OCTAHEDRAL EXTENSIONS WITH A GIVEN CUBIC SUBFIELD

KEVIN CHILDERS AND DARRIN DOUD

ABSTRACT. Let $K/\mathbb{Q}$ be a non-Galois cubic extension with $|d_k|$ a power of a prime p. We prove a conjecture of Wong, namely that the number of S_4-extensions of $\mathbb{Q}$ containing K and having discriminant a power of p is of the form $2^n - 1$ for some nonnegative $n \in \mathbb{Z}$, and that n is positive if K is totally real.

1. INTRODUCTION

In [8] 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. [8, Conjecture 1] *Let $K/\mathbb{Q}$ be a non-Galois cubic extension such that the discriminant $|d_K|$ 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 we will show that a standard application of Kummer theory yields the following theorem.

Theorem 1.2. *Let F be a number field and let $\mathcal{P}$ be a finite 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 containing K and unramified outside $\mathcal{P}$ is $2^n - 1$ for some non-negative integer n.*

With the exception of its last assertion, Theorem 1.1 is a special case of Theorem 1.2, in which $F = \mathbb{Q}$ and $\mathcal{P} = \{p, \infty\}$. The main contribution of this paper is the proof in section 3 of this last assertion. The proof proceeds 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 value of n in Theorem 1.2 is nonzero.

2. COUNTING S_4-EXTENSIONS

We thank an anonymous reviewer for suggestions that significantly shortened the proof of Theorem 1.2.

Proof of Theorem 1.2: Let K/F be any non-Galois cubic extension of number fields, $\mathcal{P}$ a finite set of primes of F containing all primes which ramify in K. By [5, Section

Date: September 1, 2015.
2010 *Mathematics Subject Classification.* 11R21, 11R32.
Key words and phrases. Octahedral extension, group structure.

3.1] (see also [3, Theorem 2.2]), there is a bijection between the set of S_4-extensions of F containing K and the nonidentity elements of the abelian group

$$S = \ker(N_{K/F} : K^*/(K^*)^2 \to F^*/(F^*)^2)$$

of exponent 2. Under this correspondence, a nonidentity element of S represented by $\alpha \in K^*$ is associated with the Galois closure of $K(\sqrt{\alpha})/F$, which has Galois group S_4.

If we denote by L_α and L_β the S_4-extensions of F corresponding to elements of S represented by $\alpha, \beta \in K^*$, we see easily that the ramified primes of $L_{\alpha\beta}$ are contained inside the union of the sets of ramified primes of L_α and L_β (since $L_{\alpha\beta}$ is contained in the compositum $L_\alpha L_\beta$). Hence, the set of S_4-extensions of F containing K and unramified outside $\mathcal{P}$ is in bijection with the nonidentity elements of a subgroup of S. Since this set must be finite [7, p. 122], we see that its size must be of the form $2^n - 1$ for some n. This proves Theorem 1.2. □

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 [1, 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 the discriminant d_K of 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 $L/\mathbb{Q}$ containing K 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 $L = K(\sqrt{u})$ be a quadratic extension with $u \in \mathfrak{O}_K$, and let $\mathfrak{p}$ be a prime in $\mathfrak{O}_K$.*

1. *If $2u \notin \mathfrak{p}$, then $\mathfrak{p}$ is unramified in L.*
2. *If $2 \in \mathfrak{p}$, $u \notin \mathfrak{p}$, and $u = b^2 - 4c$ for some $b, c \in \mathfrak{O}_K$, then $\mathfrak{p}$ 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 extension of K unramified outside $\{p, \infty\}$. We will then show that the extension that we construct has the correct Galois group. In order to use condition (2) of Theorem 3.1 we will first need to understand the structure of $(\mathfrak{O}_K/4\mathfrak{O}_K)^\times$, since the u in which we are interested will be squares modulo 4 that are relatively prime to 2.

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

$$(\mathfrak{O}_K/\mathfrak{q}^2)^\times \cong (\mathbb{Z}/2\mathbb{Z})^f \times \mathbb{Z}/(2^f - 1)\mathbb{Z}.$$

Proof. By [4, p. 142], there is an exact sequence

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

Since the group $(\mathfrak{O}_K/\mathfrak{q})^+$ is isomorphic to $(\mathbb{Z}/2\mathbb{Z})^f$, the group $(\mathfrak{O}_K/\mathfrak{q})^\times$ is cyclic of order 2^f-1, and the orders of the two groups are relatively prime, 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, setting $q=2^f-1$, we have*

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

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

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

We now investigate the units modulo 4.

