3 \mid h_{K_2}$.

ii) *If* $3 \mid \mathscr{A}$ *and* L_2/K_2 *contains just one ramified prime then* $3 \mid h_{K_2}$.

iii) *If* $3 \nmid \mathscr{A}$ *then* $3 \nmid h_{L_2}$ *and* $3 \nmid h_{K_2}$.

The 3-component of the ambiguous class number will be denoted by $\mathscr{A}'$ and its value is well-known to be

$$(2.6) \qquad \mathscr{A}' = 3^{d-t-1}$$

because h_{L_1} is prime to 3. Here d is the number of prime ideals of L_1 which are ramified in L_2 and

(2.7) $$3^t = [U_{L_1} : U_{L_1} \cap N_{L_2/L_1} L_2] .$$

So the bound $t \le 3$ immediately places a restriction on d for which $3 \nmid h_{K_2}$, *viz.*

(2.8) $$d \le t + 2 \le 5.$$

The factorization of prime ideals in L_1 and L_2 is as follows :

If $p \mid n_0$ with $p \ne 3$ then $(p) = \mathfrak{p}^3$ in L_1 since $p \equiv -1 \bmod 3$. Let r be the number of such primes. Then $r \le 2$ by (2.1) and (2.2) and r is the number of their divisors ramified in L_2/L_1.

If $p \nmid n_0$ with $p \equiv 1 \bmod 3$ and $\left(\frac{n_0}{p}\right)_3 = 1$ then (p) has six prime divisors in L_1. These are all ramified in L_2 if $p|n$ and this would contradict (2.8). So no such primes divide n.

If $p \nmid n_0$ with $p \equiv 1 \bmod 3$ and $\left(\frac{n_0}{p}\right)_3 \ne 1$ then $(p) = \mathfrak{p}\mathfrak{p}^\tau$ in L_1. Let a be the number of such primes dividing n so that $2a$ is the number of their prime divisors ramified in L_2/L_1.

If $p \nmid n_0$ with $p \equiv -1 \bmod 3$ then $(p) = \mathfrak{p}\mathfrak{p}^\sigma\mathfrak{p}^{\sigma^2}$ in L_1. Let b be the number of such primes dividing n so that $3b$ is the number of their prime divisors ramified in L_2/L_1 .

Finally $(3) = (\mathfrak{l}\mathfrak{l}^\sigma\mathfrak{l}^{\sigma^2})^2$ or $\mathfrak{l}^6$ in L_1 according as $n_0 \equiv \pm 1 \bmod 9$ or not. If $n_0 \not\equiv \pm 1 \bmod 9$ then (3) has one ramified prime divisor in L_2/L_1. If $n \equiv \pm 1 \bmod 27$ then $n_0 \equiv \pm 1 \bmod 9$ and (3) has two ramified prime divisors in L_2/L_1, *viz.* $\mathfrak{l}^\sigma$ and $\mathfrak{l}^{\sigma^2}$ if $\mathfrak{l}$ is the divisor satisfying $\mathfrak{l}^\tau = \mathfrak{l}$. If $n \not\equiv \pm 1 \bmod 27$ but $n_0 \equiv \pm 1 \bmod 9$ then (3) has three ramified prime divisors in L_2/L_1. Let c be the number of divisors of (3) ramified in L_2/L_1.

Then (2.8) becomes

(2.9) $$d = r + 2a + 3b + c \le t + 2 \le 5.$$

3. The units of L_1.

Let e_1 be a fundamental unit of K_1 so chosen that $e_1 > 0$. Then $-\zeta$, e_1, and $e_1{}^\sigma$ generate $U_{L_0} \prod U_{K_1}$. Since $Q_1 = 3$ there is a unit $e_2 \in U_{L_1}$ such that $U_{L_1} = \langle -\zeta, e_1, e_2 \rangle$ and

$$(3.1) \qquad e_2^3 = \zeta^a e_1^{\sigma+2}$$

for some integer a mod 3. It is easy to deduce that

$$(3.2) \qquad e_2^{1+\sigma+\sigma^2} = \zeta^a$$

and further manipulation (see [1] corollary 15.4.1) shows that

$$(3.3) \qquad e_1 = e_2^{1-\sigma} = e_2^{1+\tau}.$$

(3.4) LEMMA. – *The number* a *in* (3.1) *satisfies* $a \equiv 0 \bmod 3$ *if, and only if,* ζ *is not a norm in* L_1/L_0, i.e. n_0 *is of type* (2.2).

