Can. J. Math., Vol. XXVIII, No. 2, 1976, pp. 429–439

DIHEDRAL FIELD EXTENSIONS OF ORDER $2p$ WHOSE CLASS NUMBERS ARE MULTIPLES OF p

T. CALLAHAN

1. Introduction. If L is a cyclic extension of $\mathbf{Q}$ of prime degree p, then the class number of L is divisible by p if and only if more than one prime divides the discriminant D, of L. If $p \neq 2$, then this condition is equivalent to the existence of more than one cyclic extension of $\mathbf{Q}$ of degree p with discriminant equal to D. In this paper we generalize these results to non-galois extensions of $\mathbf{Q}$ of degree p whose normal closures have degree $2p$ over $\mathbf{Q}$. We show that the same sort of theorems are true in this more general situation, but that there are a few distinctive differences.

In 1971, T. Honda [**9**] completely determined when a field of the form $\mathbf{Q}(n^{1/3})$ has class number divisible by 3. Our paper generalizes Honda's work to any cubic field of negative discriminant and extends it to all other odd primes. However, the pure cubic fields considered by Honda have unique properties which do not carry over to the general case.

Some of the techniques of Section 3 are contained in [**3**] and [**4**], which deal with a more complete analysis of the situation when $p = 3$.

2. Suppose that p is an odd prime and d is a negative quadratic discriminant. Let M be a number field satisfying the following criteria:

(1) $[M, \mathbf{Q}] = p$;

(2) If N is the normal closure of M, then $[N : \mathbf{Q}] = 2p$;

(3) $N = M \cdot \mathbf{Q}(\sqrt{d})$;

(4) disc $(N/M) = f$.

Conditions (1) and (2) imply that the galois group of N over Q is isomorphic to D_{2p}, the dihedral group of order $2p$. Therefore there are p distinct fields conjugate to M (we count M as a conjugate to itself). Let $F(p, d, f)$ denote a set of fields satisfying (1) – (4) such that each set of p conjugate fields has a single representative in $F(p, d, f)$.

If $M \in F(p, d, f)$, then f is a rational integer. In fact,

$$\text{disc } (N/M) = p^{v+w} \prod_{i=1}^{t} k_i \prod_{i=1}^{s} q_i,$$

where

(i) k_i is a rational prime such that

$$k_i \equiv (d/k_i) = 1 \pmod{p}$$

for $i = 1, 2, \ldots, t$,

Received May 21, 1975.

https://doi.org/10.4153/CJM-1976-043-x Published online by Cambridge University Press

(ii) q_i is a rational prime such that $q_i \equiv (d/q_i) = -1 \pmod{p}$ for $i = 1, 2, \ldots s$,

(iii) $w = 1$ if $p|f$ and $p \nmid d$, $w = 0$ otherwise,

(iv) $v = 0$ or 1 if $p \geqq 5$ or $p = 3$ and $d \not\equiv -3 \pmod{9}$,

(v) $v = 0, 1$, or 2 if $p = 3$ and $d \equiv -3 \pmod{9}$. Further, if $M \in F(p, d, f)$, then

$$\text{disc}\ (M/\mathbf{Q}) = df^{p-1}.$$

Notice that p is the only prime which can ramify fully in $N/\mathbf{Q}$. The above facts were proved for $p = 3$ by H. Hasse [**7**], and in general by J. Martinet [**10**].

For the rest of the paper we let $M \in F(p, d, f)$, $K = \mathbf{Q}(\sqrt{d})$ and N be the normal closure of M. We also let σ denote a generator of Gal (N/M) and τ denote a generator of Gal (N/K). Thus

$$\text{Gal}\ (N/\mathbf{Q}) = \langle \sigma, \tau | \sigma^2 = (\sigma\tau)^2 = \tau^P = 1 \rangle.$$

Class Field Theory says that each field $M \in F(p, d, f)$ corresponds to a character χ defined on J_K of order p and conductor f which is identically 1 on K^*. Two such characters correspond to the same field if and only if one is a power of the other. Further in order that Gal $(N/\mathbf{Q}) \simeq D_{2p}$ it is necessary and sufficient that

$$\chi^\sigma = \chi^{-1}$$

where

$$\chi^\sigma(x) = \chi(\sigma(x)).$$

This last condition is equivalent to

$$\chi(x) = 1 \text{ for all } x \in J_{\mathbf{Q}}.$$

We let $C(p, d, f)$ denote the set of characters on J_K which satisfy the above condition. Thus $\chi \in C(p, d, f)$ if and only if the following conditions are satisfied:

(1) χ is defined on J_K;

(2) χ has order p;

(3) χ has conductor f;

(4) $\chi(x) = 1$ for all $x \in J_{\mathbf{Q}}$.

