STRONG INHOMOGENEITY OF ESCHENBURG SPACES

KRISHNAN SHANKAR*

Abstract. In this paper we investigate the strong inhomogeneity of the seven dimensional Eschenburg manifolds. We show that roughly two thirds of this infinite family is strongly inhomogeneous. Among the remaining Eschenburg spaces we exhibit the first known examples of simply connected, positively curved manifolds that are homotopy equivalent but not homeomorphic to each other.

Introduction

In this paper we investigate the topology of the Eschenburg spaces in some detail. This is carried out in order to determine how inhomogeneous these spaces are topologically. Using the idea of the biquotient construction in [?], J.-H. Eschenburg constructed, in 1982, an infinite family of 7-manifolds admitting positive sectional curvature (cf. [?]) and in a sequel, another example in dimension six (cf. [?]); see Section 1 for construction and notation.

We point out two subclasses of the Eschenburg spaces of interest to us. The first of these is the subclass of the Aloff–Wallach spaces. These are obtained by setting $\bar{a} = (0,0,0)$ and are usually denoted as $N_{p,q} := M_{(0,0,0),(p,q,-p-q)}$, where $\gcd(p,q) = 1$. These spaces admit homogeneous metrics of positive sectional curvature (cf. [?]) with the exception of the space $N_{1,-1}$. The Aloff–Wallach spaces were also investigated by M. Kreck and S. Stolz (cf. [?], [?]); they found examples of (positively curved) Aloff–Wallach spaces that are homeomorphic, but not diffeomorphic to each other. Every one of these spaces fibers over the homogeneous flag manifold, $F = \mathrm{SU}(3)/\mathrm{T}^2$. The other subclass is given by $\bar{a} = (1,1,k)$, $\bar{b} = (0,0,k+2)$, where k is any integer. It is shown in [?] that this is precisely the class of Eschenburg spaces that admits a cohomogeneity one metric i.e., the orbit space of the action of the isometry group of the Eschenburg metric is an interval. Note that the cohomogeneity one metric on these spaces (with one exception) has positive sectional curvature.

1991 *Mathematics Subject Classification.* 53C20, 53C30, 57N65.

Key words and phrases. Strong inhomogeneity, Eschenburg spaces, homotopy types.

* Partially supported by an NSF grant.

A topological space is said to be *strongly inhomogeneous* if it is not homotopy equivalent to any compact homogeneous space G/H, where G is a compact Lie group and H is a closed subgroup.

The motivation comes from studying Riemannian manifolds that admit a metric of positive sectional curvature. The Eschenburg spaces are metrically inhomogeneous since the homogeneous examples have been classified (see [**?**], [**?**], [**?**], [**?**]), but one may ask: Do they admit a transitive group action or are they topologically inhomogeneous as well? Eschenburg himself gave a partial answer; see Theorem 3.2. In this paper we shall give a more complete answer by using homotopy invariants computed independently by J. Milgram and B. Krüggel (cf. [**?**], [**?**]).

Theorem 1. *The Eschenburg space $M^7_{\bar{a},\bar{b}}$ is strongly inhomogeneous if it satisfies one of the following conditions:*

(i) $\Sigma := \Sigma a_i = \Sigma b_i \not\equiv 0 \pmod 3$.
(ii) If $n = |H^4(M^7_{\bar{a},\bar{b}}, \mathbf{Z})|$, then $3^2 \mid n$ or there is a prime $p \mid n$ such that $p \equiv 2 \pmod 3$.

Turning to the class of cohomogeneity one Eschenburg spaces, a simple application of Theorem 1 yields the following corollary.

Corollary 2. *Let $M_k := M_{(1,1,k),(0,0,k+2)}$ represent a cohomogeneity one Eschenburg space. If k is congruent to 0 or 2 mod(3), then M_k is strongly inhomogeneous. If $k \equiv 1 \pmod 3$, then with the exception of the cases $k = 1$ and $k = -2$, M_k is never homeomorphic to any homogeneous space.*

The manifolds M_1 and M_{-2} in the corollary above are both diffeomorphic to the Aloff–Wallach space $N_{1,1}$. The above corollary is a critical step in the computation of the isometry groups of the cohomogeneity one Eschenburg spaces in [**?**].

Another simple application of Theorem 1 and Corollary 2 is to produce examples of inhomogeneous Einstein manifolds. In their papers [**?**] and [**?**], the authors show among the cohomogeneity one Eschenburg spaces, the families M_{3d+1} and M_{3d} both contain infinitely many strongly inhomogeneous Einstein manifolds (see [**?**, Proposition 5.2]). We can improve their result by using Corollary 2. Note that the Einstein metrics constructed in [**?**] and [**?**] are not isometric to the Eschenburg metrics.

Corollary 3. *Let M_k be a cohomogeneity one Eschenburg space equipped with a 3-Sasakian structure as in [**?**]. If k is congruent to 0 or 2 mod(3), then M_k is a strongly inhomogeneous Einstein manifold. If $k \equiv 1 \pmod 3$, then with the exception of the cases $k = 1$ and $k = -2$, M_k is an Einstein manifold not homeomorphic to any homogeneous space.*

One may well ask about the case when both conditions in Theorem 1 above are negated? Obviously there are Eschenburg spaces that are *not* strongly inhomogeneous namely, the Aloff–Wallach spaces, but we can do a little better.

Theorem 4. *Under the conditions* $\Sigma = \Sigma a_i = \Sigma b_i \equiv 0 \pmod 3$ *and* $n = 3^t p_1^{t_1} \cdot p_2^{t_2} \cdots p_l^{t_l}$ *where* $t \leq 1$ *and* $p_i \equiv 1 \pmod 3$ *for all* i*, there exist Eschenburg spaces* $M^7_{\bar{a},\bar{b}}$ *with* $H^4(M, \mathbf{Z}) = \mathbf{Z}_n$ *homotopy equivalent to some Aloff–Wallach space, but not homeomorphic to any homogeneous space (see Table 1).*

For instance, the spaces $M_{(4,10,-14),(13,17,-30)}$ and $M_{(0,0,0),(9,17,-26)}$ are homotopy equivalent, but not homeomorphic to each other. Note that either space admits a metric of positive sectional curvature. These are the first known examples of:

Corollary 5. *There exist simply connected, positively curved manifolds that are homotopy equivalent, but not homeomorphic to each other.*

Without the assumption of simple connectedness, the lens spaces provide examples of such a phenomenon. For instance $L(7,1)$ and $L(7,2)$ are homotopy equivalent, but not homeomorphic to each other (see for instance Theorem 10.14 in [**?**]).

Acknowledgments. I would like to thank Karsten Grove for his generous support during the academic year ′96–′97, and for many illuminating discussions. I would also like to thank N. Kitchloo and B. Krüggel for clarifying many topological questions and J. Wyss-Gallifent for programming assistance.

1. Preliminaries

Given a compact Lie group G, let U be a subgroup of $G \times G$. Consider the following two sided action of U on G:

$$U \times G \to G$$
$$(u_1, u_2) \cdot g \to u_1, \cdot g \cdot u_2^{-1}$$

If this action is free, then the resulting quotient space, denoted as $G//U$, is called a double coset space or a biquotient. Note that when U lies strictly in one component of $G \times G$, then the quotient is simply a homogeneous space. The following class of manifolds will be focus of this paper.