Proof. – *From* (3.2) ζ is a norm in L_1/L_0 if $a \not\equiv 0 \bmod 3$. However, if $a \equiv 0 \bmod 3$, then ζ is not the norm of a unit because $\alpha^{1+\sigma+\sigma^2} = 1$ for $\alpha = \zeta$, e_1, and e_2. If ζ is not the norm of a unit but is yet a norm from L_1 then K_1 has a weakly ambiguous ideal class of order 3 by [10] lemma 1.11. This contradicts the class number of K_1 being prime to 3. Thus if ζ is a norm in L_1/L_0 then it is the norm of a unit.

(3.5) LEMMA. – *Let* m *be a cube-free product of rational primes which are totally ramified in* K_1 *and suppose* m *is not the product of a power of* n_0 *and the cube of a rational number. Then there is an integer* $\alpha \in K_1$ *satisfying*

$$(3.6) \qquad m e_1^{\pm 1} = \alpha^3 \qquad \textit{and} \qquad m = \alpha^{1+\sigma+\sigma^2}$$

and such that $e'_2 = \alpha^{1-\sigma}$ *is a unit for which* $U_{L_1} = \langle -\zeta, e_1, e'_2 \rangle$.

Proof. – Suppose $m = \prod p_i^{a_i}$ is the prime decomposition of m. Then $(p_i) = \mathfrak{p}_i^3$ for a prime divisor $\mathfrak{p}_i$ of (p_i) in K_1. Since K_1 has class number prime to 3 the ideal $\mathfrak{p}_i$ is principal, say $\mathfrak{p}_i = (\alpha_i)$. Put $\alpha = \prod \alpha_i^{a_i}$. Then $\alpha^3 m^{-1} = \prod(\alpha_i^3 p_i^{-1})^{a_i}$ which is a unit of K_1. So $\alpha^3 m^{-1} = \pm e_1^b$ for some integer b. Without loss of generality the sign is positive and $b = \pm 1$ because $\sqrt[3]{m} \notin K_1$. Clearly $(p_i) = \mathfrak{p}_i^{1+\sigma+\sigma^2} = (\alpha_i^{1+\sigma+\sigma^2})$ so that $m = \alpha^{1+\sigma+\sigma^2}$ by the earlier choice of sign. Now

$$(e_2^{b\sigma}\alpha^{1-\sigma})^{1-\sigma} = e_1^{b\sigma}\alpha^{1+\sigma+\sigma^2}\alpha^{-3\sigma} = 1$$

shows that $e_2^{b\sigma}\alpha^{1-\sigma} \in L_0$. Thus $\alpha^{1-\sigma} = e'_2 = \pm e_2^{-b\sigma}\zeta^c = \pm e_2^{-b} e_1^{b} \zeta^c$ for some integer c, so that $\langle -\zeta, e_1, e'_2\rangle = \langle -\zeta, e_1, e_2\rangle = U_{L_1}$.

Notice that such integers m exist if and only if n_0 is of type (2.2). The lemma itself generalises to pure cubic fields with class number divisible by 3 under the extra hypothesis that (m) must be the cube of a principal ideal of K_1.