LEMMA 2.1. *The number of independent characters contained in $C(p, d, f)$ is equal to the number of fields in $F(p, d, f)$.*

Readers not familiar with characters on idele groups may find H. Heilbronn [**8**] to be helpful.

We let Cl_K denote the p-class group of K, i.e. the p-Sylow subgroup of the ideal class group of K, and we let r_K denote the rank of Cl_K, i.e. the minimal number of generators of Cl_K.

https://doi.org/10.4153/CJM-1976-043-x Published online by Cambridge University Press

We need to determine the characters contained in $C(p, d, f)$ when $r_K = 0$ and f is equal to a prime. Suppose that k is the unique prime dividing $f (k = p$ is permitted). Let $K_\mathfrak{l}$ be the localization of K at a prime $\mathfrak{l}$ lying over k, and let $B_\mathfrak{l}$ be the ring of integers of $K_\mathfrak{l}$. Then a character in $C(p, d, f)$ is completely determined by its local component on $K_\mathfrak{l}$.

If we choose d so that $r_K \neq 0$, then it is not true that a character on $K_\mathfrak{l}$ completely determines a character in $C(p, d, f)$. However, if $r_K = 0$ and $\chi_\mathfrak{l}$ is a character of order p on $K_\mathfrak{l}$ which is non-trivial on the unit group of $K_\mathfrak{l}$, then there is a unique character whose conductor is equal to the conductor of $\chi_\mathfrak{l}$ and whose local component at $K_\mathfrak{l}$ is equal to $\chi_\mathfrak{l}$ if and only if $\chi_\mathfrak{l}$ is trivial on all units of K. This last condition is automatically met for $d < -3$ and may not be satisfied if $d = -3$ and $p = 3$. Therefore we shall restrict ourselves to $d < 0$ and to $d < -3$ if $p = 3$. The results for $d > 0$ are essentially the same as those for $d < 0$. For $p = 3$ and $d = -3$ the reader is referred to [**9**] and [**11**]. Thus we need only determine characters of order p defined on $(B_\mathfrak{l}/k^n B_\mathfrak{l})^*$ which are trivial on the canonical image of $\mathbf{Z}_\mathfrak{p}$. In order to do this we need to know something about the structure of $(B_\mathfrak{l}/k^n B_\mathfrak{l})^*$. The next few lemmas provide this information; the proofs are straightforward but tedious, and so we leave them out.

For any positive rational integer n we let $C(n)$ denote the cyclic group of order n.

LEMMA 2.2. *If $p \geqq 5$ (or $p = 3$ and $d \equiv -3 \pmod 9$), $p|d$, and $\mathfrak{p}$ is the prime in K lying ove p, then*
(i) $(B_\mathfrak{p}/pB_\mathfrak{p})^* \simeq C(p(p-1))$
(ii) $(B_\mathfrak{p}/p^n B_\mathfrak{p})^* \simeq C(p^{n-1}(p-1) \times C(p^n)$ *for* $n \geqq 2$.

LEMMA 2.3. *If $d \equiv -3 \pmod 9$, $p = 3$, and $\mathfrak{l}$ is the prime in K which lies over 3, then*
(i) $(B_\mathfrak{p}/3B_\mathfrak{p})^* \simeq C(6)$
(ii) $(B_\mathfrak{p}/3^n B_\mathfrak{p})^* \simeq C(2 \cdot 3^{n-1}) \times C(3^{n-1}) \times C(3)$ *for* $n \geqq 2$.

The anomalous behaviour of the prime 3 in $K = \mathbf{Q}(\sqrt{d})$ when $d \equiv -3 \pmod 9$ is not unexpected since $K_\mathfrak{l}$, the localization of K at the prime in K which lies over 3, is equal to $\mathbf{Q}_3(\xi_3)$, where ξ_3 is a primitive third root of unity, if and only if $d \equiv -3 \pmod 9$.

LEMMA 2.4. *If q is an odd prime, $(d/q) = 1$, and $\mathfrak{q}$ is either of the primes of K lying over q, then*

$$(B_\mathfrak{q}/q^n B_\mathfrak{q})^* \simeq C((q-1)q^{n-1}) \times C((q-1)q^{n-1}).$$

Therefore $q \equiv 1 \pmod p$ implies $p\,|\,|(B_\mathfrak{q}/qB_\mathfrak{q})^*|$.

