BULL. AUSTRAL. MATH. SOC. 11R16, 11R29
VOL. 72 (2005) [471–476]

ON 3-CLASS GROUPS OF CERTAIN PURE CUBIC FIELDS

FRANK GERTH III

Recently Calegari and Emerton made a conjecture about the 3-class groups of certain pure cubic fields and their normal closures. This paper proves their conjecture and provides additional insight into the structure of the 3-class groups of pure cubic fields and their normal closures.

1. INTRODUCTION

Let p be a prime number, and let $K = \mathbb{Q}(\sqrt[3]{p})$. Let $M = \mathbb{Q}(\zeta, \sqrt[3]{p}) = \mathbb{Q}(\sqrt{-3}, \sqrt[3]{p})$, where ζ is a primitive cube root of unity. Let S_K be the 3-class group of K (that is, the Sylow 3-subgroup of the ideal class group of K). Let S_M (respectively, $S_{\mathbb{Q}(\zeta)}$) be the 3-class group of M (respectively, $\mathbb{Q}(\zeta)$). Since $\mathbb{Q}(\zeta)$ has class number 1, then $S_{\mathbb{Q}(\zeta)} = \{1\}$.

Assuming $p \equiv 1 \pmod 9$, Calegari and Emerton [**3**, Lemma 5.11] proved that the rank of S_M equals two if 9 divides $|S_K|$, where $|S|$ denotes the order of a finite group S. Based on numerical calculations, they conjecture that the converse is also true. Their conjecture is equivalent to the following theorem that we shall prove.

THEOREM 1. *Assume $p \equiv 1 \pmod 9$, and S_K and S_M are defined as above. If $9 \nmid |S_K|$, then the rank of S_M equals one.*

We shall prove some results about the structure of S_K and S_M for arbitrary pure cubic fields K, and then we shall prove Theorem 1 when $K = \mathbb{Q}(\sqrt[3]{p})$ with $p \equiv 1 \pmod 9$.

2. SOME RESULTS FOR ARBITRARY PURE CUBIC FIELDS

We first consider arbitrary pure cubic fields $K = \mathbb{Q}(\sqrt[3]{n})$ with cube-free integer $n > 1$. Let $M = \mathbb{Q}(\zeta, \sqrt[3]{n})$. Various results about the 3-class groups S_K and S_M appear in [**1, 2, 4, 5**]. So the reader may consult those papers for more details about some of the results we present.

We let σ be a generator of $\mathrm{Gal}(M/K)$, and we let τ be a generator of $\mathrm{Gal}\big(M/\mathbb{Q}(\zeta)\big)$. So $\mathrm{Gal}(M/K) = \langle\sigma\rangle$ is a cyclic group of order 2, and $\mathrm{Gal}\big(M/\mathbb{Q}(\zeta)\big) = \langle\tau\rangle$ is a cyclic group of order 3. Also $\tau\sigma = \sigma\tau^2$ in $\mathrm{Gal}(M/\mathbb{Q}) = \langle\sigma, \tau\rangle$. Using the fact that the 3-class group $S_{\mathbb{Q}(\zeta)} = \{1\}$, we observe that if $a \in S_M$, then $a^{1+\tau+\tau^2} = \mathcal{N}_{M/\mathbb{Q}(\zeta)}a = 1$, where

Received 23rd August, 2005

$\mathcal{N}_{M/\mathbb{Q}(\zeta)} : S_M \to S_{\mathbb{Q}(\zeta)}$ is the norm map on ideal classes. Then S_M may be viewed as a module over $\mathbb{Z}_3[\langle\tau\rangle]/(1+\tau+\tau^2) \cong \mathbb{Z}_3[\zeta]$, where $\mathbb{Z}_3$ is the ring of 3-adic integers. Let

$$S_M^{(1-\tau)^i} = \{a^{(1-\tau)^i} \mid a \in S_M\} \quad \text{for} \quad i = 0, 1, 2, \dots .$$

Since $(1-\zeta)^2 \cdot \mathbb{Z}_3[\zeta] = 3 \cdot \mathbb{Z}_3[\zeta]$, then $S_M^{(1-\tau)^{i+2}} = (S_M^{(1-\tau)^i})^3$ for $i = 0, 1, 2, \dots$. So for the 3-rank of S_M, we have