4. Norm residue symbols.

In most cases the value of t in (2.7) can be found exactly using the norm residue symbols which Endô has calculated for a basis of U_{L_1}. The symbols are powers of ζ, which satisfies $\zeta^{-\tau} = \zeta$ and $\zeta^{\sigma} = \zeta$. Hence

$$(4.1) \qquad \left(\frac{\zeta,\sqrt[3]{n}}{\mathfrak{p}}\right) = \left(\frac{\zeta,\sqrt[3]{n}}{\mathfrak{p}^{\sigma}}\right) = \left(\frac{\zeta,\sqrt[3]{n}}{\mathfrak{p}^{\tau}}\right)$$

and

$$\left(\frac{e_1,\sqrt[3]{n}}{\mathfrak{p}}\right) = \left(\frac{e_1,\sqrt[3]{n}}{\mathfrak{p}^{\tau}}\right)^{-1}.$$

So for primes p which decompose as $(p) = \mathfrak{p}^{1+\sigma+\sigma^2}$ in L_1 the convention is that $\mathfrak{p}$ is the divisor fixed by τ, i.e. $\mathfrak{p}^{\tau} = \mathfrak{p}$, and $\mathfrak{p}^{\sigma\tau} = \mathfrak{p}^{\sigma^2}$. Endô [3] proves the following lemmas using the properties of the norm residue symbol as described by Hasse in [4] and the relations in section 3.

(4.2) LEMMA. – *If* $p \mid n_0$, $p \neq 3$ *and* $(p) = \mathfrak{p}^3$ *in* L_1 *then*

$$\left(\frac{\zeta,\sqrt[3]{n}}{\mathfrak{p}}\right) = 1 \iff p \equiv -1 \bmod 9 .$$

$$\left(\frac{e_1,\sqrt[3]{n}}{\mathfrak{p}}\right) = 1.$$

In case (2.2) $\left(\frac{e_2,\sqrt[3]{n}}{\mathfrak{p}}\right) = 1$ *if* $p \equiv -1 \bmod 9$; *and*

$$\left(\frac{e'_2,\sqrt[3]{n}}{\mathfrak{p}}\right) = 1 \iff p \nmid m \quad \textit{if} \quad p \not\equiv -1 \bmod 9 .$$

(4.3) LEMMA. – *If* $p \nmid n_0, p \mid n$, $p \equiv 1 \bmod 3$, $\left(\frac{n_0}{p}\right)_3 \neq 1$ *and* $(p) = \mathfrak{p}\mathfrak{p}^{\tau}$ *in* L_1 *then*

$$\left(\frac{\zeta,\sqrt[3]{n}}{\mathfrak{p}}\right) = \left(\frac{\zeta,\sqrt[3]{n}}{\mathfrak{p}^{\tau}}\right) = 1.$$

$$\left(\frac{e_1,\sqrt[3]{n}}{\mathfrak{p}}\right) = \left(\frac{e_1,\sqrt[3]{n}}{\mathfrak{p}^{\tau}}\right) = 1.$$

I n case (2.2) $\left(\frac{e_2,\sqrt[3]{n}}{\mathfrak{p}}\right) = \left(\frac{e_2,\sqrt[3]{n}}{\mathfrak{p}^{\tau}}\right) = 1.$

(4.4) LEMMA. – *If* $p \nmid n_0, p \mid n$, $p \equiv -1 \bmod 3$, *and* $(p) = \mathfrak{p}\mathfrak{p}^{\sigma}\mathfrak{p}^{\sigma^2}$ *in* L_1 *then*

$$\left(\frac{\zeta,\sqrt[3]{n}}{\mathfrak{p}}\right) = \left(\frac{\zeta,\sqrt[3]{n}}{\mathfrak{p}^{\sigma}}\right) = \left(\frac{\zeta,\sqrt[3]{n}}{\mathfrak{p}^{\sigma^2}}\right); \textit{ and}$$

$$\left(\frac{\zeta,\sqrt[3]{n}}{\mathfrak{p}}\right) = 1 \Leftrightarrow p \equiv -1 \bmod 9.$$

$$\left(\frac{e_1,\sqrt[3]{n}}{\mathfrak{p}}\right) = 1 \textit{ and } \left(\frac{e_1,\sqrt[3]{n}}{\mathfrak{p}^{\sigma}}\right) = \left(\frac{e_1,\sqrt[3]{n}}{\mathfrak{p}^{\sigma^2}}\right)^{-1}; \qquad \textit{and}$$

$$\left(\frac{e_1,\sqrt[3]{n}}{\mathfrak{p}^{\sigma}}\right) = 1$$

if, and only if, n_0 *is of type* (2.2) *or* $p \equiv -1 \bmod 9$.

$$\left(\frac{e_2,\sqrt[3]{n}}{\mathfrak{p}}\right) = \left(\frac{e_2,\sqrt[3]{n}}{\mathfrak{p}^{\sigma}}\right) = \left(\frac{e_2,\sqrt[3]{n}}{\mathfrak{p}^{\sigma^2}}\right)$$

if, and only if, n_0 *is of type* (2.2) *or* $p \equiv -1 \bmod 9$.