Proposition 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 in Corollary 3.3. Let $\{u_1,u_2\}$ be a system of fundamental units for $\mathfrak{O}_K$. Let $S=\{\pm1,\pm u_1^q,\pm u_2^q,\pm(u_1u_2)^q\}$. Then the elements of S have distinct images in $(\mathfrak{O}_K/4\mathfrak{O}_K)^\times$.*

Proof. If two distinct elements in the set were congruent modulo 4, then their quotient v would be a non-square unit congruent to 1 modulo 4. 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 $(\mathfrak{O}_K/4\mathfrak{O}_K)^\times$. Then H is a subgroup of order 8 in $(\mathfrak{O}_K/4\mathfrak{O}_K)^\times$, and a complete set of coset representatives for H consists of the set of squares of elements in $(\mathfrak{O}_K/4\mathfrak{O}_K)^\times$.*

Proof. The set H consists of eight distinct qth powers in $(\mathfrak{O}_K/4\mathfrak{O}_K)^\times$, which form a subgroup. The subgroup H contains only one of the squares in $(\mathfrak{O}_K/4\mathfrak{O}_K)^\times$, so each of the q squares is in one of the q cosets of H. □

We are now 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 $p\mathfrak{O}_K=\mathfrak{p}_1\mathfrak{p}_2^2$ be the factorization of $p\mathfrak{O}_K$ into prime ideals of $\mathfrak{O}_K$. Then there is a quadratic extension of K in which the only finite prime that ramifies is $\mathfrak{p}_2$.*

Proof. Let h be the narrow class number of K. Then $\mathfrak{p}_2^h$ is principal, say $\mathfrak{p}_2^h=\pi\mathfrak{O}_K$ for some $\pi\in\mathfrak{O}_K$. Let $S=\{\pm1,\pm u_1^q,\pm u_2^q,\pm(u_1u_2)^q\}$. Then πS contains an element v which is a square modulo 4 (since the image of πS in $(\mathfrak{O}_K/4\mathfrak{O}_K)^\times$ is a coset of H, and contains a square by Corollary 3.5). Note that v itself cannot be a square in $\mathfrak{O}_K$, since it is a generator of an odd power of $\mathfrak{p}_2$. Because the only prime containing v is $\mathfrak{p}_2$ and v is a square modulo $4\mathfrak{O}_K$, Theorem 3.1 shows that $K(\sqrt{v})/K$ is unramified at all finite primes except possibly $\mathfrak{p}_2$. 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 $\mathfrak{p}_2$. □

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. Since $\mathfrak{p}_2$ 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 [2, 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. □

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 [1, 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 combine to yield the same conclusion. □

Corollary 3.8 completes the proof of the final assertion 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, for totally real K ramified at only one prime, the value of $2^n - 1$ in Theorem 1.1 is at least one, so that $n > 0$.

References

[1] Kevin Childers and Darrin Doud. Proof of a conjecture of Wong concerning octahedral Galois representations of prime power conductor. *J. of Number Theory*, 154:101–104, 2015.

[2] Henri Cohen. *A course in computational algebraic number theory*, volume 138 of *Graduate Texts in Mathematics*. Springer-Verlag, Berlin, 1993.

[3] Henri Cohen and Frank Thorne. Dirichlet series associated to quartic fields with given resolvent. *Research in Number Theory*, to appear. arXiv:1302.5728v1.

[4] David A. Cox. *Primes of the form $x^2 + ny^2$*. Pure and Applied Mathematics (Hoboken). John Wiley & Sons, Inc., Hoboken, NJ, second edition, 2013.

[5] J. E. Cremona. Classical invariants and 2-descent on elliptic curves. *J. Symbolic Comput.*, 31(1-2):71–87, 2001. Computational algebra and number theory (Milwaukee, WI, 1996).

[6] H. Heilbronn. On the 2-classgroup of cubic fields. In *Studies in Pure Mathematics (Presented to Richard Rado)*, pages 117–119. Academic Press, London, 1971.

[7] Serge Lang. *Algebraic number theory*, volume 110 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, second edition, 1994.

[8] Siman Wong. Arithmetic of octahedral sextics. *J. Number Theory*, 145:245–272, 2014.

University of Utah, Department of Mathematics, Salt Lake City, UT 84112
E-mail address: kevinrchilders@gmail.com

Brigham Young University, Department of Mathematics, Provo, UT 84602
E-mail address: doud@math.byu.edu