(1) $$\operatorname{rank} S_M = \operatorname{rank}(S_M/S_M^3) = \operatorname{rank}(S_M/S_M^{1-\tau}) + \operatorname{rank}(S_M^{1-\tau}/S_M^{(1-\tau)^2}) .$$

Next, if $\langle\sigma\rangle$ operates on a finite group S with $2 \nmid |S|$, we let

$$S^+ = \{a \in S \mid a^\sigma = a\} \quad \text{and}$$
$$S^- = \{a \in S \mid a^\sigma = a^{-1}\} .$$

Then with $S = S_M$, it is easy to see that $S_M \cong S_M^+ \times S_M^-$, and $S_M^+ \cong S_K$. If $a \in S_M^{(1-\tau)^i}$, let $a = c^{(1-\tau)^i}$ with $c \in S_M$. Then $a^\sigma = c^{(1-\tau)^i\sigma} = c^{\sigma(1-\tau^2)^i} \in S_M^{(1-\tau)^i}$. Also $(a^{1-\tau})^\sigma = (a^\sigma)^{1-\tau^2} \in S_M^{(1-\tau)^{i+1}}$. So $S_M^{(1-\tau)^i}/S_M^{(1-\tau)^{i+1}}$ is a module over $\mathbb{Z}_3[\langle\sigma\rangle]$ for $i = 0, 1, 2, \dots$. Hence

$$\operatorname{rank}(S_M^{(1-\tau)^i}/S_M^{(1-\tau)^{i+1}}) = \operatorname{rank}(S_M^{(1-\tau)^i}/S_M^{(1-\tau)^{i+1}})^+ + \operatorname{rank}(S_M^{(1-\tau)^i}/S_M^{(1-\tau)^{i+1}})^-$$

for $i = 0, 1, 2, \dots$. We then define surjective maps Δ_i for each i by

$$\Delta_i : S_M^{(1-\tau)^i}/S_M^{(1-\tau)^{i+1}} \longrightarrow S_M^{(1-\tau)^{i+1}}/S_M^{(1-\tau)^{i+2}}$$
$$a \bmod S_M^{(1-\tau)^{i+1}} \longmapsto a^{1-\tau} \bmod S_M^{(1-\tau)^{i+2}}$$

for $a \in S_M^{(1-\tau)^i}$. Let $b \in (S_M^{(1-\tau)^i}/S_M^{(1-\tau)^{i+1}})^+$. Then

$$(b^{1-\tau})^\sigma = (b^\sigma)^{1-\tau^2} = b^{1-\tau^2} = b^{3-(1-\tau)-(1+\tau+\tau^2)} \equiv (b^{1-\tau})^{-1} \bmod S_M^{(1-\tau)^{i+2}} .$$

Similarly, if $b \in (S_M^{(1-\tau)^i}/S_M^{(1-\tau)^{i+1}})^-$, then $(b^{1-\tau})^\sigma \equiv b^{1-\tau} \bmod S_M^{(1-\tau)^{i+2}}$. So Δ_i maps $(S_M^{(1-\tau)^i}/S_M^{(1-\tau)^{i+1}})^+$ onto $(S_M^{(1-\tau)^{i+1}}/S_M^{(1-\tau)^{i+2}})^-$ and maps $(S_M^{(1-\tau)^i}/S_M^{(1-\tau)^{i+1}})^-$ onto $(S_M^{(1-\tau)^{i+1}}/S_M^{(1-\tau)^{i+2}})^+$.

We now recall some results from genus theory. Let $S_M^{(\tau)} = \{a \in S_M \mid a^\tau = a\}$. Then

