CUBIC FIELDS WHOSE CLASS NUMBERS ARE NOT DIVISIBLE BY 3

BY

FRANK GERTH III

1. Main results

In this paper we describe a procedure for finding the discriminants of all cubic extensions L of the rational numbers $\mathbf{Q}$ such that $3 \nmid h_L$, where h_L is the class number of L. We first consider the case where $L/\mathbf{Q}$ is Galois. In this case $L/\mathbf{Q}$ is a cyclic cubic extension, and the following result is well known (cf. [4, Theorem 1 and Corollary to Theorem 4]).

THEOREM 1. *For $D = 9^2$ and $D = p^2$, where p is any rational prime $\equiv$ 1 (mod 3), there is a unique cyclic cubic extension $L/\mathbf{Q}$ whose discriminant is D. These fields are the only cyclic cubic extensions of $\mathbf{Q}$ whose class numbers are not divisible by* 3.

We now consider the case where $L/\mathbf{Q}$ is not Galois. We let K denote the normal closure of $L/\mathbf{Q}$, and we let F be the quadratic subfield of K. We let D denote the discriminant of $L/\mathbf{Q}$. The following results are known (cf. [3] and [6]).

LEMMA 1. *$D = df^2$, where d and f are rational integers, d is the discriminant of $F/\mathbf{Q}$, and f is the conductor of the cyclic cubic extension K/F. Furthermore, if p is a rational prime dividing f and $p \neq 3$, then p decomposes in $F/\mathbf{Q}$ if $p \equiv 1$ (mod 3), and p is inert in $F/\mathbf{Q}$ if $p \equiv -1$ (mod 3). Also $p^2 \nmid f$ for any rational prime $p \neq 3$, and $3^3 \nmid f$.*

We now specify all non-Galois cubic extensions $L/\mathbf{Q}$ such that $3 \nmid h_L$.

THEOREM 2. *Let F be a quadratic extension of $\mathbf{Q}$ with discriminant d. Let S_F denote the 3-class group of F. In each part below, we give the discriminants D of the non-Galois cubic extensions $L/\mathbf{Q}$ such that F is contained in the normal closure of $L/\mathbf{Q}$ and $3 \nmid h_L$, where h_L is the class number of L. Unless otherwise indicated, there is a unique L (up to conjugacy) with the specified discriminant D.*

(a) *S_F is not cyclic. Then no such L exists.*

(b) *$S_F \neq \{1\}$ but S_F is cyclic. Then L has discriminant $D = d$.*

(c) *$S_F = \{1\}$. Let A be the set of rational primes $\equiv -1$ (mod 3) which are inert in F. Let e be a primitive cube root of unity if $d = -3$; let e be the fundamental unit of F when $d > 0$; and let $e = 1$ otherwise. Let*

$$A_1 = \{p \in A \mid e \text{ is a cubic residue } (\text{mod } p\mathcal{O}_F)\},$$

Received June 6, 1975.

where $\mathcal{O}_F$ is the ring of integers of F, and let

$$A_2 = \{p \in A \mid e \text{ is not a cubic residue } (\text{mod } p\mathcal{O}_F)\}.$$

(Note that $A_1 = A$ and A_2 is empty when $e = 1$.) If $d \equiv -1 \pmod 3$, let $B = \{3\}$ if e is a cubic residue $(\text{mod } 9\mathcal{O}_F)$, and let B be empty if e is not a cubic residue $(\text{mod } 9\mathcal{O}_F)$. If $d \equiv \pm 3 \pmod 9$, let $B = \{3\}$ if e is a cubic residue $(\text{mod } 3\mathcal{O}_F)$, and let B be empty if e is not a cubic residue $(\text{mod } 3\mathcal{O}_F)$. Then the L such that $3 \nmid h_L$ have the following discriminants:

(i) $D = dp^2$ *where p is any element of* A_1;
(ii) $D = dp_1^2 p_2^2$ *where* p_1 *and* p_2 *are any distinct elements of* A_2;
(iii) $D = d \cdot 9^2$ *if* $d \equiv -1 \pmod 3$ *and* $3 \in B$;
(iv) $D = d \cdot 9^2 \cdot p^2$ *if* $d \equiv -1 \pmod 3$, $3 \notin B$, *and p is any element of* A_2;
(v) $D = d \cdot 3^2$ *if* $d \equiv 3 \pmod 9$ *and* $3 \in B$;
(vi) $D = d \cdot 3^2 \cdot p^2$ *if* $d \equiv 3 \pmod 9$, $3 \notin B$, *and p is any element of* A_2;
(vii) $D = d \cdot 3^2$ *if* $d \equiv -3 \pmod 9$ *and* $3 \in B$;
(viii) $D = d \cdot 3^2 \cdot p^2$ *if* $d \equiv -3 \pmod 9$, $3 \notin B$, *and p is any element of* A_2;
(ix) $D = d \cdot 9^2$ *(for three nonconjugate L) if* $d \equiv -3 \pmod 9$ *and* $3 \in B$;
(x) $D = d \cdot 9^2$ *if* $d \equiv -3 \pmod 9$ *and* $3 \notin B$;
(xi) $D = d \cdot 9^2 \cdot p^2$ *(for two nonconjugate L) if* $d \equiv -3 \pmod 9$, $3 \notin B$, *and p is any element of* A_2.

Remark. Assume $d = -3$. Then e is not a cubic residue $(\text{mod } 3\mathcal{O}_F)$. Furthermore e is a cubic residue $(\text{mod } p\mathcal{O}_F)$ if $p \equiv 8 \pmod 9$, and e is not a cubic residue $(\text{mod } p\mathcal{O}_F)$ if $p \equiv 2$ or $5 \pmod 9$. Then it is easy to see that our results in Theorem 2 agree with the results in [5] for the case $d = -3$.

In Sections 2 and 3, we shall prove Theorem 2.

2. Necessary conditions for D

We let L be a non-Galois cubic extension of $\mathbf{Q}$, K the normal closure of L, and F the quadratic subfield of K. We first prove the following lemma (cf. [1, Lemmas 4.7 and 4.8]).

LEMMA 2. *If p is a rational prime which ramifies totally in $L/\mathbf{Q}$ and decomposes in $F/\mathbf{Q}$, then $3 \mid h_L$, where h_L is the class number of L.*

Proof. By Lemma 1, either $p = 3$ or $p \equiv 1 \pmod 3$. Let $M/\mathbf{Q}$ be the cyclic cubic extension with discriminant 9^2 if $p = 3$ and with discriminant p^2 if $p \equiv 1 \pmod 3$. Then $M \cdot L$ is a cyclic cubic extension of L. We shall show that $M \cdot L$ is unramified over L, and hence $3 \mid h_L$ by class field theory. Let $\mathfrak{p}$ be the unique prime of L above p. Since only p ramifies in $M/\mathbf{Q}$, it suffices to show that $\mathfrak{p}$ is unramified in $M \cdot L/L$. Let $\mathbf{Q}_p$ denote the field of p-adic numbers, and let $L_\mathfrak{p} = L \cdot \mathbf{Q}_p$. Since p decomposes in $F/\mathbf{Q}$, then $F \cdot \mathbf{Q}_p = \mathbf{Q}_p$, and hence $L_\mathfrak{p} = L \cdot F \cdot \mathbf{Q}_p = K \cdot \mathbf{Q}_p$. Since K/F is a cyclic cubic extension in which the primes above p ramify, then $L_\mathfrak{p}/\mathbf{Q}_p$ is a cyclic cubic extension in which p ramifies.

Let $M_{\mathfrak{P}} = M \cdot \mathbf{Q}_p$. Then $M_{\mathfrak{P}}/\mathbf{Q}_p$ is also a cyclic cubic extension in which p ramifies. Now if $\mathfrak{p}$ ramifies in $M \cdot L/L$, then $M_{\mathfrak{P}} \cdot L_{\mathfrak{p}}$ is a totally ramified extension of $\mathbf{Q}_p$ with Galois group isomorphic to $\mathbf{Z}/3\mathbf{Z} \oplus \mathbf{Z}/3\mathbf{Z}$. By local class field theory there is no such extension. Hence $\mathfrak{p}$ must be unramified in $M \cdot L/L$, and then $3 \mid h_L$.

