OCTAHEDRAL EXTENSIONS WITH A COMMON CUBIC SUBFIELD

KEVIN CHILDERS AND DARRIN DOUD

Abstract. Consider a cubic extension $K/F$ of number fields with Galois closure of degree 6, and a finite set $\mathcal{P}$ of primes of $F$ containing the primes at which $K/F$ ramifies. We prove that the collection of $S_4$-extensions of $F$ containing $K$ and unramified outside $\mathcal{P}$, together with the Galois closure of $K/F$ forms a finite elementary abelian 2-group. For the case $F = \mathbb{Q}$ we prove that this group is nontrivial if $K$ is totally real and ramified only at one prime $p \equiv 1 \pmod{4}$. This proves a conjecture of Wong.

1. Introduction

In [11] Siman Wong studies octahedral extensions of $\mathbb{Q}$ (i.e. extensions with Galois group $S_4$, the symmetry group of the octahedron) and states the following conjecture.

Theorem 1.1. [11, Conjecture 1] Let $K/\mathbb{Q}$ be a non-Galois cubic extension such that $|d_K|$ is a prime power. Then the number of $S_4$-extensions $L/\mathbb{Q}$ containing $K$ and having $|d_L|$ a prime power is $2^n - 1$ for some integer $n$. Furthermore, if $K$ is totally real, then $n > 0$.

In this paper we will prove Wong’s conjecture.

We prove the conjecture in two parts. In Section 2, for an arbitrary non-Galois cubic extension $K/F$ that is unramified outside a set $\mathcal{P}$ of primes of $F$, we describe a group structure on the set of all $S_4$-extensions of $F$ containing $K$ and unramified outside $\mathcal{P}$, together with the Galois closure of $K$ (which will act as the identity element). The resulting group is a finite elementary abelian two-group, and we obtain the following theorem.

Theorem 1.2. Let $L$ be a number field and let $\mathcal{P}$ be a set of primes of $F$. Let $K/F$ be a non-Galois cubic extension unramified outside $\mathcal{P}$. Then the number of $S_4$-extensions $L/F$ containing $K$ and unramified outside $\mathcal{P}$ is $2^n - 1$ for some non-negative integer $n$.

We note that the group operation we use is similar to that described using Galois cohomology in [5, Section 3.1] although [5] does not restrict the ramification, and hence does not obtain a finite group. A simple modification of the construction of [5] could be used to give an alternative proof of Theorem 1.2.

With the exception of the last assertion, Theorem 1.1 is a special case of Theorem 1.2, in which $F = \mathbb{Q}$ and $\mathcal{P} = \{p, \infty\}$. In Section 3 we prove this last assertion
by explicitly constructing a quadratic extension of the cubic field \( K \) that is unramified outside \( \{ p, \infty \} \) and has Galois group \( S_4 \), so that the group used to prove Theorem 1.2 is nontrivial.

2. A GROUP STRUCTURE ON \( S_4 \)-EXTENSIONS

2.1. Group cohomology calculations. The symmetric group \( S_4 \) is an extension of \( S_3 \) by the Klein 4-group \( V \), with the elements of \( S_3 \) acting as permutations on the three non-identity elements of \( V \).

Lemma 2.1. Let \( S_3 \) act on the Klein four group \( V \) by permuting the non-identity elements. Then

\[ H^2(S_3, V) = 0. \]

Proof. Applying the Hochschild-Serre spectral sequence [10, p. 195] to the exact sequence

\[ 1 \to A_3 \to S_3 \to \mathbb{Z}/2\mathbb{Z} \to 0, \]

we obtain a convergent spectral sequence:

\[ E_2^{pq} = H^p(\mathbb{Z}/2\mathbb{Z}, H^q(A_3, V)) \Rightarrow H^{p+q}(S_3, V). \]

Since \( |A_3| \) is relatively prime to \( |V| \), each \( H^q(A_3, V) \) with \( q > 0 \) is trivial [10, Proposition 6.1.10]. Direct calculation gives that \( H^0(A_3, V) \) is trivial. Hence, the spectral sequence collapses, and the cohomology is trivial. \( \square \)

Theorem 2.2. Let \( L \) and \( L' \) be two distinct \( S_4 \)-extensions of a number field \( F \) containing a common cubic subfield \( K \). Then the composite field \( LL' \) has \( \text{Gal}(LL'/F) \cong G \), where \( G \) is the semidirect product of \( S_3 \) and \( V \oplus V \), with \( V \) considered as an \( S_3 \)-module as above.