(2) $$|S_M^{(\tau)}| = 3^{t-2+\delta}$$

where t is the number of ramified primes for the extension $M/\mathbb{Q}(\zeta)$, $\delta = 1$ if $\zeta \in N_{M/\mathbb{Q}(\zeta)}M^\times$, and $\delta = 0$ otherwise. Here $N_{M/\mathbb{Q}(\zeta)} : M^\times \to \mathbb{Q}(\zeta)^\times$ is the norm map. Now from the exact sequence

$$1 \longrightarrow S_M^{(\tau)} \longrightarrow S_M \xrightarrow{1-\tau} S_M \longrightarrow S_M/S_M^{1-\tau} \longrightarrow 1$$

we see that $|S_M/S_M^{1-\tau}| = |S_M^{(\tau)}|$. Furthermore, if M_1 is the maximal Abelian extension of $\mathbb{Q}(\zeta)$ which is unramified over M, then $\mathrm{Gal}(M_1/M) \cong S_M/S_M^{1-\tau}$. By Kummer theory, there is a subgroup B of $M^\times$ with $(M^\times)^3 \subset B \subset M^\times$ such that $M_1 = M(\sqrt[3]{B})$. Let

$$(B/(M^\times)^3)^+ = \{z \in B/(M^\times)^3 \mid z^\sigma = z\} \text{ and}$$
$$(B/(M^\times)^3)^- = \{z \in B/(M^\times)^3 \mid z^\sigma = z^{-1}\}.$$

Then $B/(M^\times)^3 \cong (B/(M^\times)^3)^+ \times (B/(M^\times)^3)^-$. There is a natural pairing

$$\begin{aligned} B/(M^\times)^3 \times S_M/S_M^{1-\tau} &\longrightarrow \langle\zeta\rangle \\ (z, a) &\longmapsto (\sqrt[3]{z})^{a-1} \end{aligned}$$

with $(B/(M^\times)^3)^+$ and $(S_M/S_M^{1-\tau})^-$ dual groups in this pairing, and with $(B/(M^\times)^3)^-$ and $(S_M/S_M^{1-\tau})^+$ dual groups in this pairing. (See [**4**, Proposition 2.4].)

Finally, if h_K (respectively, h_M) is the class number of K (respectively, M), it is known that $h_M = q \cdot h_K^2/3$, where $q = 1$ or 3. (See [**1**, Theorem 12.1 and Theorem 14.1].) In fact, if U_M is the group of units in the ring of integers of M, and if $U_{M,1}$ is the subgroup of U_M generated by the units in the rings of integers of the fields $\mathbb{Q}(\zeta)$, $\mathbb{Q}(\sqrt[3]{n})$, $\mathbb{Q}(\zeta\sqrt[3]{n})$, and $\mathbb{Q}(\zeta^2\sqrt[3]{n})$, then $q = [U_M : U_{M,1}]$. Then we get

$$|S_M| = q \cdot \left(|S_K|\right)^2/3 \quad \text{with} \quad q = 1 \quad \text{or} \quad 3. \tag{3}$$

3. Results for special pure cubic fields

We now suppose $n = p$ with p a prime number. As before, we let $K = \mathbb{Q}(\sqrt[3]{p})$ and $M = \mathbb{Q}(\zeta, \sqrt[3]{p})$. Honda [7] showed that $|S_K| = 1$ (and hence $|S_M| = 1$) if $p = 3$ or if $p \equiv -1 (\mathrm{mod}\ 3)$, and $|S_K| > 1$ (and hence $|S_M| > 1$) if $p \equiv 1 (\mathrm{mod}\ 3)$. Barrucand and Cohn [1] classified K and M into four types. We shall consider various cases depending on the congruence class of p (mod 9). Most of the results in cases 1, 2, and 3 below were previously known, but we include them for the sake of completeness and to illustrate the techniques we are using.

Case 1. $p = 3$ or $p \equiv 8$ (mod 9).

Since only one prime ramifies in $M/\mathbb{Q}(\zeta)$, then in Equation 2, $t = 1$, $\delta = 1$, and $|S_M^{(\tau)}| = 1$. This implies that $|S_M| = 1$, and hence from Equation 3, $q = 3$ and $|S_K| = 1$. Thus the fields K and M are of Type IV in [**1**].

Case 2. $p \equiv 2$ or 5 (mod 9).