(4.5) LEMMA. – *If* $n_0 \equiv \pm 1 \bmod 9$, $n = 3^e n'$ *with* $3 \nmid n'$, *and* $(3) = (\mathfrak{l}\mathfrak{l}^{\sigma}\mathfrak{l}^{\sigma^2})^2$ in L_1 where $\mathfrak{l}$ is fixed by τ *then*

$$\left(\frac{\zeta,\sqrt[3]{n}}{\mathfrak{l}}\right) = \left(\frac{\zeta,\sqrt[3]{n}}{\mathfrak{l}^{\sigma}}\right) = \left(\frac{\zeta,\sqrt[3]{n}}{\mathfrak{l}^{\sigma^2}}\right); \textit{ and}$$

$$\left(\frac{\zeta,\sqrt[3]{n}}{\mathfrak{l}}\right) = 1 \Leftrightarrow n' \equiv \pm 1 \bmod 27.$$

$$\left(\frac{e_1,\sqrt[3]{n}}{\mathfrak{l}}\right) = 1 \qquad \textit{and} \qquad \left(\frac{e_1,\sqrt[3]{n}}{\mathfrak{l}^{\sigma}}\right) = \left(\frac{e_1,\sqrt[3]{n}}{\mathfrak{l}^{\sigma^2}}\right)^{-1}.$$

In case (2.2) $\quad \prod_{i=0}^{2}\left(\dfrac{e_2,\sqrt[3]{n}}{\mathfrak{l}^{\sigma^i}}\right) \;=\; \left(\dfrac{e_1,\sqrt[3]{n}}{\mathfrak{l}^{\sigma}}\right)^{-1} \;\neq\; 1\,.$

Proof. – The result for ζ is as given by Endô, and the first claim about e_1 is immediate from (4.1). For e_2 in case (2.2) Endô has shown that

$$\prod_{i=0}^{2}\left(\frac{e'_2,\sqrt[3]{n}}{\mathfrak{l}^{\sigma^i}}\right) \;=\; \left(\frac{m,\zeta}{\mathfrak{l}}\right).$$

Now $\prod\left(\dfrac{\zeta,\sqrt[3]{n}}{\mathfrak{l}^{\sigma^i}}\right) = \prod\left(\dfrac{e_1,\sqrt[3]{n}}{\mathfrak{l}^{\sigma^i}}\right) = 1$ and so e'_2 can be changed by powers of ζ and e_1 to give

$$\prod_i\left(\frac{e_2,\sqrt[3]{n}}{\mathfrak{l}^{\sigma^i}}\right) \;=\; \left(\frac{m,\zeta}{\mathfrak{l}}\right)^{\mp 1}$$

where, by the proof of (3.5), the sign is minus the undefined sign in (3.6). Also from (3.6) with the same ambiguity of sign,

$$\begin{aligned}
\left(\frac{e_1,\sqrt[3]{n}}{\mathfrak{l}^{\sigma}}\right) &= \left(\frac{e_1,\sqrt[3]{n}}{\mathfrak{l}^{\sigma}}\right)^{2}\left(\frac{e_1,\sqrt[3]{n}}{\mathfrak{l}^{\sigma^2}}\right)^{-2} \\
&= \left(\frac{m,\sqrt[3]{n}}{\mathfrak{l}^{\sigma}}\right)^{\mp 2}\left(\frac{m,\sqrt[3]{n}}{\mathfrak{l}^{\sigma^2}}\right)^{\pm 2} \\
&= \left(\frac{m,\zeta^{-1}\sqrt[3]{n}}{\mathfrak{l}}\right)^{\mp 2}\left(\frac{m,\zeta\sqrt[3]{n}}{\mathfrak{l}}\right)^{\pm 2} \;=\; \left(\frac{m,\zeta}{\mathfrak{l}}\right)^{\pm 1}.
\end{aligned}$$