Proof. Denote by \( I \) the Galois closure of \( K/F \). Then \( I \) is an \( S_3 \)-extension of \( F \) contained in both \( L \) and \( L' \). Each of \( L \) and \( L' \) is a \( V \)-extension of \( I \), with \( S_3 \) acting on \( V \) by permuting the non-identity elements. Hence, the composite \( LL' \) is a \( V \oplus V \) extension of \( I \). We thus have an exact sequence

\[ 0 \to V \oplus V \to \text{Gal}(LL'/F) \to S_3 \to 1. \]

By Lemma 2.1,

\[ H^2(S_3, V \oplus V) \cong H^2(S_3, V) \oplus H^2(S_3, V) = 0, \]

so the sequence splits, and \( \text{Gal}(LL'/F) \cong (V \oplus V) \rtimes S_3 \) as desired. \( \square \)

From this result we see that \( \text{Gal}(LL') \) is always isomorphic to the same group of order 96. For the remainder of the paper, we call this group \( G \). The group \( G \) can be identified in Magma [1] as \texttt{SmallGroup(96,227)}.

In order to more conveniently describe certain subgroups of \( G \), we will make the following definition.

Definition 2.3. Let \( L/F \) be an \( S_4 \)-extension containing the cubic subextension \( K/F \). Then \( \text{Gal}(L/F) \) contains a single non-normal subgroup \( W \) isomorphic to the Klein four-group and fixing \( K \). We denote the fixed field of \( W \) by \( W_K(L) \) and note that it is a quadratic extension of \( K \).
Given two $S_4$-extensions $L/F$ and $L'/F$ with a common cubic subextension $K/F$, we identify several subgroups of $G \cong \text{Gal}(LL'/F)$. According to Magma [1] the group $G$ has exactly three normal subgroups of order 4, which we will denote $H_1$, $H_2$, and $H_3$. Each quotient $G/H_i$ is isomorphic to $S_4$. Without loss of generality we let $H_1$ correspond (under the Galois correspondence) with $L$, and $H_2$ correspond with $L'$. Then $H_3$ corresponds to a third $S_4$-extension of $F$, which we will denote $L''$.

We will denote by $A$ the subgroup of order 32 of $G$ having fixed field $K$. Computations in Magma [1] verify that each $H_i$ is contained in $A$. Hence, each of $L$, $L'$, and $L''$ contains $K$.

The group $G$ contains three subgroups $N_1, N_2, N_3 \subset A$ of order 16 corresponding to the three fields $L_6 = W_K(L)$, $L_6' = W_K(L')$, and $L_6'' = W_K(L'')$. We note (again by computations in Magma) that the composite $L_6L_6'$ is a Klein four-extension of $K$, and the third quadratic subextension in $L_6L_6'/K$ is the field that we have denoted $L_6''$. We see easily that the Galois closure of $L_6''$ must be $L''$.

Note that since all fields discussed here lie inside $ML'$, if $L/F$ and $L'/F$ are unramified outside a set $\mathcal{P}$ of primes of $F$, then so are $L''$, $L_6$, $L_6'$, and $L_6''$.

This discussion of subgroups of $G$ and subfields of $ML'/F$ is summarized by the lattices in Figure 1 (which correspond under the Galois correspondence). We remark that these lattices are incomplete; they do not include all subgroups/subfields, but only the ones in which we are interested.

These calculations prove the following theorem.

**Theorem 2.4.** Let $F$ be a number field, let $\mathcal{P}$ be a set of primes of $F$, and let $L$ and $L'$ be $S_4$-extensions of $F$ unramified outside $\mathcal{P}$ with a common cubic subfield $K$. Then the composite $LL'/F$ contains exactly three $S_4$-extensions of $F$: $L$, $L'$, and a third field which we denote $L''$. Furthermore, $L''/F$ is unramified outside $\mathcal{P}$.
Let $L_6 = W_K(L)$ and let $L_6' = W_K(L')$. Then the composite $L_6L_6'$ contains a unique third quadratic extension of $K$, which we denote $L_6''$.