Eschenburg spaces. Let $\bar{a} := (a_1, a_2, a_3)$, $\bar{b} := (b_1, b_2, b_3)$ be triples of integers such that $\sum a_i = \sum b_i$. Let

$$S^1_{\bar{a},\bar{b}} = \left\{ \left(\begin{pmatrix} z^{a_1} & & \\ & z^{a_2} & \\ & & z^{a_3} \end{pmatrix}, \begin{pmatrix} z^{b_1} & & \\ & z^{b_2} & \\ & & z^{b_3} \end{pmatrix} \right) : z \in \mathrm{U}(1) \right\}$$

Then $S^1_{\bar{a},\bar{b}}$ acts on SU(3) by a two sided action. The action is free if and only if g.c.d.$(a_1 - b_{\sigma(1)}, a_2 - b_{\sigma(2)}, a_3 - b_{\sigma(3)}) = 1$ for every permutation $\sigma \in \mathrm{S}_3$. When the action is free, we will call the resulting 7-manifold, $M_{\bar{a},\bar{b}} := \mathrm{SU}(3)//S^1_{\bar{a},\bar{b}}$, an *Eschenburg space*. In his paper [**?**], Eschenburg considered normal homogeneous metrics on SU(3) that are right invariant with respect to U(2). Under these conditions, he showed that $M_{\bar{a},\bar{b}}$ has positive sectional curvature if and only if $b_i \notin [a_{\min}, a_{\max}]$ (or $a_i \notin [b_{\min}, b_{\max}]$ if the invariance of the metric is switched) for all i.

The cohomology of these spaces is well known; see [**?**], [**?**].

$$\begin{aligned} H^2(M_{\bar{a},\bar{b}}, \mathbf{Z}) &= \langle u \rangle \cong \mathbf{Z}, \\ H^4(M_{\bar{a},\bar{b}}, \mathbf{Z}) &= \langle u^2 \rangle \cong \mathbf{Z}/(\sigma_2(\bar{a}) - \sigma_2(\bar{b})) \quad \text{(torsion)}, \\ H^5(M_{\bar{a},\bar{b}}, \mathbf{Z}) &= \langle v \rangle \cong \mathbf{Z}, \\ H^7(M_{\bar{a},\bar{b}}, \mathbf{Z}) &= \langle uv \rangle \cong \mathbf{Z}. \end{aligned}$$

2. The homotopy invariants

In this section we will review the construction of part of the homotopy invariants in [**?**]. Although that paper includes calculation of PL-homeomorphism invariants (up to a possible $\mathbf{Z}_2$ indeterminacy), we shall only be concerned with homotopy invariants in this paper. Moreover, we remain consistent with the notation and conventions of [**?**]. We regard SU(3) as $V_{2,1}$, the Stiefel manifold of 2-frames in $\mathbb{C}^3$ i.e., as pairs of vectors

$$\begin{pmatrix} v_1 & w_1 \\ v_2 & w_2 \\ v_3 & w_3 \end{pmatrix}$$

where $\bar{v} \cdot \bar{w} = 0$, $\|\bar{v}\|^2 = \|\bar{w}\|^2 = 1$. Given four integers p_1, p_2, p_3, p_4 satisfying the constraint $p_1 \equiv p_2 \equiv p_3 \equiv p_4 \pmod 3$, we define an S^1- action on $V_{2,1}$ as follows.

$$z \cdot \begin{pmatrix} v_1 & w_1 \\ v_2 & w_2 \\ v_3 & w_3 \end{pmatrix} = \begin{pmatrix} z^{\frac{p_1 - p_3}{3}} v_1 & z^{\frac{p_1 - p_4}{3}} w_1 \\ z^{\frac{p_2 - p_3}{3}} v_2 & z^{\frac{p_2 - p_4}{3}} w_2 \\ z^{\frac{-(p_1 + p_2 + p_3)}{3}} v_3 & z^{\frac{-(p_1 + p_2 + p_4)}{3}} w_3 \end{pmatrix}$$

where $z \in S^1$. The resulting quotient space is denoted as $M^7(p_1, p_2, p_3, p_4)$ and is an Eschenburg space. We now introduce two assumptions on the set (p_1, p_2, p_3, p_4) for this section.

(2.1). The gcd of the four integers (p_1, p_2, p_3, p_4) is either 1 or 3. This is equivalent to assuming that the circle, S^1 we picked embeds in a torus of $\mathrm{SU}(3) \times \mathrm{SU}(3)$.

(2.2). The intersection of the sets $\{p_1, p_2, -(p_1+p_2)\}$ and $\{p_3, p_4, -(p_3+p_4)\}$ contains at most one element.

The invariant r.

Consider a fibration $V_{2,1} \to E \to B$ with structure group $\mathrm{SU}(3) * \mathrm{SU}(3)$, where $\mathrm{SU}(3) * \mathrm{SU}(3) = \mathrm{SU}(3) \times_{\mathbf{Z}_3} \mathrm{SU}(3)$. All cohomology is understood to be in $\mathbb{F}_3$ coefficients unless otherwise stated.

Consider the universal case:

$$V_{2,1} \longrightarrow B_{\mathrm{PSU}(3)} \xrightarrow{Bi} B_{\mathrm{SU}(3)*\mathrm{SU}(3)} \longrightarrow M(Bi)$$

where $i : \mathrm{PSU}(3) \hookrightarrow \mathrm{SU}(3) * \mathrm{SU}(3) \cong \mathrm{SU}(3) \rtimes \mathrm{PSU}(3)$ and $M(Bi)$ is the mapping cone of the map Bi.

The cohomology of $B_{\mathrm{SU}(3)*\mathrm{SU}(3)}$ with $\mathbb{F}_3$ coefficients has the following structure (see Remark 7.5 in [**?**]).

$$\begin{aligned} &H^2 = \langle i_2 \rangle, \\ &H^3 = \langle \beta i_2 \rangle, \quad \text{where } \beta \text{ is the Bockstein,} \\ &H^4 \neq 0 \quad \text{i.e., there exists } 0 \neq w_4 \in H^4. \end{aligned}$$

The map $(Bi)^* : H^*(B_{\mathrm{SU}(3)*\mathrm{SU}(3)}) \to H^*(B_{\mathrm{PSU}(3)})$ has the following properties:

$$(Bi)^*(i_2) \neq 0, \qquad (Bi)^*(\beta i_2) \neq 0, \qquad (Bi)^*(w_4) = 0.$$

Now consider the cofiber sequence,

$$B_{\mathrm{PSU}(3)} \xrightarrow{Bi} B_{\mathrm{SU}(3)*\mathrm{SU}(3)} \longrightarrow M(Bi).$$

The long exact sequence in cohomology splits into short exact pieces and we get

$$0 \longrightarrow H^i(M(Bi)) \longrightarrow H^i(B_{\mathrm{SU}(3)*\mathrm{SU}(3)}) \xrightarrow{(Bi)^*} H^i(B_{\mathrm{PSU}(3)}) \longrightarrow 0$$

which implies $H^*(M(Bi)) = \ker(Bi)^*$. Also there exists $u_4 \in H^4(M(Bi))$ such that $i_2 u_4 \in H^6(M(Bi))$. Note that $i_2 \notin H^2(M(Bi))$.