The following result is proved in [2, Theorem 3.5].

LEMMA 3. *Let S_L (resp. S_F) denote the 3-class group of L (resp. F). Then*

$$\text{rank } S_L = r + t - 1 - z - w$$

where $r = \text{rank } S_F$, $t =$ *number of ramified primes in K/F,*

$z =$ *rank of a certain subgroup of S_F/S_F^3,*

$w =$ *rank of a certain matrix of norm residue symbols.*

Also $0 \leq z \leq \min(r, u)$, where u is the number of rational primes which ramify totally in $L/\mathbf{Q}$ and decompose in $F/\mathbf{Q}$. Furthermore, the matrix has $t - 1$ rows and $r + u - z + 1$ columns.

Note. In Lemma 3, the rank of an abelian 3-group S (e.g., rank S_L, rank S_F) is defined as follows: rank $S = \dim_{\mathbf{F}_3}(S/S^3)$, where $\mathbf{F}_3$ is the finite field of 3 elements. This rank is also called the 3-rank of S.

Remark. $w = 0$ if $t \leq 1$.

Now assume $3 \nmid h_L$. By Lemma 2, $u = 0$. Hence $z = 0$ in Lemma 3. Then from Lemma 3, we get

$$\text{rank } S_L = r + t - 1 - w \tag{1}$$

where w is the rank of a certain matrix with $t - 1$ rows and $r + 1$ columns. We first suppose that $r > 0$. If we also suppose that $t > 0$, then $w \leq t - 1$, and Equation 1 implies

$$\text{rank } S_L = r + t - 1 - w \geq r > 0,$$

which contradicts $3 \nmid h_L$. So we cannot have $3 \nmid h_L$ if both $r > 0$ and $t > 0$. Next we suppose $r > 0$ and $t = 0$. Then $w = 0$, and rank $S_L = r - 1$. So $3 \nmid h_L$ if and only if $r = 1$. Hence when $r > 0$ (which means $S_F \neq \{1\}$), we have proved that $3 \nmid h_L$ if and only if $r = 1$ (which means S_F is cyclic but $S_F \neq \{1\}$) and $t = 0$ (which means that K/F is unramified, and hence the discriminant of L is $D = d \cdot 1^2 = d$). This proves Theorem 2 (a–b), provided there exists a unique (up to conjugacy) non-Galois cubic field with discriminant $D = d$ when S_F is cyclic but $S_F \neq \{1\}$. Now by class field theory, when S_F is cyclic and $S_F \neq \{1\}$, there is a unique cyclic cubic unramified extension K of F, and $K/\mathbf{Q}$ is Galois with Galois group isomorphic to the symmetric group on three letters. K contains three conjugate subfields of degree 3 over $\mathbf{Q}$, and each has discriminant $D = d$. Hence there exists a non-Galois cubic extension L of $\mathbf{Q}$ with discriminant $D = d$, and L is unique up to conjugacy.

We must still prove Theorem 2 (c)(i–xi). So we suppose $S_F = \{1\}$, which means $r = 0$. By class field theory $r = 0$ implies that K/F cannot be unramified, and hence $t \geq 1$. Then from Equation 1,

$$\text{rank } S_L = t - 1 - w$$

where w is the rank of a $(t - 1) \times 1$ matrix. So $w = 0$ or 1. Then $3 \nmid h_L$ if and only if $t = 1$ and $w = 0$, or $t = 2$ and $w = 1$. Let e be defined as in Theorem 2 (c). Then by [2, Corollary 3.7], $w = 0$ if e is a local norm at each prime of F which ramifies in K, and $w = 1$ otherwise. We note that $t = 1$ implies $w = 0$ by the product formula for norm residue symbols, and if $t = 2$, the product formula implies that e is a local norm at both of the ramified primes of K/F or at neither of them. Furthermore, if $3 \nmid h_L$, then Lemmas 1 and 2 imply that the primes of F which ramify in K must be either rational primes $p \equiv -1 \pmod 3$, 3 (if 3 is inert in $F/\mathbf{Q}$), or the unique prime of F above 3 if 3 ramifies in $F/\mathbf{Q}$. Also it is easy to see that e is a local norm at a prime $p \equiv -1 \pmod 3$ if and only if e is a cubic residue (mod $p\mathcal{O}_F$). Correlating the above results for the case where $S_F = \{1\}$, we obtain the following restrictions for the discriminants D of the non-Galois cubic fields $L/\mathbf{Q}$ such that $3 \nmid h_L$.