LEMMA 2.5. *If q is an odd prime and $(d/q) = -1$, then*
(i) $(Bq/qBq)^* \simeq C(q^2 - 1)$
(ii) $(Bq/q^n Bq)^* \simeq C((q^2 - 1)p^{n-1}) \times C(q^{n-1})$ *for* $n \geqq 2$.
Therefore $q \equiv -1 \pmod p$ implies $p\,|\,|(Bq/qBq)^*|$.

LEMMA 2.6. *If $r_K = 0$, $F(p, d, f)$ is not empty, and $t + s + v = 1$, then* $|F(p, d, f)| = 1$.

Proof. Since $r_K + s + v = 1$, it follows that $f = q$, where q is a prime possibly equal to p. Therefore we need only determine the characters of $C(p, d, q)$. However, this is equivalent to determining characters of $B_\mathfrak{q}/qB_\mathfrak{q}$ which are trivial on the canonical image of $\mathbf{Z}q$. The canonical image of $\mathbf{Z}q$ generates a subgroup of $B_\mathfrak{q}/qB_\mathfrak{q}$ of order $q - 1$. Therefore Lemmas 2.2–2.5 show that there is only one independent character in $C(p, d, q)$. Lemma 2.1 completes the proof.

LEMMA 2.7. *If $r_K \geqq 1$, $s + t + v \geqq 1$, and $F(p, d, f)$ is non-empty, then* $|F(p, d, f)| > 1$.

Proof. Since $r_K \geqq 1$, we know that there is an unramified character χ of order p defined on J_K, i.e. there is a character $\chi \in C(p, d, l)$. Since $F(p, d, f)$ is non-empty, there is a character $\psi \in C(p, d, f)$. The characters $\chi\psi, \chi\psi^2, \ldots, \chi\psi^{p-1}$ all belong to $C(p, d, f)$ and are independent.

LEMMA 2.8. *If $r_K = 0$, $s + t + v \geqq 2$, and $F(p, d, f)$ is not empty, then* $|F(p, d, f)| \geqq 1$.

Proof. Suppose that $v \neq 2$ ($v = 2$ is possible only if $p = 3$ and $d \equiv -3 \pmod 9$). Then $s + t + v \geqq 2$ implies that there are at least 2 distinct primes q_1 and q_2 which divide f. Let $q_1, q_2, \ldots, q_{s+t+v}$ be a complete list of primes dividing f. Lemma 2.6 says that for each $i = 1, \ldots, s + t + v$, there is a character $\chi_i \in C(p, d, q_i)$. Each character

$$\psi = \chi_1^{a_1} \cdot \chi_2^{a_2} \cdot \ldots \cdot \chi_n^{a_n},$$

where $1 \leqq a_i \leqq p - 1$ and $a_i \in \mathbf{Z}$, belongs to $C(p, d, f)$. This is in fact a complete list of characters in $C(p, d, f)$ and includes exactly

$$\frac{(p-1)^{s+t+v}}{p-1} = (p-1)^{s+t+v-1}$$

independent characters, which is greater than 1 if $s + t + v \geqq 2$. This completes the proof when $v \neq 2$.

Suppose that χ (respectively ψ) is a character on J_K with conductor f_χ (resp. f_ψ). If $p^n \| f_\chi$ and $p^m \| f_\psi$, with $m < n$, then $p^n \| f_{\psi\cdot\chi}$ where $f_{\chi\psi}$ is the conductor of $\chi\psi$. It follows that, if $v = 2$ and $s + t = 0$ then $f = 9$, $F(3, d, 9) = 3$, and $F(3, d, 3) = 1$. If $v = 2$ and $t + s \geqq 1$, then there is a character $\chi \in C(3, d, f/9)$ (this was proved above) and there is a character $\psi \in C(3, d, 9)$. It follows that $\chi\psi$ and $\chi\psi^{-1}$ both belong to $C(3, d, f)$. These characters are independent which shows that $|F(p, d, f)| \geqq 2$.

THEOREM 1.9. *Suppose that $F(p, d, f)$ is non-empty. Then*

$|F(p, d, f)| > 1$ if and only if $r_K + s + t + v \geqq 2$.

https://doi.org/10.4153/CJM-1976-043-x Published online by Cambridge University Press

Proof. This theorem is just a statement of the last three lemmas.