Now let $V_{2,1} \to E \to B$ be any fibration with structure group $\mathrm{SU}(3) * \mathrm{SU}(3)$. Then it can be written as a pullback:

$$\begin{array}{ccc}
V_{2,1} & = & V_{2,1} \\
\downarrow & & \downarrow \\
E & \longrightarrow & B_{\mathrm{PSU}(3)} \\
{\scriptstyle f}\downarrow & & \downarrow \\
B & \longrightarrow & B_{\mathrm{SU}(3)*\mathrm{SU}(3)} \\
\downarrow & & \downarrow \\
M(f) & \xrightarrow[g]{} & M(Bi)
\end{array}$$

When E in the fibration above is homotopy equivalent to an Eschenburg space i.e., $E = E_{S^1} \times_{S^1} \mathrm{SU}(3)$, we have $H^6(M(f)) = \langle u \rangle \cong \mathbb{F}_3$ and $B = B_{S^1} = \mathbb{CP}^\infty$. Let $r \in \mathbb{F}_3$ be defined by the equation

$$ru = g^*(i_2 u_4)$$

The following result now follows; see Section 7 in [**?**].

Proposition 2.1 (Milgram)**.** *If X and X' are Eschenburg spaces that are homotopy equivalent, then $r(X) = \pm r(X')$ in $\mathbb{F}_3$.*

The result implies that r is an invariant in the oriented category. The indeterminacy comes from the fact that there is no canonical choice for the generator of $H^2(X, \mathbf{Z})$. If we don't care about orientation preserving homotopy equivalences, then we need only check r up to sign.

The correspondence.

We now provide the correspondence between Milgram's description and the more familiar description of Eschenburg spaces as $\mathrm{SU}(3)//S^1$. An element of $V_{2,1}$ can be thought of as an element in $\mathrm{SU}(3)$ by 'completing' the matrix:

$$\begin{pmatrix} v_1 & w_1 \\ v_2 & w_2 \\ v_3 & w_3 \end{pmatrix} \leftrightarrow \begin{pmatrix} v_1 & w_1 & x_1 \\ v_2 & w_2 & x_2 \\ v_3 & w_3 & x_3 \end{pmatrix}$$

where the vector $(x_1, x_2, x_3) \in \mathbb{C}^3$ is the unique unit vector that is orthogonal to the other two and makes the determinant of the resulting matrix equal to 1. If the space $M^7(p_1, p_2, p_3, p_4)$ corresponds to the Eschenburg space $M^7_{\bar{a},\bar{b}}$, then equating the S^1 action on SU(3), we have for $z \in S^1$,

$$\begin{pmatrix} z^{\frac{p_1-p_3}{3}} v_1 & z^{\frac{p_1-p_4}{3}} w_1 \\ z^{\frac{p_2-p_3}{3}} v_2 & z^{\frac{p_2-p_4}{3}} w_2 \\ z^{\frac{-(p_1+p_2+p_3)}{3}} v_3 & z^{\frac{-(p_1+p_2+p_4)}{3}} w_3 \end{pmatrix} = \begin{pmatrix} z^{a_1-b_1} v_1 & z^{a_1-b_2} w_1 & z^{a_1-b_3} x_1 \\ z^{a_2-b_1} v_2 & z^{a_2-b_2} w_2 & z^{a_2-b_3} x_2 \\ z^{a_3-b_1} v_3 & z^{a_3-b_2} w_3 & z^{a_3-b_3} x_3 \end{pmatrix}$$

which yields the following set of equations:

$$\begin{aligned} p_1 - p_3 &= 3(a_1 - b_1), \qquad & p_1 - p_4 &= 3(a_1 - b_2), \\ p_2 - p_3 &= 3(a_2 - b_1), \qquad & p_2 - p_4 &= 3(a_2 - b_2), \\ p_1 + p_2 + p_3 &= -3(a_3 - b_1), \qquad & p_1 + p_2 + p_4 &= -3(a_3 - b_2). \end{aligned}$$

Solving these equations we get,

$$p_1 = 3a_1 - \Sigma, \quad p_2 = 3a_2 - \Sigma, \quad p_3 = 3b_1 - \Sigma, \quad p_4 = 3b_2 - \Sigma,$$

where $\Sigma = \sum a_i = \sum b_i$. From [**?**], we see that the homotopy invariant r is equal to $p_1 \pmod 3$ and we have for the Eschenburg space $M^7_{\bar{a},\bar{b}}$,

Proposition 2.2. $r(M^7_{\bar{a},\bar{b}}) = -\Sigma \pmod 3$ *is a homotopy invariant.*

3. Homogeneous spaces with similar homotopy.

In his paper [**?**], Eschenburg showed the following result, although not explicitly stated as such. In this section, $M^7 = M^7_{\bar{a},\bar{b}}$ will denote an Eschenburg space i.e., an S^1-biquotient of SU(3).

Proposition 3.1 (Eschenburg)**.** *If M^7 is homotopy equivalent to a compact Riemannian homogeneous space, N^7, then N^7 must be an Aloff–Wallach space.*

The proof of this theorem relies on the observation that the homotopy groups of Eschenburg spaces put restriction on the pairs (G, H) such that G/H is homotopy equivalent to an Eschenburg space. Furthermore, since G/H must be a compact, orientable manifold, we must have $\dim(G/H) = 7$, and hence $H \subset O(7)$. A careful enumeration and study of the finitely many pairs then yields the result. Using this Eschenburg was able to show the next result.

Theorem 3.2 (Eschenburg)**.** *For the Eschenburg space with $H^4(M^7, \mathbf{Z}) = \mathbf{Z}_n$, if $n \equiv 2 \pmod 3$, then M^7 is strongly inhomogeneous.*

This is now a simple application of Proposition 3.1 once we note that for an Aloff–Wallach space $H^4(N_{p,q}, \mathbf{Z}) = \mathbf{Z}/(p^2 + q^2 + pq)$ and the quadratic form $p^2 + q^2 + pq$ is never congruent to 2 modulo 3.

We are now in a position to improve on this considerably. Given an Eschenburg space M^7, we have the homotopy invariant $r(M^7)$. From Proposition 2.2 this is easily computed: For the biquotient $M^7 = M^7_{\bar{a},\bar{b}}$, we have $r(M^7) \equiv \sum a_i \pmod 3 \equiv \sum b_i \pmod 3$. For an Aloff–Wallach space $N_{p,q}$, it is clear that $r(N_{p,q}) \equiv 0 \pmod 3$. Putting this together along with the theorem above yields, for any Eschenburg space,

Proposition 3.3. *If $\sum a_i = \sum b_i \not\equiv 0 \pmod 3$, then M^7 is strongly inhomogeneous.*

This shows that in a rough sense, two thirds of the Eschenburg spaces are strongly inhomogeneous. We now proceed to generalize the congruence conditions of Theorem 3.2.

A little number theory.