LEMMA 4. *Let notations be as in Theorem 2. If $S_F = \{1\}$, then $3 \nmid h_L$ if and only if the discriminant D of L has one of the following forms:*

(i) $D = dp^2$ *with* $p \in A_1$;
(ii) $D = d \cdot 3^2$ *or* $d \cdot 9^2$;
(iii) $D = dp_1^2p_2^2$ *with* p_1 *and* p_2 *distinct elements of* A_2;
(iv) $D = d \cdot 3^2 \cdot p^2$ or $d \cdot 9^2 \cdot p^2$ *with* $p \in A_2$.

Remark. D is restricted to dp^2, $d \cdot 3^2$, and $d \cdot 9^2$ when $t = 1$ (and $w = 0$), and D is restricted to $dp_1^2p_2^2$, $d \cdot 3^2 \cdot p^2$, and $d \cdot 9^2 \cdot p^2$ when $t = 2$ and $w = 1$. However we have not proved that there exists an L for each of the possible values of D; what we have proved is that if there is an L with discriminant D, then $3 \nmid h_L$ if and only if D has one of the above forms. In the next section we determine for which of the possible values of D there exists an L with discriminant D.

3. Completion of proof of Theorem 2(c)

We first review some results on ideal class groups. Let F be a finite extension field of $\mathbf{Q}$, and let $\mathfrak{m}$ be an integral ideal of F. Let $I(\mathfrak{m})$ denote the group of all fractional ideals of F which are relatively prime to $\mathfrak{m}$, and let

$$P(\mathfrak{m}) = \{\alpha\mathcal{O}_F \mid \alpha \in F^x \text{ and } \alpha \equiv 1 \ (\text{mod}^* \ \mathfrak{m})\},$$

where $\mathcal{O}_F$ is the ring of integers of F, $F^x = F - \{0\}$, and "$\alpha \equiv 1$ (mod*$\mathfrak{m}$)" means "for every prime $\mathfrak{p} \mid \mathfrak{m}$, α is a $\mathfrak{p}$-unit and $\alpha \equiv 1 \pmod{\mathfrak{m}_\mathfrak{p}}$ in the $\mathfrak{p}$ completion of F". (When dealing with integral elements of F, we shall usually write mod $\mathfrak{m}$ instead of mod* $\mathfrak{m}$.) For $\mathfrak{m} = \mathcal{O}_F$, we let I denote $I(\mathcal{O}_F)$ and P denote $P(\mathcal{O}_F)$. Then I/P is the ideal class group, and for arbitrary integral ideals $\mathfrak{m}$ of F,

$I(\mathfrak{m})/P(\mathfrak{m})$ is called the ideal class group modulo $\mathfrak{m}$. For a given $\mathfrak{m}$, it is known that each element of I/P can be represented by an ideal which is prime to $\mathfrak{m}$; hence there is a natural surjection ψ: $I(\mathfrak{m})/P(\mathfrak{m}) \to I/P$. The kernel of ψ is $(I(\mathfrak{m}) \cap P)/P(\mathfrak{m})$. Let $\alpha_1, \ldots, \alpha_s \in \mathcal{O}_F$ be a set of representatives for $(\mathcal{O}_F/\mathfrak{m})^x$, where $(\mathcal{O}_F/\mathfrak{m})^x$ denotes the group of invertible elements of $\mathcal{O}_F/\mathfrak{m}$. Then $(\alpha_i) \in I(\mathfrak{m}) \cap P$ for each i, where (α_i) denotes $\alpha_i\mathcal{O}_F$. If $\beta_1, \ldots, \beta_s$ is another set of representatives for $(\mathcal{O}_F/\mathfrak{m})^x$ with $\beta_i \equiv \alpha_i \pmod{\mathfrak{m}}$ for each i, then $(\beta_i\alpha_i^{-1}) \in P(\mathfrak{m})$. So the image of (β_i) in $(I(\mathfrak{m}) \cap P)/P(\mathfrak{m})$ is the same as the image of (α_i) in $(I(\mathfrak{m}) \cap P)/P(\mathfrak{m})$. So there is a well-defined map

$$\lambda\colon (\mathcal{O}_F/\mathfrak{m})^x \to (I(\mathfrak{m}) \cap P)/P(\mathfrak{m}).$$