If we choose d so that $r_K = 0$, then $s + t + v \geqq 2$ is a necessary and sufficient condition for $F(p, d, f)$ to contain more than one field. However, if $r_K \geqq 1$ then $F(p, d, q)$ may be empty even if $r_K + s + t + v \geqq 2$; for example, $F(3, -23, 5)$ is empty even though $r_K = 1$, $s = 1$ and $(-23/5) = -1 \equiv 5 \pmod 3$. This situation was examined for $p = 3$ by H. Hasse [**7**] and H. Reichardt [**11**].

3. Throughout this section we let $M \in F(p, d, f)$, N be the normal closure of M, and $K = \mathbf{Q}(\sqrt{d})$. We shall use the notation introduced in Section 2 and we shall continue to assume that $d < 0$ and that $d \neq -3$ when $p = 3$. If L is any algebraic number field then we shall use the following notation:

R_L = ring of integers of L;

I_L = ideals of L;

Cl_L = p-class group of L; i.e., those ideal-classes of L whose order is a power of p;

h_L = p-class number of L; i.e., $h_L = |Cl_L|$;

r_L = rank of Cl_L; i.e., minimal number of generators of Cl_L;

L' = Hilbert p-class field of L; i.e. the maximal unramified abelian extension of L whose degree is a power of p.

If $\mathfrak{a} \in I_L$, then $[\mathfrak{a}]_L$ will denote the equivalence class in Cl_L generated by the ideal $\mathfrak{a}$. If L/P is a galois extension, then Gal (L/P) will denote its galois group. We shall need the following groups:

$G = \mathrm{Gal}\ (N'/\mathbf{Q})$,

$J = \mathrm{Gal}\ (N'/K)$,

$A = \mathrm{Gal}\ (N'/N)$.

Note that J is the p-Sylow subgroup of G. Class field theory says that

(1) $Cl_N \simeq A$.

We pick a group element $\sigma \in G$ which has order 2 and whose canonical image in G/A generates Gal (N/M). Thus, σ operates on J by conjugation and A is stable under this action. Similarly, we pick an element $\tau \in J$ such that the canonical image of τ in G/A generates Gal (N/K). Hence

$$\sigma^2 = 1,$$
$$\tau^3 = 1 \pmod{A}, \text{ and}$$
$$\sigma\tau\sigma \equiv \tau^{-1} \pmod{A}.$$

The group of ambiguous classes of Cl_N with respect to M (respectively K) is the group of classes of Cl_N which are fixed by the action of σ (respectively τ). We shall denote these groups by $\mathscr{A}_M$ and $\mathscr{A}_K$ respectively.

There is a natural map ϕ, from Cl_K into Cl_N, defined as follows

$$\phi([\mathfrak{a}]_K) = [\mathfrak{a}R_N]_N,$$

where $\mathfrak{a}$ is any ideal in I_K. It is clear that

$$\phi(\mathrm{Cl}_K) \leqq \mathscr{A}_K.$$

LEMMA 3.1. *$\mathscr{A}_K$ is composed of the image of Cl_K under ϕ and the classes generated by the prime ideals of I_N which have ramified in N/K. Thus, $\mathscr{A}_K = \{[\mathscr{B}]_N | \mathscr{B}^p \in I_K\}$. Further $|\mathscr{A}_K| = h_K \cdot p^{s+2t+\alpha-1}$ where*

$$\alpha = \begin{cases} 0 & \text{if } p \nmid f \\ 1 & \text{if } p | f \text{ and } \left(\frac{d}{P}\right) \neq 1 \\ 2 & \text{if } p | f \text{ and } \left(\frac{d}{P}\right) = 1. \end{cases}$$

Proof. See Satz 13 of [**6**].

The above lemma shows that the 'expected' value of $|\mathscr{A}_K|$ is in fact p times the actual value.

LEMMA 3.2. (i) $|\ker \phi| = 1$ *or* p.

(ii) *If J is abelian, then $\phi(\mathrm{Cl}_K) \simeq (\mathrm{Cl}_K)^p$.*

Proof. The first part of this lemma follows from Lemma 3.1, and the second part is an easy consequence of the transfer map (see [**2**] or [**6**]).

This crucial lemma is not true if $d > 0$ or $p = 3$ and $d = -3$; in both cases, the units of K complicate matters. For $p = 3$ and $d = -3$, T. Honda [**9**] has determined exactly when $3|h_M$. For $d > 0$, the results are essentially the same but there is an additional complication. In fact for $d > 0$, the final results depend on whether or not all units of U are norms of units of N.

LEMMA 3.3. $\mathrm{Cl}_M \simeq \mathscr{A}_M$.