For an Eschenburg space M^7 with $H^4(M^7, \mathbf{Z}) = \mathbf{Z}_n$ to be homotopy equivalent to an Aloff–Wallach space $N_{p,q}$, it is at least necessary that $n = |H^4(N_{p,q}, \mathbf{Z})| = p^2 + q^2 + pq$. Recall that p and q are relatively prime. Let $\zeta = e^{\frac{2\pi i}{3}}$ be a primitive cube root of unity. Then in the ring $\mathbf{Z}[\zeta]$ we have the factorization $p^2 + q^2 + pq = (p - q\zeta)(p - q\zeta^2)$. We are interested in knowing when the integer n is properly representable by the quadratic form p^2+q^2+pq. Here properly means that $\gcd(p,q) = 1$. The following theorem indicates when this is possible. The case $n = 1$ yields just one solution (up to equivalence), so we may assume that $n > 1$.

Proposition 3.4. *A positive integer n is properly representable by the quadratic form $p^2 + q^2 + pq$ if and only if the following conditions hold:*

(i) If $3^t \mid n$, then $t \leq 1$ and
(ii) If r is a prime dividing n, then $r \equiv 1 \pmod 3$.

Moreover, given any n as above the number of distinct proper representations of n by the quadratic form is 2^{m-1} where m is the number of distinct prime factors of n congruent to $1 \pmod 3$.

Proof. A positive integer n is properly representable by some quadratic form of discriminant d if and only if d is a quadratic residue modulo $4n$; see for instance [**?**, Chapter VI]. Note that p^2+q^2+pq is the unique quadratic form of discriminant -3.

If -3 is a quadratic residue modulo $4n$, then it is a quadratic residue modulo n and hence a quadratic residue modulo r for any prime r that divides n. The prime $r = 3$ is allowed, but if $9 \mid n$, then -3 is a quadratic residue modulo 9 which is patently untrue. Hence, if 3^t divides n, then $t \leq 1$. Now suppose $r > 3$ is any prime dividing n (note that n is necessarily odd). By quadratic reciprocity -3 is a quadratic residue modulo r if and only if r is a quadratic residue modulo 3 which is equivalent to saying $r \equiv 1 \pmod 3$.

Conversely, suppose $n = 3^t \cdot r_1 \cdot r_2 \cdots r_m$ is a positive integer, where $t \leq 1$ and $r_i \equiv 1 \pmod 3$. Every integer prime congruent to 1 modulo 3 splits in $\mathbf{Z}[\zeta]$ (only the integer primes congruent to 2 modulo 3 remain prime in $\mathbf{Z}[\zeta]$). This implies that every prime dividing n can be properly represented by the quadratic form i.e., $3 = (1-\zeta)(1-\zeta^2)$ and we may write $r_i = p_i^2 + q_i^2 + p_i q_i = (p_i - q_i\zeta)(p_i - q_i\zeta^2) =: \mathfrak{r}_i\bar{\mathfrak{r}}_i$. We now have a factorization of n in $\mathbf{Z}[\zeta]$,

$$n = ((1-\zeta)(1-\zeta^2))^t \prod_{i=1}^{m}(p_i - q_i\zeta)(p_i - q_i\zeta^2) = ((-\zeta^2)(1-\zeta)^2)^t \prod_{i=1}^{m} \mathfrak{r}_i\bar{\mathfrak{r}}_i.$$

Since $\mathbf{Z}[\zeta]$ is a PID, showing that n is properly representable by the quadratic form is equivalent to finding $\alpha \in \mathbf{Z}[\zeta]$ such that $\alpha\bar{\alpha} = n$ and $\alpha \notin \mathbf{Z}$. Note that multiplication by the six units in $\mathbf{Z}[\zeta]$ yields six 'equivalent' solutions. Equating these solutions is the same as saying that we only care about the ideal (α). From each prime factor r_i, choose either $\mathfrak{r}_i$ or $\bar{\mathfrak{r}}_i$ and multiply these out along with $(1-\zeta)$ (discard this factor if $3 \nmid n$). After multiplying, this will yield a factorization of n into $\alpha = (p - q\zeta)$ and $\bar{\alpha} = (p - q\zeta^2)$, whence p and q are the desired solutions. By unique factorization of prime ideals in $\mathbf{Z}[\zeta]$, this is the only way to get p and q. It is now a simple exercise to show that the number of distinct solutions is 2^{m-1} if n has m distinct prime factors congruent to 1 modulo 3. □

The six equivalent solutions discussed above reflect the fact that the circle action corresponding to (p,q) yields $N_{p,q}$ which is diffeomorphic to any of the spaces $N_{-p,-q}$, $N_{p,-p-q}$, $N_{q,-p-q}$, $N_{-p,p+q}$, $N_{-q,p+q}$.

Some examples.

We now proceed to prove Theorem 4. Given the space $M = M_{\bar{a},\bar{b}}$ with $\Sigma\bar{a} = \Sigma\bar{b} = 0$ and $H^4(M_{\bar{a},\bar{b}}, \mathbf{Z}) = \mathbf{Z}_n$, we define:

$$\begin{aligned} s(M) &:= s(M_{\bar{a},\bar{b}}) = \sigma_3(\bar{a}) - \sigma_3(\bar{b}), \\ q(\bar{a}) &:= -\frac{1}{2}\sigma_2(\bar{a})(\sigma_2(\bar{a}) + 1), \\ q(M) &:= q(\bar{a}) + q(\bar{b}) \pmod 2, \end{aligned}$$

where σ_i are the elementary symmetric functions. B. Krüggel showed in [**?**] that $\{s(M) \in (\mathbf{Z}_n)^*/\{\pm 1\}, q(M), |H^4(M,\mathbf{Z})|\}$ is a complete set of homotopy invariants within the class of Eschenburg spaces. The invariant $s(M)$ is determined up to sign since it is an invariant in the oriented category like the invariant $r(M)$ computed earlier. Hence if $s(M) = \pm s(M')$, then all things being equal, M and M' are homotopy equivalent possibly by an orientation reversing map.

$M = M_{\bar{a},\bar{b}}$	$\lvert H^4(M, \mathbf{Z})\rvert$	$s(M)$	$q(M)$	$p_1(M)$
$M_{(2,8,-10),(6,7,-13)}$	43	42	0	19
$M_{(0,0,0),(1,6,-7)}$	43	1	0	0
$M_{(4,10,-14),(3,13,-16)}$	61	3	1	42
$M_{(0,0,0),(4,5,-9)}$	61	3	1	0
$M_{(4,10,-14),(5,13,-18)}$	103	95	0	36
$M_{(0,0,0),(2,9,-11)}$	103	8	0	0
$M_{(4,10,-14),(13,17,-30)}$	523	317	0	303
$M_{(0,0,0),(9,17,-26)}$	523	206	0	0
$M_{(6,12,-18),(41,60,-101)}$	7489	27	1	4465
$M_{(0,0,0),(3,85,-88)}$	7489	27	1	0

TABLE 1. Some examples.

To find Eschenburg spaces homotopy equivalent to some Aloff–Wallach space, the strategy is to find a pair with the same H^4 and then check whether their homotopy invariants matched up. A computer program written on *Mathematica* helped perform the search. The results were then checked by hand. From the table we see that the spaces listed pairwise are homotopy equivalent, where the second space listed is an Aloff–Wallach space. Moreover, the first integral Pontrjagin class for an Eschenburg space is given by (cf. [**?**])

$$p_1 = (2\sigma_1(\bar{a})^2 - 6\sigma_2(\bar{a}))u^2,$$

where $H^2(M^7, \mathbf{Z}) = \langle u \rangle \cong \mathbf{Z}$. Since the first integral Pontrjagin class, $p_1(M) \in H^4(M, \mathbf{Z})$, is a homeomorphism invariant (this result is due to Kirby and Siebenmann; see for instance [**?**]), the spaces listed in Table 1 are pairwise not homeomorphic. Each of the spaces in the last two pairs admits a metric of positive sectional curvature (see Section 1). These are the first known examples of simply connected, positively curved manifolds that are homotopy equivalent but not homeomorphic to each other.