Finally, (3) is not totally ramified in K_1 as $n_0 \equiv \pm 1 \bmod 9$ and so 3 is not a factor of m. Thus, m is a product of divisors of n_0, and, by (2.2), $m \equiv \pm 1 \bmod 9$ if, and only if, m is a cube times a power of n_0. However, such an m does not satisfy the hypotheses of (3.5), and therefore $m \not\equiv \pm 1$ mod 9. Hence

$$\left(\frac{m,\zeta}{\mathfrak{l}}\right) \;=\; \zeta^{(m^2-1)/3} \;\neq\; 1.$$

(4.6) LEMMA. – *If* $n_0 \not\equiv \pm 1$ mod 9, $n = 3^e n'$ *with* $3 \nmid n'$, *and* $(3) = \mathfrak{l}^6$ in L_1 *then*

$$\left(\frac{\zeta,\sqrt[3]{n}}{\mathfrak{l}}\right) = 1 \;\Leftrightarrow\; n' \equiv \pm 1 \bmod 9.$$

$$\left(\frac{e_1,\sqrt[3]{n}}{\mathfrak{l}}\right) = 1\,.$$

In case (2.2),

$$\left(\frac{e'_2, \sqrt[3]{n}}{\mathfrak{l}}\right) = 1 \Leftrightarrow m' \equiv \pm 1 \bmod 9 \quad \textit{where} \;\; m = 3^f m' \;\; \textit{with} \;\; 3 \nmid m'.$$

(4.7) LEMMA. – *In case* (2.2) *with* $n_0 \equiv \pm 1 \bmod 9$ *the only units of* L_1 *which are norms are the cubes.*

Proof. – Suppose $e = \zeta^i e_1{}^j e_2{}^k$ is a norm. Then

$$1 = \prod_i \left(\frac{e, \sqrt[3]{n}}{\mathfrak{l}^{\sigma^i}}\right) = \left(\frac{e_1, \sqrt[3]{n}}{\mathfrak{l}^{\sigma}}\right)^{-k}$$

by (4.5). Hence $k \equiv 0 \bmod 3$ by (4.5). So

$$1 = \left(\frac{e, \sqrt[3]{n}}{\mathfrak{l}}\right)\left(\frac{e, \sqrt[3]{n}}{\mathfrak{l}^{\sigma}}\right)^{-1} = \left(\frac{e_1, \sqrt[3]{n}}{\mathfrak{l}^{\sigma}}\right)^{-j}$$

by (4.5). Hence $j \equiv 0 \bmod 3$ by (4.5). So

$$1 = \left(\frac{e, \sqrt[3]{n}}{\mathfrak{p}}\right) = \left(\frac{\zeta, \sqrt[3]{n}}{\mathfrak{p}}\right)^i$$

for a prime divisor $\mathfrak{p}$ of $p \mid n_0$. Hence $i \equiv 0 \bmod 3$ by (4.2) as $p \not\equiv \pm 1 \bmod 9$.

(4.8) LEMMA. – *In case* (2.2) *with* $n_0 \not\equiv \pm 1 \bmod 9$ *suppose* n *has no prime factor* $p \equiv 1 \bmod 3$ *with* $\left(\frac{n_0}{p}\right)_3 = 1$. *Let* e'_2 *correspond to* $m = 3$. *If* e'_2 *is a norm then the units of* L_1 *which are norms are cubes times powers of* e_1 *and* e'_2. *If* e'_2 *is not a norm, the units of* L_1 *which are norms are cubes times powers of* e_1. *In particular, the former case holds,* i.e. e'_2 *is a norm, when* n *has no factor* $p \equiv -1 \bmod 3$.