The prime ideals $(1 - \zeta)$ and (p) of $\mathbb{Q}(\zeta)$ ramify in M. So $t = 2$ in Equation 2. Since the cubic Hilbert symbol $((\zeta, p)/p) \neq 1$ when $p \equiv 2$ or 5 (mod 9), then $\delta = 0$. So $|S_M^{(\tau)}| = 1$. Hence $|S_M| = 1$, $q = 3$, and $|S_K| = 1$. This implies that the prime ideal above (3) in K is a principal ideal. (Of course, the prime ideal above (p) in K is obviously principal since it is generated by $\sqrt[3]{p}$.) The fields K and M are of Type I in [**1**].

https://doi.org/10.1017/S0004972700035292 Published online by Cambridge University Press

It remains to consider cases when $p \equiv 1$, 4, or 7 (mod 9). In cases 3 and 4 below, we shall see that $|S_M^{(\tau)}| = 3$. Let j be the positive integer such that $S_M^{(\tau)} \subseteq S_M^{(1-\tau)^{j-1}}$ but $S_M^{(\tau)} \not\subseteq S_M^{(1-\tau)^j}$. Then

$$|S_M/S_M^{1-\tau}| = |S_M^{1-\tau}/S_M^{(1-\tau)^2}| = \cdots = |S_M^{(1-\tau)^{j-1}}/S_M^{(1-\tau)^j}| = 3$$

and $|S_M| = 3^j$. From Equation 1, we see that the 3-rank of the ideal class group of M equals one if $j = 1$ and equals two if $j > 1$. Also, since $|S_M/S_M^{1-\tau}| = |S_M^{(\tau)}| = 3$, there is an unramified cyclic extension M_1 of M of degree 3 which is an Abelian extension of $\mathbb{Q}(\zeta)$, and $\mathrm{Gal}(M_1/M) \cong S_M/S_M^{1-\tau}$. Since $p \equiv 1 \pmod 3$, there is a unique cyclic extension F of $\mathbb{Q}$ of degree 3 in which only p ramifies. If $p = \pi\overline{\pi}$ is a prime factorisation of p in the ring of integers of $\mathbb{Q}(\zeta)$, then $F \cdot \mathbb{Q}(\zeta) = \mathbb{Q}(\zeta, \sqrt[3]{\pi\overline{\pi}^2})$, and $M_1 = M(\sqrt[3]{\pi\overline{\pi}^2})$. Since

$$(\pi\overline{\pi}^2)^\sigma = \overline{\pi}\pi^2 \equiv (\pi\overline{\pi}^2)^{-1} \bmod (M^\times)^3$$

then from the duality results in the previous section, we see that $|(S_M/S_M^{1-\tau})^+| = 3$ and $|(S_M/S_M^{1-\tau})^-| = 1$. From our observations about the maps Δ_i in the previous section,

$$|(S_M^{(1-\tau)^i}/S_M^{(1-\tau)^{i+1}})^+| = 3 \quad \text{and} \quad |(S_M^{(1-\tau)^i}/S_M^{(1-\tau)^{i+1}})^-| = 1$$

if i is even and $0 \leqslant i \leqslant j-1$;

$$|(S_M^{(1-\tau)^i}/S_M^{(1-\tau)^{i+1}})^+| = 1 \quad \text{and} \quad |(S_M^{(1-\tau)^i}/S_M^{(1-\tau)^{i+1}})^-| = 3$$

if i is odd and $1 \leqslant i \leqslant j-1$. Then

$$|S_K| = |S_M^+| = 3^{j/2} \quad \text{and} \quad |S_M^-| = 3^{j/2}$$

if j is even, and

$$|S_K| = |S_M^+| = 3^{(j+1)/2} \quad \text{and} \quad |S_M^-| = 3^{(j-1)/2}$$

if j is odd. These results provide additional insight for Equation 3; namely $q = 3$ in Equation 3 if j is even, and $q = 1$ in Equation 3 if j is is odd. Furthermore, j is even if $|(S_M^{(\tau)})^-| = 3$; on the other hand, j is odd if $|S_M^{(\tau)})^+| = 3$.

CASE 3. $p \equiv 4$ or $7 \pmod 9$ (see [**1, 2**]).