It is easy to see that λ is surjective. Now $(\alpha_i) \in P(\mathfrak{m})$ if and only if $\alpha_i\varepsilon \equiv 1 \pmod{\mathfrak{m}}$ for some unit ε of F if and only if $\alpha_i \equiv \varepsilon^{-1} \pmod{\mathfrak{m}}$ for some unit ε of F. So kernel $\lambda \cong E/E_{\mathfrak{m}}$, where E is the group of units of F, and $E_{\mathfrak{m}} = \{\varepsilon \in E \mid \varepsilon \equiv 1 \pmod{\mathfrak{m}}\}$. From the exact sequences

$$1 \longrightarrow (I(\mathfrak{m}) \cap P)/P(\mathfrak{m}) \longrightarrow I(\mathfrak{m})/P(\mathfrak{m}) \xrightarrow{\psi} I/P \longrightarrow 1$$

and

$$1 \longrightarrow E/E_{\mathfrak{m}} \to (\mathcal{O}_F/\mathfrak{m})^x \xrightarrow{\lambda} (I(\mathfrak{m}) \cap P)/P(\mathfrak{m}) \longrightarrow 1$$

we get the exact sequence

$$1 \to (\mathcal{O}_F/\mathfrak{m})^x/(E/E_{\mathfrak{m}}) \to I(\mathfrak{m})/P(\mathfrak{m}) \to I/P \to 1. \tag{2}$$

We now return to the case where F is quadratic with discriminant d, and the 3-class group $S_F = \{1\}$. We want to find all non-Galois cubic fields $L/\mathbf{Q}$ with discriminants df^2, where f is a rational integer, such that $3 \nmid h_L$, where h_L is the class number of L. Let $C(\mathfrak{m}) = I(\mathfrak{m})/P(\mathfrak{m})$, and let σ be the generator of $G = \mathrm{Gal}\,(F/\mathbf{Q})$. If we assume $\mathfrak{m}^\sigma = \mathfrak{m}$, then $C(\mathfrak{m})$ is a G-module. Let $S(\mathfrak{m}) = C(\mathfrak{m})/(C(\mathfrak{m}))^3$. Then $S(\mathfrak{m})$ is a G-module, and it is straightforward to check that

$$S(\mathfrak{m}) \cong S(\mathfrak{m})^+ \times S(\mathfrak{m})^-$$

where $S(\mathfrak{m})^+ = \{a \in S(\mathfrak{m}) \mid a^\sigma = a\}$ and $S(\mathfrak{m})^- = \{a \in S(\mathfrak{m}) \mid a^\sigma = a^{-1}\}$. By class field theory $S(\mathfrak{m})$ is isomorphic to the Galois group of the abelian extension M of F of exponent 3 which is the composition of all cyclic cubic extensions of F whose conductors divide $\mathfrak{m}$. Let M^+ be the compositum of F and all cyclic cubic extensions of $\mathbf{Q}$ contained in M. Let M^- be the compositum of the normal closures K of all non-Galois cubic extensions L of $\mathbf{Q}$ that are contained in M. Then $(M^+/F) \cong S(\mathfrak{m})^+$, and $\mathrm{Gal}\,(M^-/F) \cong S(\mathfrak{m})^-$.