Proof. – It is readily seen that e_1 is a norm and that when n has no factor $p \equiv -1 \bmod 3$ then e'_2 is also a norm. Since $\left(\frac{\zeta, \sqrt[3]{n}}{\mathfrak{l}}\right) \neq 1$ in (4.6) it is clear that no linear combination of e'_2 and ζ can be a norm except possibly cubes times powers of e'_2.

(4.9) LEMMA. – *In case* (2.1) *if* ζ *is not a norm in* $\mathrm{L}_2/\mathrm{L}_1$ *then the only units of* L_1 *which are norms are the cubes.*

Proof. – From (3.1) and (3.4) $e_2^3 = \zeta^{\pm 1} e_1^{\sigma+2}$. Hence ζ not a norm $\Rightarrow$ $e_1^{\sigma+2}$ not a norm $\Rightarrow$ $(\zeta^i e_1)^{\sigma+2}$ not a norm $\Rightarrow$ $\zeta^i e_1$ not a norm, for any integer i.

Choose a prime $\mathfrak{p}$ in L_1 for which $\left(\frac{e_1, \sqrt[3]{n}}{\mathfrak{p}}\right) \neq 1$. By (4.1) certainly $\mathfrak{p}^\tau \neq \mathfrak{p}$. Let $e = \zeta^i e_1^j e_2^k$ be a general unit of L_1. Then

$$\left(\frac{e^{1-\sigma}, \sqrt[3]{n}}{\mathfrak{p}}\right) = \left(\frac{e_1^{1-\sigma}, \sqrt[3]{n}}{\mathfrak{p}}\right)^j \left(\frac{e_2^{1-\sigma}, \sqrt[3]{n}}{\mathfrak{p}}\right)^k = \left(\frac{\zeta, \sqrt[3]{n}}{\mathfrak{p}}\right)^{aj} \left(\frac{e_1, \sqrt[3]{n}}{\mathfrak{p}}\right)^k$$

by (3.1) and (3.3), and

$$\left(\frac{e^{1-\sigma}, \sqrt[3]{n}}{\mathfrak{p}^\tau}\right) = \left(\frac{\zeta, \sqrt[3]{n}}{\mathfrak{p}^\tau}\right)^{aj} \left(\frac{e_1, \sqrt[3]{n}}{\mathfrak{p}^\tau}\right)^k = \left(\frac{\zeta, \sqrt[3]{n}}{\mathfrak{p}}\right)^{aj} \left(\frac{e_1, \sqrt[3]{n}}{\mathfrak{p}}\right)^{-k}$$

by (4.1). These expressions are distinct and so they cannot both be equal to 1 if $k \not\equiv 0 \bmod 3$. Thus e a norm $\Rightarrow$ $e^{1-\sigma}$ a norm $\Rightarrow$ $k \equiv 0 \bmod 3$ $\Rightarrow$ $\zeta^i e_1^j$ a norm $\Rightarrow$ $i \equiv j \equiv 0 \bmod 3$ by the initial remarks. Therefore e is a cube if it is a norm.

(4.10) LEMMA. – *In case* (2.1) *if* ζ *is a norm in* L_2/L_1 *but* e_1 *is not a norm, then the only units of* L_1 *which are norms are cubes times a power of* ζ.

Proof. – Choose a prime $\mathfrak{p}$ in L_1 for which $\left(\frac{e_1, \sqrt[3]{n}}{\mathfrak{p}}\right) \neq 1$. Then for $e = \zeta^i e_1^j e_2^k$ the proof of (4.9) yields $k \equiv 0 \bmod 3$ if e is a norm. So $\zeta^i e_1^j$ is a norm in that case and consequently e_1^j is a norm because ζ is. Thus $j \equiv 0 \bmod 3$ also, which proves the statement.

5. The class number of K_2.

Recall from §2 the definitions of r, a, b, and c as the numbers of certain primes which ramify in L_2/L_1. The value of c (= 1, 2 or 3) places certain congruence conditions on n and n_0 which restrict the values of r. In particular,

(5.1) *If* $c = 1$ *then* $r \neq 2$;

(5.2) *If* $c \neq 1$ *then* $r \neq 0$;

because n_0 has to be of type (2.1) or (2.2).