Proof. We first prove that

(2) $\mathscr{A}_M = \{[\mathfrak{a}R_N]_N | \mathfrak{a} \in I_M\}$.

It is clear that the left side contains the right side. Suppose that $[\mathfrak{a}]_N \in \mathscr{A}_M$. Then $[\mathfrak{a}\mathfrak{a}^\sigma]_N = [\mathfrak{a}]_N{}^2$. But $\mathfrak{a}\mathfrak{a}^\sigma \in I_M$. Therefore $[\mathfrak{a}]_N{}^2 \in \{[\mathfrak{a}R_N]_N | \mathfrak{a} \in I_M\}$. Since $(p, 2) = 1$, we know that $[\mathfrak{a}]_N{}^{2m} = [\mathfrak{a}]_N$, for some $m \in Z$. Hence

$$[\mathfrak{a}]_N \in \{[\mathfrak{a}R_N]_N | \mathfrak{a} \in I_M\},$$

which proves (2).

It now suffices to show that for all $\mathfrak{a} \in I_M$, $[\mathfrak{a}]_M = 1$ if and only if $[\mathfrak{a}R_N]_N = 1$. One direction is trivial. Suppose that $[\mathfrak{a}R_N]_N = 1$. Then $\mathfrak{a}R_N = (\alpha)$, for some $\alpha \in N$. Thus

$$\mathrm{Norm}_{N/M}(\mathfrak{a}) = (\mathrm{Norm}_{N/M}(\alpha))$$

But $\mathfrak{a} \in I_M$, and so $\mathrm{Norm}_{N/M}(\mathfrak{a}) = \mathfrak{a}^2$. Hence

$$[\mathfrak{a}]_M{}^2 = (\mathrm{Norm}_{N/M}(\alpha))_M = 1.$$

This is impossible since $(2, p) = 1$.

https://doi.org/10.4153/CJM-1976-043-x Published online by Cambridge University Press

Class field theory says that $C_A(\sigma) \simeq \mathscr{A}_M$ where $C_A(\sigma)$ is the centralizer in A of σ. Therefore $C_A(\sigma) \simeq Cl_M$.

PROPOSITION 3.4. *If $r_K \geqq 2$, then $p|h_M$.*

Proof. Suppose that $p \nmid h_M$. Then Equation (1) implies that σ operates in a fixed point free manner on J. This implies that J is abelian (see Theorem 10.1.4 of [**5**]), and so Lemma 3.2 says that $\phi(\mathrm{Cl}_K) \simeq (\mathrm{Cl}_K)P$. Therefore $|\mathrm{Ker}\ \phi| = p^{r_K}$. However, Lemma 3.2 also says that $|\mathrm{Ker}\ \phi| \leqq p$. Hence $r_K \leqq 1$. Therefore $r_K \geqq 2$ implies that $p|h_M$.

PROPOSITION 3.5. *If $s \geqq 2$ (or $s = 1$, $p|f$, and $(d/p) \neq 1$), then $p|h_M$.*

Proof. The hypothesis of the lemma is that there are at least two prime ideals $\mathfrak{q}_1$ and $\mathfrak{q}_2$ in I_K which are fixed by σ and which ramify in N/K. If $p \nmid f$ then $\mathfrak{q}_1$ and $\mathfrak{q}_2$ are principal ideals generated by rational primes. If $p|f$ and $p|d$ then we may assume that $\mathfrak{q}_1^2 = pR_K$. We let

$$\mathscr{Q}_i^p = \mathfrak{q}_i R_N \quad \text{for } i = 1, 2.$$

Lemma 3.1 says that at most one of $[\mathscr{Q}_1]_N$ and $[\mathscr{Q}_2]_N$ is the identity. Therefore we may assume that $[\mathscr{Q}_1]_N$ is not the identity class. However, both $\mathscr{Q}_1$ and $\mathscr{Q}_2$ are fixed by σ and so the ideal class $[\mathscr{Q}_1]_N$ is fixed by σ. Therefore $\mathscr{A}_M$ contains more than the identity which, in view of Lemma 3.3, implies that $p|h_M$.

The next lemma is well known and we state it without proof.