Our goal is to consider the $\mathfrak{m}$ which are associated with the discriminants in Lemma 4 and determine when $S(\mathfrak{m})^- \neq \{1\}$. From Lemma 4, we see that we need to consider the following $\mathfrak{m}$:

$$\mathfrak{m} = (p) \text{ with } p \in A_1, \qquad \mathfrak{m} = (3) \text{ and } (9),$$

$$\mathfrak{m} = (p_1p_2) \text{ with } p_1 \text{ and } p_2 \text{ distinct elements of } A_2,$$

$$\mathfrak{m} = (3p) \text{ and } (9p) \text{ with } p \in A_2.$$

We note that $\mathfrak{m}^\sigma = \mathfrak{m}$ for all of these $\mathfrak{m}$, where σ is the generator of Gal $(F/\mathbf{Q})$. Hence the results of this section apply to these values of $\mathfrak{m}$. To determine when $S(\mathfrak{m})^- \neq \{1\}$, we shall exploit the exact sequence (2). We let $Y(\mathfrak{m}) = (\mathcal{O}_F/\mathfrak{m})^x/(E/E_\mathfrak{m})$ and $T(\mathfrak{m}) = Y(\mathfrak{m})/(Y(\mathfrak{m}))^3$. Since the 3-class group of F is trivial by assumption, the exact sequence (2) implies $S(\mathfrak{m}) \cong T(\mathfrak{m})$.

We first consider $\mathfrak{m} = (p)$ with $p \in A_1$. Let e be defined as in Theorem 2. We note that $(\mathcal{O}_F/(p))^x$ is a cyclic group of order $p^2 - 1$ and $3 \mid (p^2 - 1)$. Also e is a cubic residue mod (p) since $p \in A_1$. Hence $S(p) \cong T(p) \cong \mathbf{Z}/3\mathbf{Z}$. Also $S(p)^+ = \{1\}$ since there is no cyclic cubic extension of $\mathbf{Q}$ with conductor p for $p \in A_1$. So $S(p)^- \cong S(p) \cong \mathbf{Z}/3\mathbf{Z}$. This implies that there is a unique (up to conjugacy) non-Galois cubic field L with discriminant dp^2. This fact and Lemma 4(i) imply Theorem 2(c)(i).

Next we consider $\mathfrak{m} = (p_1p_2)$ with p_1 and p_2 distinct elements of A_2. Then $(\mathcal{O}_F/(p_1p_2))^x$ is the product of cyclic groups of order $p_1^2 - 1$ and $p_2^2 - 1$ with $3 \mid (p_1^2 - 1)$ and $3 \mid (p_2^2 - 1)$. Also e is not a cubic residue mod (p_1p_2) since $p_1, p_2 \in A_2$. It is then easy to see that $S(p_1p_2) \cong \mathbf{Z}/3\mathbf{Z}$. Since there is no cyclic cubic extension of $\mathbf{Q}$ with conductor p_1p_2 for $p_1, p_2 \in A_2$, then

$$S(p_1p_2)^+ = \{1\} \quad \text{and} \quad S(p_1p_2)^- \cong S(p_1p_2) \cong \mathbf{Z}/3\mathbf{Z}.$$

So there is a unique (up to conjugacy) non-Galois cubic field L with discriminant $dp_1^2p_2^2$. This fact and Lemma 4(iii) imply Theorem 2(c)(ii).

In the remaining cases $(3) \mid \mathfrak{m}$. We first note that we do not need any cases where $d \equiv 1 \pmod 3$, since then 3 would decompose in F and would ramify totally in L, and hence 3 would divide h_L by Lemma 2.

We now consider $d \equiv -1 \pmod 3$. Then 3 is inert in F. For $\mathfrak{m} = (3)$, $(\mathcal{O}_F/(3))^x$ is a cyclic group of order 8, and hence $S(3)$ is trivial. Furthermore $S(3p) = \{1\}$ for $p \in A_2$. Now let $\mathfrak{m} = (9)$. Then

$$S(9) \cong T(9) \cong \mathbf{Z}/3\mathbf{Z} \oplus \mathbf{Z}/3\mathbf{Z} \quad \text{or} \quad \mathbf{Z}/3\mathbf{Z},$$