(5.3) THEOREM. – *If* K_2 *has class number prime to* 3 *then* n *has no prime factor* $p \equiv 1 \bmod 3$.

Proof. – The case of n divisible by $p \equiv 1 \bmod 3$ with $\left(\frac{n_0}{p}\right)_3 = 1$ has already been excluded in §2 *by* (2.8) *since such a prime has six ramified divisors in* L_1. Otherwise suppose $a > 0$. The possible values of r, a, b, and c satisfying $r \leq 2$ and (2.9) are listed below with the reason why $3 \mid h_{K_2}$. In each case $b = 0$ for otherwise $2a + 3b + c \geq 2.1 + 3.1 + 1$ would contradict (2.9). When $c = 1$ the extension L_2/K_2 has a unique ramified prime and so (2.5ii) can be applied.

a	c	r	Type of n_0	d	t	$d–t–1$	Reason
1	1	0	(2.1i)	3	≤ 1	≥ 1	ζ, e_1 norms by (4.3) and (4.6); (2.5ii)
1	2	0	none				(5.2)
1	3	0	none				(5.2)
1	1	1	(2.2i)	4	≤ 2	≥ 1	e_1 norm by (4.8); (2.5ii)
1	2	1	(2.1ii)	5	≤ 2	≥ 2	ζ norm by (4.2), (4.3), and (4.5); (2.5i)
1	1	2	none				(5.1)
2	1	0	(2.1i)	5	≤ 3	≥ 1	(2.5ii)

(5.4) THEOREM. – *If* K_2 *has class number prime to* 3 *and* n *has a prime factor* $p \equiv -1 \bmod 3$ *which does not divide* n_0 *then, without loss of generality,* $n = 3p^3$ *or* $9p^3$ *where* $p \equiv 2$ *or* $5 \bmod 9$. *For such* n *the class number* h_{K_2} *is prime to* 3.

Proof. – As observed in the previous proof, $a = 0$ if $b \neq 0$. So the possible values of r, b, and c satisfying $r \leq 2$ and (2.9) are the following:

b	c	r	Type of n_0	d	t	$d–t–1$	Reason
1	1	0	(2.1i)	4	*	*	see below
1	2	0	none				(5.2)
1	1	1	(2.2i)	5	≤ 3	≥ 1	(2.5ii)

The outstanding case of $b = 1$, $c = 1$, $r = 0$ corresponds to n of the form $3p^3$ or $9p^3$ with $p \equiv -1 \bmod 3$. If $p \not\equiv -1 \bmod 9$ then ζ is not a norm by (4.4) or (4.6). Hence $t = 3$ by (4.9) and $d–t–1 = 0$. Thus $3 \nmid h_{K_2}$ by (2.5iii). On the other hand, if $p \equiv -1 \bmod 9$ then ζ is a norm by (4.4) and (4.6).

Hence $t \leq 2$ and $d{-}t{-}1 \geq 1$. Thus $3 \mid h_{K_2}$ by (2.5ii).

From (5.3) and (5.4) the only n containing prime divisors other than those of $3n_0$ and for which h_{K_2} is prime to 3 are those described in (5.4). Otherwise $a = b = 0$ and there are the following possibilities :

c	r	Type of n_0	d	t	$d{-}t{-}1$	Reason
1	0	(2.1i)	1	0	0	Only one prime is ramified. So every unit is a norm by the product formula.
1	1	(2.2i)	2	1	0	e'_2 is a norm by (4.2) and (4.6) for m = 3; (4.8)
1	2	none				(5.1)
2	0	none				(5.2)
2	1	(2.1ii)	3	≤ 2	?	ζ is a norm by (4.5)
2	2	(2.2ii)	4	3	0	(4.7)
3	0	none				(5.2)
3	1	(2.1ii)	4		?	
3	2	(2.2ii)	5	3	1	(4.7)