LEMMA 3.6. *Suppose that $\mathfrak{l}$ is any rational prime such that $\mathfrak{l} \equiv 1 \pmod p$. Then there exists a unique cyclic extension of $\mathbf{Q}$ of degree p and discriminant equal to $\mathfrak{l}^{p-1}$. Further there exists a unique cyclic extension of $\mathbf{Q}$ of degree p and discriminant equal to $p^{2(p-1)}$.*

LEMMA 3.7. *Suppose that $\mathfrak{l}$ is a prime such that $\mathfrak{l}|f$ and $\mathfrak{l} \equiv 1 \pmod p$. Let L be the cyclic extension of $\mathbf{Q}$ of degree p and discriminant $\mathfrak{l}^{p-1}$. Then $M \cdot L$ is unramified over M.*

Proof. It suffices to show that $N \cdot L/N$ is unramified at the prime $\mathfrak{l}$. Since $\mathfrak{l} \neq p$, the extension NL/K is tamely ramified, which implies that the interia group of any prime of N which divides $\mathfrak{l}$ is cyclic. However,

$$\mathrm{Gal}\ (N \cdot L/K) \simeq C(p) \times C(p).$$

Therefore this interia group must be isomorphic to $C(p)$. Since $\mathfrak{l}$ is ramified in N/K it follows that $\mathfrak{l}$ does not ramify in $N \cdot L/L$.

LEMMA 3.8. *Suppose that $p|f$. Let L be the unique cyclic extension of $\mathbf{Q}$ of degree p and discriminant $p^{2(p-1)}$. If $(d/p) = 1$, then $L \cdot M$ is unramified over M.*

Proof. It suffices to show that $L \cdot N/K$ is not fully ramified at p. Let $\mathfrak{p}$ be a prime of $N \cdot L$ which divides p. Let $(N \cdot L)_\mathfrak{p}$ denote the localization of $N \cdot L$ at $\mathfrak{p}$, and let $\mathbf{Q}_p$ denote the p-adic rationals. Suppose that $N \cdot L/K$ is fully

https://doi.org/10.4153/CJM-1976-043-x Published online by Cambridge University Press

ramified. Since p splits in $K/\mathbf{Q}$, it follows that

$$\text{Gal}\ ((N \cdot L)_{\mathfrak{p}}/\mathbf{Q}_p) \cong C(p) \times C(p),$$

and that $(N \cdot L)_{\mathfrak{p}}/\mathbf{Q}_p$ is fully ramified. This is possible only if $p = 2$, and we have assumed that $p \neq 2$. Therefore we have a contradiction if $N \cdot L/K$ is fully ramified at p.

PROPOSITION 3.9. *If $t \geqq 1$, or $p|f$ and $(d/p) = 1$, then $p|h_M$.*

Proof. The hypothesis of the proposition implies that there is a cyclic extension L of $\mathbf{Q}$ of degree p such that $L \cdot M$ is unramified over M. It is clear that Gal $(L \cdot M/M) \simeq C(p)$. Class field theory allows us to conclude that $p|h_M$.

The next two lemmas are well known but I include proofs here because I know of no easily available references.

LEMMA 3.10. *Suppose that T is a cyclic extension of prime power degree p^m of the number field L. Then p divides the class number of L if and only if p divides the order of the group of ambiguous classes of T with respect to L.*

Proof. Let $\langle x \rangle = \text{Gal}\ (T/L)$. Then x operates on Cl_T as follows:

$$[\mathfrak{a}]_T{}^x = [\mathfrak{a}^x]_T$$

for all $\mathfrak{a} \in I_T$. If $\gamma \in \text{Cl}_T$, then we define $\bar{\gamma}$, the orbit of γ, by

$$\bar{\gamma} = \{\gamma^{x^n} | n = 1, \ldots, [T : L]\}.$$

This produces a division of Cl_T into disjoint orbits. The order of $\bar{\gamma}$ is obviously divisible by p unless γ is fixed by x. Since the order of Cl_T is the sum of the orders of the orbits, it follows that the order of Cl_T is divisible by p if and only if the number of classes fixed by x is divisible by p.

LEMMA 3.11. *Suppose that Cl_L is cyclic. Then the class number of L' is not divisible by p.*

Proof. We want to prove that L'' is equal to L' (L'' is the Hilbert p-class field of L'). Let $H = \text{Gal}(L''/L)$. Then $H' = \text{Gal}(L''/L')$, and $H/H' \simeq \text{Gal}(L''/L') \simeq \text{Cl}_L$. This means that H/H' is cyclic which implies that H is cyclic (see 5.1.2 of [**5**]). Therefore L'' is abelian over L which implies that $L'' = L'$.