Cohomogeneity one Eschenburg spaces.

Recall that in [**?**], it is shown that the cohomogeneity one Eschenburg spaces are parameterized as $M_k := M_{(1,1,k),(0,0,k+2)}$. If k is congruent to 0 or 2 mod(3), then M_k is strongly inhomogeneous by Proposition 3.3. If

$k = 3d+1$, then $|H^4(M_{3d+1}, \mathbf{Z})| = 6d+3$ (cf. [**?**]). Note that by proposition 3.4, infinitely many of the family M_{3d+1} are strongly inhomogeneous. Using the formula above, we see that p_1 for the Aloff–Wallach spaces is trivial and for the spaces M_{3d+1}, $p_1 = 3(d+2) \cdot u^2$. This is trivial in precisely four cases: $d = \pm 1$, $d = 0$, $d = 2$. In the cases $d = 1$, $d = -2$, we have $|H^4| = 9$ and hence these spaces must be strongly inhomogeneous by Theorem 1. The cases $d = 0$ and $d = -1$ both yield the Aloff–Wallach space $N_{1,1}$. Hence, minus these two exceptions, the cohomogeneity one Eschenburg spaces are never homeomorphic to any homogeneous space.

Principal Eschenburg spaces.

These are the Eschenburg spaces that fiber as principal S^1-bundles over the inhomogeneous Eschenburg flag, F' (cf. [**?**]). They can be described as $M_{k,l} := M_{(k,l,k+l),(0,0,2(k+l))}$ with $|H^4(M_{k,l})| = k^2 + l^2 + 3kl$. By Proposition 3.3, $M_{k,l}$ is strongly inhomogeneous whenever $k + l \not\equiv 0 \pmod 3$. Moreover, it is shown in [**?**] that any Eschenburg space is stably parallelizable if and only if its first Pontrjagin class is trivial. They also show that a principal Eschenburg space $M_{k,l}$ is stably parallelizable if and only if $H^4(M_{k,l}, \mathbf{Z}) = 0$ (see [**?**, Appendix]). Hence, a principal Eschenburg space can never be homeomorphic to any homogeneous space unless $H^4(M_{k,l}, \mathbf{Z}) = 0$. This last observation is also proved in [**?**] (Theorem 4.2).

Also in the same paper [**?**], the authors look for examples $E_{k,l}$, $E_{k',l'}$, among the principal Eschenburg spaces that are homeomorphic but not diffeomorphic and such that $kl, k'l' > 0$. This is of interest since $E_{k,l}$ admits positive curvature if $kl > 0$. They note that a computer search for such pairs fails to yield examples for $N \leq 100,000$ where $N = |H^4| = k^2 + l^2 + 3kl$. We want to point out that such pairs are never homeomorphic.

Consider the Kreck-Stolz invariant $s_1(E_{k,l}) \in \mathbf{Q}/\mathbf{Z}$ given by

$$s_1 = \frac{k+l}{2^5 \cdot 3 \cdot 7 \cdot N}(N(2k^2 + kl + 2m^2) - 16N - 48) - \frac{1}{2^5 \cdot 7}\operatorname{sign}(W)$$

where $\partial W = E_{k,l}$ and $\operatorname{sign}(W) = -2$ if $N, k, l > 0$ (we may assume without loss of generality that k, l are both positive). In [**?**] the authors show that if $E_{k,l}$ is homeomorphic to $E_{k',l'}$, then $28s_1(E_{k,l}) = 28s_1(E_{k',l'})$ modulo 1. For any pair (k,l), note that $-24 \cdot 28s_1$ is congruent to $48(k+l)/N$ modulo 1. But $k+l$ is different for every choice (k,l) and $k+l$ must be smaller than $2\sqrt{N}$ since both $k^2 < N$ and $l^2 < N$. Hence, $0 < 48(k+l)/N < 96/\sqrt{N}$ and if $N \geq 96^2$, then no two values of $48(k+l)$ can be congruent modulo 1. One now easily checks the same is true for all $N \leq 96^2$. Hence, two positively curved, principal Eschenburg spaces are never homeomorphic to each other.

4. Strong inhomogeneity of $F' = \mathrm{SU}(3)//\,\mathrm{T}^2$

We now apply Eschenburg's methods to show that the inhomogeneous example in dimension six is strongly inhomogeneous as well. We outline the construction briefly.

Let $G = \mathrm{SU}(3)$ and $U \cong S^1 \times S^1 \subset \mathrm{U}(3) \times \mathrm{U}(3)$ where

$$U = \left\{ \left(\begin{pmatrix} \bar{z} & & \\ & zw & \\ & & w \end{pmatrix}, \begin{pmatrix} 1 & & \\ & 1 & \\ & & w^2 \end{pmatrix} \right) : z, w \in \mathrm{U}(1) \right\}.$$

Then U acts on G by a two sided action which is free and isometric for a left invariant, $\mathrm{Ad}_{\mathrm{U}(2)}$-invariant metric on SU(3). The quotient space $F' = \mathrm{SU}(3)//U$, is a six dimensional manifold which has positive sectional curvature for the submersed metric (cf. [**?**]).

By looking at the long exact sequence, $\mathrm{T}^2 \to \mathrm{SU}(3) \to F'$, it is a simple matter to compute the homotopy groups of F'.

$$\begin{aligned} \pi_0(F') &= \pi_1(F') = 0, \\ \pi_2(F') &= \mathbf{Z} \oplus \mathbf{Z}, \\ \pi_i(F') &= \pi_i(\mathrm{SU}(3)) \quad \text{for } i \geq 3. \end{aligned}$$

Its cohomology was also computed by Eschenburg (see [**?**]). $H^*(F'; \mathbf{Z}) = \mathbf{Z}[x, y]/(x^3, x^2 + 3xy + y^2)$ where $\deg(x) = \deg(y) = 2$. Using the cohomology ring, Eschenburg showed that this space is not homotopy equivalent to its 'cousin', the homogeneous flag manifold, $\mathrm{SU}(3)/\,\mathrm{T}^2$.

Homogeneous spaces with similar homotopy.

We now assume that $F' = \mathrm{SU}(3)//U$ is homotopy equivalent to some compact, homogeneous space $M = G/H$. Then M has the same homotopy groups as F'. The following proposition almost follows from [**?**, Section 4].

Proposition 4.1. *Let $\mathfrak{g}$, $\mathfrak{h}$ denote the Lie algebras of the groups G, H respectively. Then we may assume that G is simply connected and semi-simple. Furthermore $\mathfrak{h} = \mathfrak{h}' \times \mathbf{R}^2$ where $\mathfrak{h}'$ is semi-simple.*

Proof. We already remarked that M has the same homotopy groups as F'. In particular, M is simply connected and $\pi_3(M) = \mathbf{Z}$, $\pi_4(M) = 0$.