Finally, $L_6'' = W_K(L'')$ and the Galois closure of $L_6''$ over $F$ is $L''$.

2.2. The group operation. Let $F$ be a number field, $\mathcal{P}$ a set of primes of $F$, and $K/F$ a non-Galois cubic extension unramified outside $\mathcal{P}$. We will now describe the group operation $*$ on the set

$$S = \{S_4\text{-extensions of } F\text{ containing } K\text{ and unramified outside } \mathcal{P}\} \cup \{I\}.$$  

**Definition 2.5.** The operation $* : S \times S \to S$ is defined as follows.

1. $I$ acts trivially: $I * L = L = L * I$ for all $L \in S$.
2. For all $L \in S - \{I\}$, $L * L = I$.
3. If $L$ and $L'$ are distinct elements of $S - \{I\}$, then $L * L'$ is defined as the field $L''$ from Theorem 2.4 (i.e. the third $S_4$-extension of $K$ contained in $LL'$).

By Theorem 2.4, this operation is well defined. Clearly, the operation is commutative, has an identity, and every element is its own inverse. In order to prove that it is a group operation, it remains only to prove associativity.

**Proposition 2.6.** The binary operation $*$ makes $S$ into an abelian group.

**Proof.** We will prove associativity for $(S, *)$ in 4 cases.

**Case 1:** One of the fields is $I$. We have

$$(I * L) * L' = L * L' = I * (L * L').$$

Since $*$ is commutative, this proves associativity.

**Case 2:** A field is repeated. Let $L$ and $L'$ be the two fields in question, and define $L''$ as in Theorem 2.4. We have

$$(L * L) * L' = I * L' = L' = L * L'' = L * (I * L').$$

Using commutativity, associativity follows in this case.

**Case 3:** The three fields are distinct, non-identity, and lie in the same degree 96 extension. In this case, we may call the fields $L$, $L'$, and $L''$ (as in Theorem 2.4). Then

$$(L * L') * L'' = L'' * L'' = I = L * L = L * (L' * L'').$$

**Case 4:** The three fields are distinct, non-identity, and do not lie in a single degree 96 extension. Call them $L_1$, $L_2$, and $L_3$. Each $W_K(L_i)$ is a quadratic extension of $K$, so we can write each $W_K(L_i) = K(\sqrt{\alpha_i})$ for some element $\alpha_i \in K$. One checks easily (using Theorem 2.4) that $W_K(L_1 * L_3) = K(\sqrt{\alpha_1 \alpha_3})$ and that

$$W_K((L_1 * L_2) * L_3) = K(\sqrt{\alpha_1 \alpha_2 \alpha_3}) = W_K(L_1 * (L_2 * L_3)).$$

Then both $L_1 * (L_2 * L_3)$ and $(L_1 * L_2) * L_3$ are the Galois closure of $K(\sqrt{\alpha_1 \alpha_2 \alpha_3})$, so they must be equal.

$\square$

2.3. Proof of Theorem 1.2. The proof of Theorem 1.2 now follows easily.

**Proof of Theorem 1.2.** By [8, p. 122], $S$ is finite. Hence, $S$ is a finite abelian group of exponent 2, so it has order $2^n$ for some $n$. Therefore the number of $S_4$-extensions of $F$ containing $K$ and unramified outside $\mathcal{P}$ is $2^n - 1$. $\square$
2.4. Examples of Theorem 1.2. We now give several examples illustrating Theorem 1.2 with various sets \( \mathcal{P} \). All of our examples have base field \( F = \mathbb{Q} \), and all polynomials in these examples were obtained from Jones’ number field tables [7].

Example 2.7. We consider the case where \( \mathcal{P} = \{23, \infty\} \). Jones’ tables indicate that there is (up to isomorphism) a single cubic field \( K \) unramified outside \( \mathcal{P} = \{23, \infty\} \), with defining polynomial \( x^3 - x^2 + 1 \). However, Jones’ tables indicate that there are no \( S_4 \)-extensions of \( \mathbb{Q} \) unramified outside \( \mathcal{P} \). In this case the group defined in Definition 2.5 is trivial, containing only \( I \), and the value of \( n \) in Theorem 1.2 is 0. Since \( 23 \not\equiv 1 \pmod{4} \), this is not a counterexample to Theorem 1.1.