according as e is a cubic residue mod (9) or not. We note that $S(9)^+ \cong \mathbf{Z}/3\mathbf{Z}$ since there is a unique cyclic cubic extension of $\mathbf{Q}$ with conductor 9. So $S(9)^- \cong \mathbf{Z}/3\mathbf{Z}$ or $\{1\}$, according as e is a cubic residue mod (9) or not. In the notation of Theorem 2, $S(9)^- \cong \mathbf{Z}/3\mathbf{Z}$ or $\{1\}$, according as $3 \in B$ or $3 \notin B$. So when $3 \in B$, there is a unique (up to conjugacy) non-Galois cubic field L with discriminant $d \cdot 9^2$. When $3 \notin B$, it can be checked that $S(9p)^- \cong \mathbf{Z}/3\mathbf{Z}$ if $p \in A_2$. Hence when $3 \notin B$ and $p \in A_2$, there is a unique (up to conjugacy) non-Galois cubic field L with discriminant $d \cdot 9^2 \cdot p^2$. When $3 \in B$ and $p \in A_2$, it is also true that $S(9p)^- \cong \mathbf{Z}/3\mathbf{Z}$. However, since $S(9)^- \cong \mathbf{Z}/3\mathbf{Z}$ when $3 \in B$, the cubic extension associated with $S(9p)^-$ is the one associated with $S(9)^-$. So no new cubic field occurs in this case. The results of this paragraph and Lemma 4(ii and iv) imply Theorem 2(c)(iii–iv).

Now we consider $d \equiv 3 \pmod 9$. In this case $S(3) \cong \mathbf{Z}/3\mathbf{Z}$ or $\{1\}$, according as e is a cubic residue mod (3) or not, according as $3 \in B$ or $3 \notin B$ (using the notation of Theorem 2). Since there is no cyclic cubic extension of $\mathbf{Q}$ with conductor 3, then $S(3)^- \cong \mathbf{Z}/3\mathbf{Z}$ or $\{1\}$, according as $3 \in B$ or $3 \notin B$. So there is a unique (up to conjugacy) non-Galois cubic field L with discriminant $d \cdot 3^2$ when $3 \in B$. If $3 \notin B$, then it can be checked that $S(3p)^- \cong \mathbf{Z}/3\mathbf{Z}$ if $p \in A_2$, and hence there is a unique (up to conjugacy) non-Galois cubic field with discriminant $d \cdot 3^2 \cdot p^2$. When $3 \in B$ and $p \in A_2$, then $S(3p)^- \cong \mathbf{Z}/3\mathbf{Z}$. However $S(3)^- \cong \mathbf{Z}/3\mathbf{Z}$ when $3 \in B$, and hence no new cubic field is associated with $S(3p)^-$. Next we consider $\mathfrak{m} = (9)$. We note that the Sylow 3-subgroup of $(\mathcal{O}_F/(9))^x$ is isomorphic to $\mathbf{Z}/3\mathbf{Z} \oplus \mathbf{Z}/9\mathbf{Z}$. So

$$S(9) \cong \mathbf{Z}/3\mathbf{Z} \oplus \mathbf{Z}/3\mathbf{Z} \quad \text{or} \quad \mathbf{Z}/3\mathbf{Z}.$$

If $3 \in B$, then $S(9) \cong \mathbf{Z}/3\mathbf{Z} \oplus \mathbf{Z}/3\mathbf{Z}$ with $S(9)^+ \cong \mathbf{Z}/3\mathbf{Z}$ (since there is a unique cyclic cubic extension of $\mathbf{Q}$ with conductor 9) and $S(9)^- \cong \mathbf{Z}/3\mathbf{Z}$. However, since $S(3)^- \cong \mathbf{Z}/3\mathbf{Z}$ when $3 \in B$, no new cubic field is associated with $S(9)^-$. When $3 \notin B$, it can be checked that $S(9) \cong S(9)^+ \cong \mathbf{Z}/3\mathbf{Z}$ and $S(9)^- \cong \{1\}$. If $p \in A_2$, then $S(9p)^- \cong \mathbf{Z}/3\mathbf{Z}$. However no new cubic field occurs because $S(3)^- \cong \mathbf{Z}/3\mathbf{Z}$ when $3 \in B$, and $S(3p)^- \cong \mathbf{Z}/3\mathbf{Z}$ when $3 \notin B$. The results of this paragraph and Lemma 4(ii and iv) imply Theorem 2 (c) (v–vi).