For any compact Lie group, G, it is well known that $\pi_2(G) = 0$ and $\pi_3(G) = \mathbf{Z}^k$, where k is the number of simple factors in its Lie algebra. From the exact sequence in homotopy for the principal bundle $H \to G \to M$ and the homotopy groups of M we have

(*i*) $\pi_0(H) = \pi_0(G)$,

(*ii*) $0 \to \mathbf{Z} \oplus \mathbf{Z} \to \pi_1(H) \to \pi_1(G) \to 0$,
(*iii*) $\pi_3(H) = \pi_3(G) \times \mathbf{Z}$.

Because of (i) we may assume that both G and H are connected since G_0/H_0 is diffeomorphic to G/H. From (ii) it follows that $\mathrm{rank}(\pi_1(H)) = \mathrm{rank}(\pi_1(G)) + 2$ (as abelian groups). So if $\mathfrak{g} = \mathfrak{g}' \times \mathfrak{t}$ where $\mathfrak{g}'$ is semi-simple and T is an l-torus, then we must have $\mathfrak{h} = \mathfrak{h}' \times \mathfrak{s}$ where $\mathfrak{h}'$ is semi-simple and S is an $(l+2)$-torus. Moreover, from (iii), we know that $\mathfrak{g}'$ has one more simple factor than $\mathfrak{h}'$.

Let G' be the simply connected Lie group with Lie algebra $\mathfrak{g}'$. Then $\widehat{G} := G' \times \mathrm{T}^l$ is a covering group of G. Let $\pi : \widehat{G} \to G$ be the covering homomorphism and let $\widehat{H} := \pi^{-1}(H)$. Then the induced covering map, $\bar{\pi} : \widehat{G}/\widehat{H} \to G/H$, is in fact a diffeomorphism since G/H is simply connected. So we may assume that $G = G' \times \mathrm{T}^l$ where G' is a simply connected, compact, semi-simple Lie group.

Now $\mathfrak{h} = \mathfrak{h}' \times \mathfrak{s} \subset \mathfrak{g} = \mathfrak{g}' \times \mathfrak{t}$. $\mathfrak{h}'$ is semi-simple, so its projection to $\mathfrak{t}$ is trivial. So $\mathfrak{h}' \subset \mathfrak{g}'$ and we define $H' = \exp(\mathfrak{h}')$ which is a subgroup of G'. Consider the following chain of morphisms

$$S \overset{i}{\hookrightarrow} H \overset{j}{\hookrightarrow} G \overset{p}{\longrightarrow} \mathrm{T}\,.$$

Let $f = p \circ j \circ i : S \to \mathrm{T}$ be the composite map. By (ii) $j_* : \pi_1(H) \to \pi_1(G)$ is onto. Also $p_* : \pi_1(G) \to \pi_1(T)$ is an isomorphism and $i_* : \pi_1(S) \to \pi_1(T)$ has finite index. Hence, $f_* : \pi_1(S) \to \pi_1(T)$ has finite index. Therefore, the sub-torus, $f(S) \subset \mathrm{T}$ must have the same rank as T and since S and T are connected, f must be surjective. This implies that $\ker(f)_0$, the identity component of the kernel, is a 2-torus, $U \subset S$, which is a subgroup of the semi-simple part G'. Hence, $\mathfrak{g}' \cap \mathfrak{h} = \mathfrak{h}' \times \mathfrak{u}$.

Let $H'' := \exp(\mathfrak{h}' \times \mathfrak{u}) \subset G'$. Then the map

$$\begin{aligned} G'/H'' &\longrightarrow G/H, \\ gH'' &\longmapsto (g,1)\cdot H, \end{aligned}$$

is a covering map and is hence a diffeomorphism. So we may now assume that G is simply connected, semi-simple and $\mathfrak{h} = \mathfrak{h}' \times \mathbf{R}^2$ with $\mathfrak{h}'$ semi-simple. □

We now determine all possible pairs $(\mathfrak{g}, \mathfrak{h}' \times \mathbf{R}^2)$. The spaces F' and G/H are assumed to be closed, orientable, smooth manifolds that are homotopy equivalent. Hence, $\dim F' = \dim G/H = 6$. This implies that the isotropy group H, is a subgroup of $\mathrm{O}(6)$. Since $\mathfrak{h} = \mathfrak{h}' \times \mathbf{R}^2$, rank $\mathfrak{h}' \leq 1$, so either $\mathfrak{h}'$ is trivial or $\mathfrak{h}' = \mathbf{A}_1$. Since $\dim G - \dim H' = 8$ and $\mathfrak{g}$ has one more simple factor than $\mathfrak{h}'$, the corresponding possibilities for $\mathfrak{g}$ are: $\mathbf{A}_2$ and $\mathbf{A}_2 \times \mathbf{A}_1$.

Inspection of the pairs $(\mathfrak{g}, \mathfrak{h}' \times \mathbf{R}^2)$.

For the pair $(\mathfrak{g}, \mathfrak{h}' \times \mathbf{R}^2)$, let $\mathrm{pr}_i : \mathfrak{h} \to \mathfrak{g}_i$ denote the projection of the sub-algebra $\mathfrak{h}$ to $\mathfrak{g}_i$, the i-th simple factor of $\mathfrak{g}$.

1. $(\mathbf{A}_2, \mathbf{R}^2)$

This is the homogeneous space, $\mathrm{SU}(3)/\,\mathrm{T}^2$, the flag manifold over $\mathbb{CP}^2$. As remarked earlier, this is not homotopy equivalent to F' (their cohomology rings are not isomorphic; see [**?**]).

2. $(\mathbf{A}_2 \times \mathbf{A}_1, \mathbf{A}_1 \times \mathbf{R}^2)$

Up to equivalence, there are two representations of $\mathbf{A}_1$ into $\mathbf{A}_2$ corresponding to the standard embeddings,

$$f_1 : \mathfrak{so}(3) \hookrightarrow \mathfrak{su}(3),$$
$$f_2 : \mathfrak{su}(2) \hookrightarrow \mathfrak{su}(3).$$

Also since $\mathbf{A}_1$ is simple, any representation of $\mathbf{A}_1$ into itself must be trivial or an isomorphism (denoted by id). We have the following possibilities for embeddings of $\mathbf{A}_1$ into $\mathbf{A}_2 \times \mathbf{A}_1$:

$$(0, \mathrm{id}), \quad (f_1, \mathrm{id}), \quad (f_2, \mathrm{id}), \quad (f_1, 0), \quad (f_2, 0).$$

(a). $(0, \mathrm{id})$: In this case $\mathrm{pr}_2(\mathbf{R}^2) = 0$ and $G/H = \mathrm{SU}(3)/\,\mathrm{T}^2$ which is not homotopy equivalent to F'.

(b). $(f_1, 0)$, (f_1, id): $\mathfrak{so}(3)$ has no centralizer in $\mathfrak{su}(3)$, so $\mathrm{pr}_1(\mathbf{R}^2) = 0$. But $\mathbf{A}_1$ has rank 1 and $\mathbf{R}^2$ is abelian so $\mathrm{pr}_2(\mathbf{R}^2)$ has dimension at most 1 i.e., $\mathbf{R}^2$ cannot be embedded in $\mathbf{A}_1$. So these embeddings are not possible.