Example 2.8. In contrast, for \( \mathcal{P} = \{6571, \infty\} \) there is again a single cubic field \( K \) unramified outside \( \mathcal{P} \) (with defining polynomial \( x^3 - x^2 - 9x - 16 \)), but this time Jones’ tables indicate that there are seven \( S_4 \)-extensions of \( \mathbb{Q} \) unramified outside \( \mathcal{P} \), each of which must contain \( K \), so that the group defined in Definition 2.5 has order eight. Defining quartic polynomials for these extensions are

\[
\begin{align*}
x^4 - 6571x - 45997, & \quad x^4 - x^3 - 2x^2 + 4x + 1, \\
x^4 + 4x^2 - 5x + 1, & \quad x^4 - x^3 - 821x^2 + 20945x - 85500, \\
x^4 - 2x^2 - 3x + 2, & \quad x^4 - x^3 - 821x^2 - 11910x - 59216, \\
x^4 - x^3 - 821x^2 + 7803x - 26361. & 
\end{align*}
\]

Example 2.9. For \( \mathcal{P} = \{2, 3, 5, \infty\} \) there are many examples of non-Galois cubic extensions \( K/\mathbb{Q} \) unramified outside \( \mathcal{P} \). One is defined by \( x^3 - 18x - 12 \). Jones’ tables list 143 extensions of \( \mathbb{Q} \) with Galois group \( S_4 \) unramified outside \( \mathcal{P} \), and computing in GP/PARI [9] we find that exactly fifteen of them contain \( K \). Hence, the group described in Definition 2.5 has order 16.

3. Cubic fields ramified only at \( p \equiv 1 \pmod{4} \)

Throughout this section we will denote by \( K \) a totally real cubic extension of \( \mathbb{Q} \) with Galois group \( S_3 \) ramified only at one prime \( p > 3 \). By [2, Lemma 2.4] this is equivalent to saying that \( K \) is a cubic field with Galois group \( S_3 \) that is ramified only at one prime \( p \equiv 1 \pmod{4} \). Since \( K/\mathbb{Q} \) must be tamely ramified, we see that \( d_K \) must equal \( p \).

In the case that the narrow class number of \( K \) is even, Heilbronn [6] has shown that \( K \) is contained in an \( S_4 \)-extension \( L/\mathbb{Q} \) defined by a quartic polynomial whose root field has the same discriminant as \( K \). The absolute value of the discriminant of \( L/\mathbb{Q} \) will then be a power of \( p \). We wish to prove a similar theorem in the case that the narrow class number of \( K \) is odd; namely, that there is an \( S_4 \)-extension \( L/\mathbb{Q} \) with \( |d_L| \) equal to a power of \( p \).

The key to our proof is the following theorem.

Theorem 3.1. [4, Lemma 5.32] Let \( L = K(\sqrt[4]{u}) \) be a quadratic extension with \( u \in \mathcal{O}_K \), and let \( p \) be a prime in \( \mathcal{O}_K \).

1. If \( 2u \not\equiv p \pmod{p} \), then \( p \) is unramified in \( L \).
2. If \( 2p \not\equiv 0 \pmod{p} \) and \( u = b^2 - 4c \) for some \( b, c \in \mathcal{O}_K \), then \( p \) is unramified in \( L \).

The fact that the unit group of \( K \) is of rank 2 (since \( K \) is a totally real cubic field) will give us a large number of units modulo squares. This will enable us to construct non-square elements \( u \) of \( K \) for which adjoining the square root of \( u \) will give a quadratic extensions unramified outside \( \{p, \infty\} \). We will then show that the
Proof. The set $H$ consists of the squares modulo 4. Since each of the $q$ squares is in one of the $q$ cosets of $H$, we see that $H$ contains exactly one of the $q$ squares in each coset. Therefore, $H$ is a subgroup of order $q$.