THEOREM 3.12. *Suppose that $p \geqq 5$, or $p = 3$ and $d \not\equiv -3 \pmod 9$. If there is more than one field in $F(p, d, f)$ then the class number of each field in $F(p, d, f)$ is divisible by p.*

Proof. Theorem 2.9 says that there is more than one field in $F(p, d, f)$ if and only if $r_K + s + t + v \geqq 2$. Therefore we shall assume that $r_K + s + t + v \geqq 2$ and that $M \in F(p, d, f)$. If $r_K \geqq 2$, $s \geqq 2\ t \geqq 1$, or $v = 1$ and $(d/p) = 1$, then Propositions 3.4, 3.5 and 3.9 respectively, imply that $p|h_M$. There are several special cases still to be considered.

https://doi.org/10.4153/CJM-1976-043-x Published online by Cambridge University Press

Suppose $v = t = 0$ and that $r_K = s = 1$. Then f is equal to a prime which is inert in K. Let $qR_K = \mathfrak{q}$ and $qR_N = \mathscr{Q}^p$. Suppose that $p \nmid h_M$. Then the argument used in the proof of Proposition 3.4 shows that $|\text{Ker } \phi| = p$. This would imply, by Lemma 3.1, that $[\mathscr{Q}]_N$ is not the identity class. However, as was shown in the proof of Proposition 3.5, $[\mathscr{Q}]_N$ is an $\mathscr{A}_M$. Therefore Lemma 3.3 says that $p|h_M$. This is a contradiction and so $r_K = s = 1$ must imply that $p|h_M$.

If $r_K = v = 1$ and $(d/p) \neq 1$, then the same argument can be used. If $v = 2$ we must have $p = 3$ and $d \equiv -3 \pmod 9$ which is contrary to the hypothesis of the theorem.

LEMMA 3.13. *Suppose $r_K + s = 1$ and $t + v = 0$. Then $p \nmid h_M$. Further, if $p|f$ but $(d/p) \neq 1$ and $r_K + s = 0$, then $p \nmid h_M$.*

Proof. We first suppose that $t + s + v = 0$ and $r_K = 1$. This means that $f = 1$ and Cl_K is cyclic. Thus N is unramified over K. Lemma 3.11 says that $p \nmid h_{K'}$, which implies that $N' = K'$. Therefore, Lemma 3.1 implies that $\text{Cl}_N = \mathscr{A}_K = \phi(\text{Cl}_K)$. Since σ fixes no class in $\phi(\text{Cl}_K)$ except the identity class this means that $\mathscr{A}_M$ contains only the identity class.

Suppose that $r_K + v + t = 0$ and $s = 1$. Then Lemma 3.1 says that $|\mathscr{A}_K| = 1$. Class field theory implies that $Z(J) \cap A \simeq \mathscr{A}_K$. Therefore we know that $Z(J) \cap A = \{1\}$. Since J is a p-group this implies that $A = \{1\}$ which means that $\text{Cl}_N = \{1\}$. Therefore $\text{Cl}_M = \{1\}$. A similar proof works for $r_K + t + s = 0$ and $v = 1$ with $(d/p) \neq 1$.

THEOREM 3.14. *If $d \equiv -3 \pmod 9$, d is negative, and there is more than one field in $F(3, d, f)$, then either 3 divides the class number of each field, or $r_K = 0$ and $f = 3^2$. There are 3 fields in $F(3, d, 3^2)$ and each of them has class number prime to 3.*

Proof. This theorem can be proved in the same way as Theorem 3.12 except when $f = 3^2$ and $r_K = 0$. That this case can occur is a consequence of Lemma 2.3. Lemma 3.13 shows that $f = 3^2$ and $r_K = 0$ implies that $3 \nmid h_M$. The fact that $F(3, d, 3^2)$ contains three fields is easily deduced from Lemma 2.3.

THEOREM 3.15. *Suppose that $p \geqq 5$ (or $p = 3$ and $d \not\equiv -3 \pmod 9$). If $M \in F(p, d, f)$ and $p|h_M$, then one of the following is true:*

(1) *There is more than one field in $F(p, d, f)$;*

(2) *f is equal to a prime congruent to 1 modulo p and $r_K = 0$ or $f = p$, $(d/p) = 1$ and $r_K = 0$.*

In the second case there is exactly one field in $F(p, d, f)$.

Proof. Suppose that $p|h_M$ and that $r_K + s + t + v = 1$. Then Lemma 3.13 shows that either $L = 1$ or $v = 1$ and $(d/p) = 1$. In either case, Proposition 3.9 ensures that $p|h_M$ and Lemma 2.6 says that $|F(p, d, f)| = 1$. If $r_K + s + t + v = 0$, then $|F(p, d, f)|$ is empty. There is only one remaining possibility,

https://doi.org/10.4153/CJM-1976-043-x Published online by Cambridge University Press

$r_K + s + t + \alpha \geqq 2$. In this case Theorem 2.9 says that there is more than one field in $F(p, d, f)$.