(c). (f_2, id): Since $\mathbf{R}^2$ commutes with $\mathbf{A}_1$ in $\mathbf{A}_1 \times \mathbf{R}^2$ and id is an isomorphism, it follows that $\mathrm{pr}_2(\mathbf{R}^2) = 0$. On the other hand the centralizer of $\mathfrak{su}(2)$ in $\mathfrak{su}(3)$ is 1-dimensional which implies $\dim \mathrm{pr}_1(\mathbf{R}^2) = 1$. So this case is not possible.

(d). $(f_2, 0)$: As in the previous case, $\mathfrak{su}(2)$ has a one dimensional centralizer in $\mathfrak{su}(3)$. For $f_2 : \mathfrak{su}(2) \hookrightarrow \mathfrak{su}(3)$, the standard embedding, $f_2(\mathfrak{su}(2))$ has centralizer $\mathbf{R} \cdot Z$ where $Z = i \cdot \mathrm{diag}(1, 1, -2)$.

As before $\mathrm{pr}_1(\mathbf{R}^2)$ and $\mathrm{pr}_2(\mathbf{R}^2)$ are each at most and at least (and hence exactly) one dimensional. Hence $\mathbf{R}^2$ maps onto the 2-plane spanned by Z and the maximal toral sub-algebra of $\mathbf{A}_1$, and this map is an algebra isomorphism i.e., up to conjugation, $\mathbf{R}^2$ embeds as,

$$\begin{aligned} \phi :\ & \mathbf{R}^2 \hookrightarrow \mathfrak{su}(3) \times \mathfrak{su}(2) \\ & e_1 \longmapsto (Z, 0), \\ & e_2 \longmapsto (0, Y), \end{aligned}$$

where $Y = i \cdot \mathrm{diag}(1, -1)$ generates the usual maximal toral sub-algebra of $\mathfrak{su}(2)$.

Hence the pair $(\mathbf{A}_2 \times \mathbf{A}_1, \mathbf{A}_1 \times \mathbf{R}^2)$ splits as $(\mathbf{A}_2, \mathbf{A}_1 \times \mathbf{R}) \times (\mathbf{A}_1, \mathbf{R})$ which yields the homogeneous space $\mathbb{CP}^2 \times \mathbb{S}^2$. A comparison of the respective cohomology rings reveals that F' is not homotopy equivalent to $\mathbb{CP}^2 \times \mathbb{S}^2$.

Appendix A. Homotopy types of Aloff–Wallach spaces

MARK DICKINSON and KRISHNAN SHANKAR

In this note we consider the homotopy types of the Aloff–Wallach spaces (see Introduction for the definition). In particular we address the question of whether there exist Aloff–Wallach spaces that are homotopy equivalent but not homeomorphic. This is a natural question to ask in view of the examples constructed in this paper as well as the examples of Kreck and Stolz in [**?**] (see also [**?**]). The following is the main result.

Proposition A.1. *Two Aloff–Wallach spaces, $N_{p,q}$ and $N_{r,s}$ are homotopy equivalent if and only if they are homeomorphic.*

This will follow immediately from the next proposition. Recall the cohomology of the Aloff–Wallach spaces (cf. [**?**]): $H^0 = H^2 = H^5 = H^7 = \mathbf{Z}$, $H^4(N_{p,q}, \mathbf{Z})$ is a cyclic group of order $p^2 + pq + q^2$. From theorem 0.1 of [**?**] the Aloff–Wallach spaces $N_{p,q}$ and $N_{r,s}$ are homotopy equivalent if and only if:

(*i*) $n := p^2 + pq + q^2 = r^2 + rs + s^2$,

(*ii*) $pq(p + q) \equiv \pm rs(r + s) \pmod{n}$.

From the main theorem of [**?**] we see that the conditions for homeomorphism are very similar; condition (*ii*) above is replaced by the apparently stronger requirement

(*ii*)′ $pq(p + q) \equiv \pm rs(r + s) \pmod{24n}$.

With these characterizations we can rewrite proposition A.1 in a purely arithmetic form.

Proposition A.2. *Suppose that (p, q) and (r, s) are pairs of integers such that $\gcd(p, q) = \gcd(r, s) = 1$, with $n := p^2 + pq + q^2 = r^2 + rs + s^2$. If $pq(p + q)$ and $rs(r + s)$ are congruent modulo n then they are congruent modulo $24n$.*

Replacing (r, s) with $(-r, -s)$, this proposition also says that if $pq(p+q)$ and $-rs(r+s)$ are congruent modulo n then they are congruent modulo $24n$, so that proposition A.2 implies proposition A.1. The proof of proposition A.2 will be given in the next section.

The main result along with the classification of simply connected, homogeneous, positively curved manifolds now yields the following corollary.

Corollary A.3. *In the class of simply connected, homogeneous, positively curved manifolds, two spaces are homotopy equivalent if and only if they are homeomorphic.*

Note that the corollary is sharp; omitting any of the assumptions makes it false.

Proof of proposition A.2.

We will first reformulate proposition A.2 in terms of the arithmetic of the ring of integers $\mathbf{Z}[\omega]$ of the quadratic field $\mathbf{Q}(\omega)$, where $\omega = (1+\sqrt{-3})/2$ is a primitive sixth root of unity. An application of the law of quadratic reciprocity will then yield a proof of the reformulation. For basic properties of the ring $\mathbf{Z}[\omega]$, including the important fact that $\mathbf{Z}[\omega]$ is a unique factorization domain, we refer the reader to chapters 1 and 9 of [**?**].

A pair of integers (x, y) with $\gcd(x, y) = 1$ corresponds to an element $\alpha = x + y\omega$ of $\mathbf{Z}[\omega]$ which is primitive (that is, not divisible by any non-unit of $\mathbf{Z}$). Writing $\mathrm{N}\xi = \xi\bar{\xi}$ and $\mathrm{Tr}\,\xi = \xi + \bar{\xi}$ for the norm and trace of a general element ξ of $\mathbf{Q}(\omega)$, the quantities $x^2 + xy + y^2$ and $xy(x + y)$ can be recovered from α as $\mathrm{N}\alpha$ and $\mathrm{Tr}(\alpha^3/3\sqrt{-3})$ respectively. Now by assumption, $\mathrm{N}(p + q\omega) = \mathrm{N}(r + s\omega)$. As explained in section 5 of [**?**], it follows that $p + q\omega = \gamma\delta$ and $r + s\omega = \varepsilon\bar{\gamma}\delta$ for some primitive elements γ and δ of $\mathbf{Z}[\omega]$ and some unit ε; by exchanging p and q if necessary we may further arrange that ε is equal to 1. The elements γ and δ defined in this way are coprime in $\mathbf{Z}[\omega]$: if π is a prime element of $\mathbf{Z}[\omega]$ which divides both γ and δ then $\mathrm{N}\pi = \bar{\pi}\pi$ divides $r + s\omega = \bar{\gamma}\delta$, contradicting the assumption $\gcd(r, s) = 1$. In the same way, the assumption $\gcd(p, q) = 1$ implies that $\bar{\gamma}$ and δ are mutually coprime, and combining these results we see that $\mathrm{N}\gamma$ and $\mathrm{N}\delta$ are coprime in $\mathbf{Z}$.