Theorem 3.2. Let $K/\mathbb{Q}$ be a cubic extension, and let $q$ be a prime of $K$ lying over 2 and let $f$ be the inertial degree of $q$ over 2. Then

$$(\mathcal{O}_K/q^2)^\times \cong \begin{cases} 
\mathbb{Z}/2\mathbb{Z} & \text{if } f = 1, \\
\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/6\mathbb{Z} & \text{if } f = 2, \\
\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/14\mathbb{Z} & \text{if } f = 3.
\end{cases}$$

Proof. There is an exact sequence

$$0 \to (\mathcal{O}_K/q)^+ \to (\mathcal{O}_K/q^2)^\times \to (\mathcal{O}_K/q)^\times \to 1$$

where the first map takes $\alpha + q$ to $1 + \alpha \pi + q^2$ (where $\pi$ is any element of $\mathcal{O}_K$ with $v_\pi(\pi) = 1$), and the second map takes $\alpha + q^2$ to $\alpha + q$.

Since the group $(\mathcal{O}_K/q)^+$ is isomorphic to $(\mathbb{Z}/2\mathbb{Z})^f$, the group $(\mathcal{O}_K/q)^\times$ is cyclic of order $2^f - 1$, and the orders of the two groups are relatively prime, we see that the sequence splits and the theorem follows.

Corollary 3.3. Let $K/\mathbb{Q}$ be a non-Galois cubic extension in which 2 is unramified, and let $f$ be the inertial degree of any prime over 2 in the Galois closure of $K/\mathbb{Q}$. Then

$$(\mathcal{O}_K/4\mathcal{O}_K)^\times \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/(2q)\mathbb{Z}$$

where we define $q = 2^f - 1$.

Proof. This follows from Theorem 3.2, the Chinese Remainder Theorem, and the factorization of $2\mathcal{O}_K$ into prime ideals.

Corollary 3.3 shows that $(\mathcal{O}_K/4\mathcal{O}_K)^\times$ must have a unique subgroup of order 8 consisting of elements of order dividing 2. In addition, we see that the elements of order dividing 2 are precisely the $q$th powers in $(\mathcal{O}_K/4\mathcal{O}_K)^\times$.

We now investigate the units modulo 4.

Theorem 3.4. Let $K/\mathbb{Q}$ be a totally real non-Galois cubic extension with narrow class group of odd order, and let $q$ be defined as above. Let $\{u_1, u_2\}$ be a system of fundamental units for $\mathcal{O}_K$. Let $S = \{\pm 1, \pm u_1^2, \pm u_2^2, \pm (u_1u_2)^9\}$. Then the elements of $S$ have distinct images in $(\mathcal{O}_K/4\mathcal{O}_K)^\times$. 

Proof. If two distinct elements in the set were congruent modulo 4, then their quotient would be a non-square unit congruent to 1 modulo 4. Call this quotient $v$. Then by Theorem 3.1, $K(\sqrt{v})$ would be a quadratic extension of $K$ that is unramified at all finite primes. Such an extension cannot exist since the narrow class number of $K$ is odd.

Corollary 3.5. Let $H$ be the set of images of the elements of $S$ in $(\mathcal{O}_K/4\mathcal{O}_K)^\times$. Then $H$ is a subgroup of order 8 in $(\mathcal{O}_K/4\mathcal{O}_K)^\times$, and a complete set of coset representatives for $H$ consists of the set of squares of elements in $(\mathcal{O}_K/4\mathcal{O}_K)^\times$.

Proof. The set $H$ consists of eight distinct $q$th powers in $(\mathcal{O}_K/4\mathcal{O}_K)^\times$, which form a subgroup. The subgroup $H$ contains only one of the squares in $(\mathcal{O}_K/4\mathcal{O}_K)^\times$, so each of the $q$ squares is in one of the $q$ cosets of $H$. □
Now that we have a good understanding of the structure of \((\mathcal{O}_K/4\mathcal{O}_K)^\times\) and how the units fit inside it, we are prepared to construct a quadratic extension of \(K\).

**Theorem 3.6.** Let \(K/\mathbb{Q}\) be a totally real non-Galois cubic extension, ramified only at one prime \(p > 3\). Assume that the narrow class number \(h\) of \(K\) is odd. Let \(p\mathcal{O}_K = p_1p_2\) be the factorization of \(p\mathcal{O}_K\) into prime ideals of \(\mathcal{O}_K\). Then there is a quadratic extension of \(K\) in which the only finite prime that ramifies is \(p_2\).