This table gives three cases for which $3 \nmid h_{K_2}$, three cases which are impossible, and three cases which are undecided. When $c = 3$ and $r = 1$, then $n = 3^{3i}p$ where $p \equiv -1 \bmod 9$ and either $i \not\equiv 0 \bmod 3$ or $p \not\equiv -1 \bmod 27$. If $p \not\equiv -1 \bmod 27$ then ζ is not a norm by (4.5) and so $t = 3$ by (4.9). So $d{-}t{-}1 = 0$ and $3 \nmid h_{K_2}$ by (2.5iii). The following theorem has now been proved :

(5.5) MAIN THEOREM. – i) *The class number of* $\mathbf{Q}(\sqrt[9]{n})$ *is prime to* 3 *when* n *is one of the following* :

$n = 3$,

$n = 3^i p$ *where* $p \equiv 2$ *or* $5 \bmod 9$ *and* i *is any integer,*

$n = 3^i p3$ *where* $p \equiv 2$ *or* $5 \bmod 9$ *and* $i = 1$ *or* 2,

$n = 3^{3i} p$ *where* $p \equiv 8$ *or* $17 \bmod 27$ *and* i *is any integer,*

$n = p^j q$ *where* $p, q \equiv 2$ *or* $5 \bmod 9$ *and* j *satisfies* $n \equiv \pm 1 \bmod 27$.

In each case p *and* q *denote distinct primes.*

ii) *It may be possible that the class number of* $\mathbf{Q}(\sqrt[9]{n})$ *is prime to* 3 *when* n *is one of the following* :

$n = 3^{3i}p$ *where* $p \equiv -1 \bmod 27$ *and* i *is any integer* ,

$n = 3^{3i}p^j q$ *where* $p, q \equiv 2$ *or* $5 \bmod 9$, j *satisfies* $p^j q \equiv \pm 1 \bmod 9$
and i *satisfies* $n \not\equiv \pm 1 \bmod 27$.

Here p *and* q *denote distinct primes again*.

iii) *If* $\mathbf{Q}(\sqrt[9]{n})$ *is not given by taking one of the above values of* n *then the class number of* $\mathbf{Q}(\sqrt[9]{n})$ *is divisible by* 3.

Remark. – The case of $n = 3$ is well-known and Endô proves the result for $n = 3p^3$ or $9p^3$ where $p \equiv 2$ or $5 \bmod 9$.

BIBLIOGRAPHY

[1] P. BARRUCAND and H. COHN, Remarks on principal factors in a relative cubic field, *J. Number Theory,* 3 (1971), 226-239.

[2] R. BRAUER, Beziehungen zwischen Klassenzahlen von Teilkörpern eines galoisschen Körpers, *Math. Nachr*., 4 (1951), 158-174.

[3] A. ENDÔ, On the divisibility of the class number of $\mathbf{Q}(\sqrt[9]{n})$ by 3, *Mem. Fac. Sci., Kyushu Univ.*, A, 30 (1976), 299-311.

[4] H. HASSE, Bericht über neuere Untersuchungen und Probleme aus der Theorie der algebraischen Zahlkörper, II, Physica Verlag, Würzburg/Wien, 1970.

[5] T. HONDA, Pure cubic fields whose class numbers are multiples of three, *J. Number Theory,* 3 (1971), 7-12.

[6] K. IWASAWA, A note on class numbers of algebraic number fields, *Abh. Math. Sem. Univ. Hamburg,* 20 (1956), 257-258.

[7] C. J. PARRY, Class number relations in pure quintic fields, *Symposia Mathematica*, 15 (1975), 475-485.

[8] C. D. WALTER, A class number relation in Frobenius extensions of number fields, *Mathematika,* 24 (1977), 216-225.

[9] C. D. WALTER, Kuroda's class number relation, *Acta Arithmetica*, 35 (1979), 41-51.

[10] C. D. WALTER, The ambiguous class group and the genus group of certain non-normal extensions, *Mathematika*, 26 (1979), 113-124.

Manuscrit reçu le 1er octobre 1979.

Colin D. WALTER,

Department of Mathematics
University College
Belfield
Dublin 4 (Ireland).