The prime ideals $(1-\zeta)$, (π), and $(\overline{\pi})$ of $\mathbb{Q}(\zeta)$ ramify in M. So $t = 3$ in Equation 2. As in case 2, $\delta = 0$. So $|S_M^{(\tau)}| = 3$. In contrast to cases 1 and 2 where q always equals 3, q may be either 1 or 3 in case 3. To see why this is possible, suppose first that 3 is not a cubic residue modulo p. (For example, $p = 7$.) Then the ideal (3) is inert in the cyclic extension F of $\mathbb{Q}$ of degree 3 in which only p ramifies. Thus the unique prime ideal $\wp_3$ above (3) in M is inert in the unramified Abelian extension $F \cdot M$, which by class field theory implies that $\wp_3$ is not a principal ideal. Hence the ideal class of $\wp_3$ generates $S_M^{(\tau)}$ and is not contained in $S_M^{1-\tau}$. Thus $j = 1$, $|S_K| = |S_M| = 3$, and $q = 1$. So K and M are of Type III in [1] with the ideal $\wp\overline{\wp}^2$ a principal ideal, where $\wp$ (respectively, $\overline{\wp}$) is the prime ideal of M above (π), (respectively, $(\overline{\pi})$).

On the other hand, if $p = 61$, then the class numbers $h_K = 6$ and $h_M = 36$. So $|S_K| = 3$ and $|S_M| = 9$. Thus $q = 3$ and $j = 2$. In this case the prime ideal $N_{M/K}\wp_3$ is principal, and the ideal $\wp\overline{\wp}^2$ generates $(S_M^{(\tau)})^-$. Note $S_M^{(\tau)} = (S_M^{(\tau)})^-$, and K and M are of Type I in [1]. For this example with $p = 61$, 3 is a cubic residue modulo 61. (However, I do not know whether 3 being a cubic residue modulo a prime p with $p \equiv 4$ or $7 \pmod 9$ is sufficient to guarantee that $q = 3$.) This example with $p = 61$ does show that Theorem 1 cannot be extended to all primes $p \equiv 1 \pmod 3$ since $9 \nmid |S_K|$ but $\operatorname{rank} S_M = 2$.

CASE 4. $p \equiv 1 \pmod 9$.

The prime ideals (π) and $(\overline{\pi})$ of $\mathbb{Q}(\zeta)$ ramify in M. So $t = 2$ in Equation 2. Since $p \equiv 1 \pmod 9$, the cubic Hilbert symbols $\big((\zeta, p)/\pi\big) = \big((\zeta, p)/\overline{\pi}\big) = 1$, and hence $\delta = 1$. So $|S_M^{(\tau)}| = 3$.

Let $\wp$ and $\overline{\wp}$ be the prime ideals of M above (π) and $(\overline{\pi})$, respectively. Note that $\wp\overline{\wp} = (\sqrt[3]{p})$, a principal ideal. If $\wp$ is not a principal ideal, then $\overline{\wp}$ is not a principal ideal, and the ideal class of $\wp\overline{\wp}^2$ generates $S_M^{(\tau)}$. So if that happens, $|S_M^{(\tau)})^-| = 3$ and $|S_M^{(\tau)})^+| = 1$. If $\wp$ is a principal ideal, then $\overline{\wp}$ is also a principal ideal, and hence a generator of $S_M^{(\tau)}$ does not contain a ramified prime of the extension $M/\mathbb{Q}(\zeta)$. (In the terminology of [1, 4], there exist ambiguous classes which are not strong ambiguous, which occurs when $\zeta \notin N_{M/\mathbb{Q}(\zeta)}U_M$ even though $\zeta \in N_{M/\mathbb{Q}(\zeta)}M^\times$.)

We first focus on the case where $\wp$ is principal. From part (1) of [6, Proposition 2], we know that a generator of $S_M^{(\tau)}$ comes from S_M^+. So $\big|(S_M^{(\tau)})^+\big| = 3$ and $\big|(S_M^{(\tau)})^-\big| = 1$. In the discussion preceding case 3, we see that j is odd and $q = 1$. If $j = 1$, then $|S_K| = |S_M^+| = 3$ and $|S_M| = 3$, and hence $\operatorname{rank} S_M = 1$. If $j \geqslant 3$, then 9 divides $|S_M^+| = |S_K|$, and $\operatorname{rank} S_M = 2$. So Theorem 1 is true if $\wp$ is principal. We remark that the fields K and M are of Type III in [1]. An example where this paragraph applies is when $p = 19$.