**Proof.** Let \(h\) be the narrow class number of \(K\). Then \(p_2^h\) is principal, say \(p_2^h = \pi\mathcal{O}_K\) for some \(\pi \in \mathcal{O}_K\). Let \(S = \{\pm 1, \pm u_1^q, \pm u_2^q, \pm (u_1u_2)^q\}\). Then \(\pi S\) contains an element \(v\) which is a square modulo 4 (since the image of \(\pi S\) in \((\mathcal{O}_K/4\mathcal{O}_K)^\times\) is a coset of \(H\), and contains a square by Corollary 3.5). Note that \(v\) itself cannot be a square in \(\mathcal{O}_K\), since it is a generator of an odd power of \(p_2\). Because the only prime containing \(v\) is \(p_2\) and \(v\) is a square modulo \(4\mathcal{O}_K\), Theorem 3.1 shows that \(K(\sqrt{v})/K\) is unramified at all finite primes except possibly \(p_2\). Since \(K\) has no quadratic extensions unramified at all finite primes (because its narrow class number is odd), \(K(\sqrt{v})/K\) must ramify at \(p_2\). \(\square\)

**Theorem 3.7.** Let \(K(\sqrt{v})/K\) be the extension constructed in Theorem 3.6. Then the Galois group of the Galois closure of \(K(\sqrt{v})/\mathbb{Q}\) is isomorphic to \(S_4\).

**Proof.** Let \(K_6 = K(\sqrt{v})\) be the degree six field constructed above. We note that (since \(p_2\) ramifies in \(K_6/K\)) the Galois closure of \(K_6/\mathbb{Q}\) must have Galois group of order divisible by 4. In particular, \(K_6\) cannot be an \(S_3\)-extension of \(\mathbb{Q}\). Now \(K_6\) has the cubic subfield \(K\); by [3, p. 325] we see that the Galois group of the Galois closure of \(K_6\) must be one of

\[
C_6, \quad S_3, \quad D_6, \quad A_4, \quad S_4, \quad A_4 \times C_2, \quad S_4 \times C_2.
\]

Since \(K\) has Galois group \(S_3\) and the splitting field of \(K_6\) properly contains the splitting field of \(K\), we can rule out \(C_6, S_3, A_4,\) and \(A_4 \times C_2\). Since only one prime is ramified in \(K_6\) (and that prime is odd), its splitting field cannot contain two quadratic subfields, ruling out \(D_6\) and \(S_4 \times C_2\). Hence, the Galois group must be \(S_4\), as desired. \(\square\)

Note that [3] lists \(S_4\) twice as a possible Galois group for a sextic field with a cubic subfield, once with an embedding into \(A_6\) (positive sign), and once with an embedding into \(S_6\) that contains odd elements (negative sign). By examining the inertia group at \(p\), one can show that the field that we have constructed is a fixed field inside its Galois closure of a cyclic subgroup of order 4 in \(S_4\). Hence, it corresponds to the negative sign in the classification of [3].

**Corollary 3.8.** Let \(K/\mathbb{Q}\) be a non-Galois cubic extension with discriminant a power of \(p \equiv 1 \pmod{4}\). Then \(K\) is contained in an \(S_4\)-extension \(L/\mathbb{Q}\), and \(|d_L|\) is a power of \(p\).

**Proof.** Since \(p\) is tamely ramified in \(K/\mathbb{Q}\), we see that \(d_K = p\). Since \(p \equiv 1 \pmod{4}\), \(K\) must be totally real [2, Lemma 2.4]. If the narrow class group of \(K\) has even order, [6] shows that \(K\) is contained in an \(S_4\)-extension \(L/\mathbb{Q}\) with discriminant a power of \(p\). If the narrow class group of \(K\) has odd order, Theorems 3.6 and 3.7 yield the same conclusion. \(\square\)
Corollary 3.8 completes the proof of Theorem 1.1 by proving the existence of an $S_4$-extension of $\mathbb{Q}$ containing $K$ and unramified outside \{p, \infty\}. This proves that the value of $2^n - 1$ in the theorem is at least one, so that $n > 0$.

References