The hypothesis that $pq(p + q)$ is congruent to $rs(r + s)$ modulo n can be written in terms of γ and δ as

$$(\gamma^3 - \bar{\gamma}^3)(\delta^3 + \bar{\delta}^3)/3\sqrt{-3} \equiv 0 \pmod{\mathrm{N}\gamma\,\mathrm{N}\delta}.$$

Similarly, the conclusion of proposition A.2 becomes

$$(\gamma^3 - \bar{\gamma}^3)(\delta^3 + \bar{\delta}^3)/3\sqrt{-3} \equiv 0 \pmod{24\,\mathrm{N}\gamma\,\mathrm{N}\delta}.$$

We thus arrive at the following reformulation of proposition A.2.

Proposition A.2. (bis). *Suppose that γ and δ are primitive elements of the ring $\mathbf{Z}[\omega]$, that $\mathrm{N}\gamma$ is prime to $\mathrm{N}\delta$, and that $T := (\gamma^3-\bar\gamma^3)(\delta^3+\bar\delta^3)/3\sqrt{-3}$ is divisible by $n := \mathrm{N}\gamma\,\mathrm{N}\delta$. Then T is divisible by $24n$.*

To prove this it suffices to check divisibility locally at 2 and 3. We begin by recording some elementary observations regarding primitive elements of $\mathbf{Z}[\omega]$. As noted above, if $\alpha = x + y\omega$ is any element of $\mathbf{Z}[\omega]$ then $\mathrm{N}\alpha$ is equal to $x^2 + xy + y^2$ and $(\alpha^3 - \bar\alpha^3)/3\sqrt{-3}$ is equal to $xy(x + y)$. Similarly, $\alpha^3 + \bar\alpha^3$ can be expressed as $(x - y)(x + 2y)(2x + y)$. By examining the possible residue classes of x and y modulo 3 and 4 we obtain the following proposition.

Proposition A.4. *Suppose that $\alpha = x + y\omega$ is a primitive element of $\mathbf{Z}[\omega]$. Then $\mathrm{N}\alpha$ is congruent to either 0 or 1 modulo 3, and*

(*i*) *3 divides $\alpha^3 + \bar\alpha^3$ if and only if $\mathrm{N}\alpha \equiv 0 \pmod 3$, and*
(*ii*) *3 divides $(\alpha^3 - \bar\alpha^3)/3\sqrt{-3}$ if and only if $\mathrm{N}\alpha \equiv 1 \pmod 3$.*

Similarly, $\mathrm{N}\alpha$ is congruent to either 1 or 3 modulo 4, the integers $\alpha^3 + \bar\alpha^3$ and $(\alpha^3 - \bar\alpha^3)/3\sqrt{-3}$ are even, and

(*iii*) *4 divides $\alpha^3 + \bar\alpha^3$ if and only if $\mathrm{N}\alpha \equiv 3 \pmod 4$, and*
(*iv*) *4 divides $(\alpha^3 - \bar\alpha^3)/3\sqrt{-3}$ if and only if $\mathrm{N}\alpha \equiv 1 \pmod 4$.*

We also note that $(\alpha^3 - \bar\alpha^3)/3\sqrt{-3}$ is always prime to $\mathrm{N}\alpha$, while the greatest common divisor of $\mathrm{N}\alpha$ and $\alpha^3 + \bar\alpha^3$ is either 1 or 3.

Proposition A.4 implies that $\mathrm{N}\gamma$ is congruent to 1 modulo 3, since if it were divisible by 3 then n would be divisible by 3 but $\mathrm{N}\delta$ and T would not be, which would contradict the assumption that n divides T. The proposition now also implies that if $\mathrm{N}\delta$ is congruent to 1 modulo 3 then T is divisible by 3, and that if $\mathrm{N}\delta$ is congruent to 0 modulo 3 then T is divisible by 9, so in either case T is divisible by the largest power of 3 dividing $24n$.

It remains to show that T is divisible by the largest power of 2 dividing $24n$; since n is odd this amounts to showing that T is divisible by 8. Now by hypothesis $n = \mathrm{N}\gamma\,\mathrm{N}\delta$ divides $T = (\gamma^3 - \bar\gamma^3)(\delta^3 + \bar\delta^3)/3\sqrt{-3}$. Since $\mathrm{N}\gamma$ is prime to $(\gamma^3 - \bar\gamma^3)/3\sqrt{-3}$ it must divide $\delta^3 + \bar\delta^3$. It follows that $\mathrm{N}\gamma$ divides $-3(\delta^3 + \bar\delta^3)^2 = \mathrm{Tr}(\sqrt{-3}\delta^3)^2 - (2\,\mathrm{N}\delta)^2(3\,\mathrm{N}\delta)$, and so $3\,\mathrm{N}\delta$ is a square modulo $\mathrm{N}\gamma$. Similarly, $\mathrm{N}\delta$ has highest common factor 1 or 3 with $\delta^3 + \bar\delta^3$, so $\mathrm{N}\delta$ divides $(\gamma^3 - \bar\gamma^3)/\sqrt{-3}$. Hence $\mathrm{N}\delta$ divides $(\gamma^3 - \bar\gamma^3)^2 = \mathrm{Tr}(\gamma^3)^2 - (2\,\mathrm{N}\gamma)^2\,\mathrm{N}\gamma$ and $\mathrm{N}\gamma$ is a square modulo $\mathrm{N}\delta$. Making use of the Jacobi symbol (see chapter 5 of [**?**]) we have $(3\,\mathrm{N}\delta/\mathrm{N}\gamma) = (\mathrm{N}\gamma/\mathrm{N}\delta) = 1$ and therefore

$$1 = \left(\frac{3\,\mathrm{N}\delta}{\mathrm{N}\gamma}\right)\left(\frac{\mathrm{N}\gamma}{\mathrm{N}\delta}\right) = \left(\frac{3}{\mathrm{N}\gamma}\right)\left(\frac{\mathrm{N}\delta}{\mathrm{N}\gamma}\right)\left(\frac{\mathrm{N}\gamma}{\mathrm{N}\delta}\right).$$

Applying the law of quadratic reciprocity to $(3/\mathrm{N}\gamma)$ and $(\mathrm{N}\delta/\mathrm{N}\gamma)$ gives

$$1 = (-1)^{(\mathrm{N}\gamma-1)/2}(-1)^{(\mathrm{N}\gamma-1)(\mathrm{N}\delta-1)/4} = (-1)^{(\mathrm{N}\gamma-1)(\mathrm{N}\delta+1)/4}$$

since $(\mathrm{N}\gamma/3) = (1/3) = 1$. So $(\mathrm{N}\gamma - 1)(\mathrm{N}\delta + 1)/4$ is even, and either $\mathrm{N}\gamma$ is congruent to 1 modulo 4 or $\mathrm{N}\delta$ is congruent to 3 modulo 4. From the second half of proposition A.4 it follows that at least one of the factors $(\gamma^3 - \bar{\gamma}^3)/3\sqrt{-3}$ and $(\delta^3 + \bar{\delta}^3)$ of T is divisible by 4, so T is divisible by 8 as required. This completes the proof of proposition A.2.

Department of Mathematics, University of Michigan, Ann Arbor, MI 48109
E-mail address: shankar@umich.edu
E-mail address: dickinsm@umich.edu