The results of Theorems 3.12 and 3.15 can be combined to yield the following theorem.

THEOREM 3.16. *Suppose that* $d < 0$ *and if* $p = 3$, *that* $d \not\equiv -3 \pmod 9$. *If* $M \in F(p, d. f)$ *then* $p | h_M$ *if and only if the one of following is true:*
(i) $s + 2t + v + r_K \geqq 2$;
(ii) $v = 1$ *and* $(d/p) = 1$.

4. The table included below illustrates the principal results of this paper for $p = 3$. Larger values of p are difficult to work with for obvious reasons. I have endeavoured to list the smallest value of D (smallest in absolute value) which has the required characteristics. The examples are chosen to illustrate the "critical cases" of the theorems proved above; if we allow many prime divisors of f or large values of r_K then the size of D becomes unmanageable and the theorems are not as interesting. In the tenth column we have used the symbol # to denote the number of fields with the given discriminant; i.e. the number of fields in $F(3, d, f)$. The three cases marked by asterisks are counterexamples to the approximate statement that $|F(p, d, f)| > 1$ if and only if each field in $F(p, d, f)$ has class number divisible by p. In compiling this table essential use was made of "A Table of Complex Cubic Fields" kindly sent to me by I. Angell, (see [**1**]).

$-D$	$-d$	f	v		$(d/3)$	s	t	r_K	#	h_M
76	19	2	0			1	0	0	1	1
23	23	1		$3 \nmid f$		0	0	1	1	1
676*	4	13		$3 \nmid d$		0	1	0	1	3
2075	83	5				1	0	1	3	3
4300	43	$2 \cdot 5$		$v = 1$		2	0	0	2	3
3299	3299	1				0	0	2	4	3
324	4	3^2	1	$3 \mid f$	-1	0	0	0	1	1
648*	8	3^2			$+1$	0	0	0	1	3
8667	107	3^2		$3 \nmid d$	$+1$	0	0	1	3	3
6156	19	$2 \cdot 3^2$			-1	1	0	0	2	3
135	15	3	1	$d \equiv +3$	0	0	0	0	1	1
6936	771	3		(mod 9)	0	0	0	1	3	3
1836	51	$2 \cdot 3$		$3 \mid f$	0	1	0	1	2	3
351	39	3	1	$d \equiv -3$	0	0	0	0	1	1
3159*		3^2	2	(mod 9)	0	0	0	0	3	1

REFERENCES

1. I. O. Angell, *A table of complex cubic fields*, Bull. London Math. Soc. *5* (1973), 37–38.
2. E. Artin and J. Tate, *Class field theory* (Harvard, 1961).
3. T. Callahan, *The 3-class groups of non-Galois cubic fields I*, Mathematika *21* (1974), 72–89.

https://doi.org/10.4153/CJM-1976-043-x Published online by Cambridge University Press

4. ——— *The 3-class groups of non-Galois cubic fields II*, Mathematika *21* (1974), 168–188.

5. D. Gorenstien, *Finite groups* (Harper and Row, 1968).

6. H. Hasse, *Bericht über neuere Untersuchungen und Problem aus der Theorie der algraischen Zahlkörper*. Jahr. der D. Math. Ver., *35* (1926), 1–55; *ibid. 36* (1927), 255–311; *ibid. 39* (1930), 1–204.

7. ——— *Arithmetiche Theorie der Rubischen Zahlkörper auf Klassenkorpertheore-tischer Grundlage*, Math. Zeit. *31* (1960), 565–582.

8. H. Heilbronn, *Zeta functions and L-functions*, in *Algebraic number theory*, edited by J. Cassels and A. Frölich (Thompson 1967).

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

10. J. Martinet, *Sur l'arithmétique des extensions Galoisiennes à groupe de Galois diedral d'ordre* 2 *p*. (Thèse, Grenoble 1968) Ann. Inst. Fourier, *19* (1969), 1–80.

11. H. Reichardt, *Arithmetische theorie der rubischen körper als radikalkörper*, Monatshefte Math. Phys., *40* (1933), 323–350.

University of Toronto,
Toronto, Ontario

https://doi.org/10.4153/CJM-1976-043-x Published online by Cambridge University Press