It remains to consider the situation where $\wp$ is not principal. Because $\big|(S_M^{(\tau)})^-\big| = 3$ when $\wp$ is not principal, we see that j is even and $q = 3$. (The fields K and M would be of Type IV in [1].) Now in Theorem 1, we assume $9 \nmid |S_K|$. Hence $j = 2$. If $j = 2$ were possible, Theorem 1 would be false. So we must show that $j = 2$ is impossible. Let F be the cyclic cubic extension of $\mathbb{Q}$ in which only p ramifies, and let $L = F \cdot \mathbb{Q}(\zeta)$. Let U_L be the group of units in the ring of integers of L, and let $U_{L,1}$ be the subgroup of U_L generated by the units in the rings of integers of F and $\mathbb{Q}(\zeta)$. By [8, Theorem 4.12], $[U_L : U_{L,1}] = 1$ or 2. Since $N_{L/\mathbb{Q}(\zeta)}U_{L,1} = \{\pm 1\}$, then $\zeta \notin N_{L/\mathbb{Q}(\zeta)}U_{L,1}$, and since $[U_L : U_{L,1}] = 1$ or 2, then $\zeta \notin N_{L/\mathbb{Q}(\zeta)}U_L$. However, $\zeta \in N_{L/\mathbb{Q}(\zeta)}L^\times$ since $p \equiv 1 \pmod 9$. Now from genus theory $|S_L^{(\omega)}| = 3$, where ω is a generator of $\operatorname{Gal}\big(L/\mathbb{Q}(\zeta)\big)$, S_L is the 3-class group of L, and $S_L^{(\omega)} = \{a \in S_L \mid a^\omega = a\}$. Since $\zeta \notin N_{L/\mathbb{Q}(\zeta)}U_L$ but $\zeta \in N_{L/\mathbb{Q}(\zeta)}L^\times$, a generator of $S_L^{(\omega)}$ does not contain a ramified prime of the extension $L/\mathbb{Q}(\zeta)$. This means that $\mathcal{P}$

and $\overline{\mathcal{P}}$ are principal ideals, where $\mathcal{P}$ and $\overline{\mathcal{P}}$ are the prime ideals of L above (π) and $(\overline{\pi})$, respectively.

Now assuming $j = 2$, the Hilbert 3-class field of M is an extension M' of M of degree 9, which is a Galois extension of $\mathbb{Q}(\zeta)$ and contains the field L. Then M'/L is a Galois extension of degree 9 which is unramified at all primes. Because $|\mathrm{Gal}(M'/L)| = 9$, then $\mathrm{Gal}(M'/L)$ is Abelian. So M' is contained in the Hilbert 3-class field of L. Since $\mathcal{P}$ and $\overline{\mathcal{P}}$ are principal ideals of L, they must split completely in M'/L. But then $\wp$ and $\overline{\wp}$ split completely in M'/M, which is impossible since M' is the Hilbert 3-class field of M, and $\wp$ and $\overline{\wp}$ are not principal ideals of M. Hence we have a contradiction, which means that $j = 2$ cannot happen. So the proof of Theorem 1 is complete.

References

[1] P. Barrucand and H. Cohn, 'Remarks on principal factors in a relative cubic field', *J. Number Theory* **3** (1971), 226–239.

[2] P. Barrucand, H. Williams and L. Baniuk, 'A computational technique for determining the class number of a pure cubic field', *Math. Comp.* **30** (1976), 312–323.

[3] F. Calegari and M. Emerton, 'On the ramification of Hecke algebras at Eisenstein primes', *Invent. Math.* **160** (2005), 97–144.

[4] F. Gerth, 'On 3-class groups of pure cubic fields', *J. Reine Angew. Math.* **278/279** (1975), 52–62.

[5] F. Gerth, 'Ranks of 3-class groups of non-Galois cubic fields', *Acta Arith.* **30** (1976), 307–322.

[6] G. Gras, 'Sur les ℓ-classes d'idéaux des extensions non galoisiennes de $\mathbb{Q}$ de degré premier impair ℓ a clôture galoisienne diédrale de degré 2ℓ', *J. Math. Soc. Japan* **26** (1974), 677–685.

[7] T. Honda, 'Pure cubic fields whose class numbers are multiples of three', *J. Number Theory* **3** (1971), 7–12.

[8] L. Washington, *Introduction to cyclotonic fields* (Springer-Verlag, New York, 1982).

Mathematics Department
The University of Texas at Austin
1 University Station C1200
Austin, TX 78712-0257
United States of America
e-mail: gerth@math.utexas.edu