Finally we let $d \equiv -3 \pmod 9$. Then $S(3)^+ = \{1\}$, and $S(3)^- \cong S(3) \cong \mathbf{Z}/3\mathbf{Z}$ or $\{1\}$, according as $3 \in B$ or $3 \notin B$. So when $3 \in B$, there is a unique (up to conjugacy) non-Galois cubic field with discriminant $d \cdot 3^2$. It can be checked that $S(3p)^- \cong \mathbf{Z}/3\mathbf{Z}$ when $3 \notin B$ and $p \in A_2$, and hence there is a unique (up to conjugacy) non-Galois cubic field with discriminant $d \cdot 3^2 \cdot p^2$. Also $S(3p)^- \cong \mathbf{Z}/3\mathbf{Z}$ when $3 \in B$ and $p \in A_2$, but no new cubic field occurs since $S(3)^- \cong \mathbf{Z}/3\mathbf{Z}$ when $3 \in B$. We now take $\mathfrak{m} = 9$. The Sylow 3-subgroup of $(\mathcal{O}_F/(9))^x$ is isomorphic to

$$\mathbf{Z}/3\mathbf{Z} \oplus \mathbf{Z}/3\mathbf{Z} \oplus \mathbf{Z}/3\mathbf{Z}.$$

Then $S(9)^+ \cong \mathbf{Z}/3\mathbf{Z}$, and $S(9)^- \cong \mathbf{Z}/3\mathbf{Z} \oplus \mathbf{Z}/3\mathbf{Z}$ or $\mathbf{Z}/3\mathbf{Z}$, according as $3 \in B$ or $3 \notin B$. When $S(9)^- \cong \mathbf{Z}/3\mathbf{Z} \oplus \mathbf{Z}/3\mathbf{Z}$ (i.e., $3 \in B$), there are four non-conjugate non-Galois cubic fields associated with $S(9)^-$. One of them is the cubic field associated with $S(3)^-$. So there are three non-conjugate non-Galois cubic fields with discriminant $d \cdot 9^2$ when $3 \in B$. If $3 \notin B$, then $S(9)^- \cong \mathbf{Z}/3\mathbf{Z}$, and hence there is a unique (up to conjugacy) non-Galois cubic field with discriminant $d \cdot 9^2$. If $3 \notin B$ and $p \in A_2$, then it can be checked that $S(9p)^- \cong \mathbf{Z}/3\mathbf{Z} \oplus \mathbf{Z}/3\mathbf{Z}$. So there are four nonconjugate non-Galois cubic fields associated with $S(9p)^-$. One of these is associated with $S(3p)^-$ and another with $S(9)^-$. So there are two nonconjugate non-Galois cubic fields with discriminant $d \cdot 9^2 \cdot p^2$ when $3 \notin B$ and $p \in A_2$. For $3 \in B$ and $p \in A_2$, $S(9p)^- \cong \mathbf{Z}/3\mathbf{Z} \oplus \mathbf{Z}/3\mathbf{Z} \cong S(9)^-$. So no new cubic fields occur in this case. The results of this paragraph and Lemma 4 (ii and iv) imply Theorem 2 (c) (vii–xi).

References

1. T. Callahan, *The 3-class groups of non-Galois cubic fields II*, Mathematika, vol. 21 (1974), pp. 168–188.
2. F. Gerth, *Ranks of 3-class groups of non-Galois cubic fields*, Acta Arith., to appear.

3. H. Hasse, *Arithmetische Theorie der kubischen Zahlkörper auf Klassenkörpertheoretischer Grundlage*, Math. Z., vol. 31 (1930), pp. 565–582.
4. C. S. Herz, "Construction of class fields," in *Seminar on complex multiplication*, Lecture Notes in Math., vol. 21, Springer-Verlag, Berlin and New York, 1966.
5. T. Honda, *Pure cubic fields whose class numbers are multiples of three*, J. Number Theory, vol. 3 (1971), pp. 7–12.
6. H. Reichardt, *Arithmetische Theorie der kubischen Körper als Radikalkörper*, Monatshefte Math. Phys., vol. 40 (1933), pp. 323–350.

The University of Texas
Austin, Texas