

## ALGEBRAIC CLASSIFICATION OF DIFFEOMORPHISMS

R. E. STONG

(Received May 24, 1978, revised July 17, 1978)

**1. Introduction.** Clearly, one would like to classify diffeomorphisms of manifolds, and several people have tried to do so up to cobordism. Recently Kreck [4] settled this in the oriented case. Since the cobordism problem seems so hard, it is then reasonable to simplify further by reducing to the corresponding algebraic cobordism problem. This algebraic cobordism problem can be completely solved.

Briefly, let  $\mathfrak{N}_n(\text{Iso})$  denote the cobordism group of  $n$  dimensional Poincaré algebras  $M$  together with an isomorphism  $f: M \rightarrow M$ , and let  $\mathfrak{N}_n$  denote the unoriented cobordism group. Then:

a) For  $n = 0$ ,  $\mathfrak{N}_n(\text{Iso})$  is the  $Z_2$  vector space with base given by the mod 2 cohomology of sets with  $2j + 1$  points permuted cyclically (for all  $j \geq 0$ ).

b) For  $n$  odd,  $\mathfrak{N}_n(\text{Iso})$  is isomorphic to  $\mathfrak{N}_n$ , and

c) For  $n$  even,  $\mathfrak{N}_n(\text{Iso}) \cong \mathfrak{N}_n \oplus A$  where  $A$  is a  $Z_2$  vector space with a basis in 1-1 correspondence with the irreducible polynomials

$$p(x) = x^{2^j} + a_1 x^{2^j-1} + \cdots + a_{2^j-1} x + 1$$

over  $Z_2$  which are symmetric, i.e., satisfy  $a_{2^j-i} = a_i$ .

Relating this back to diffeomorphisms, it will be shown that every class in  $\mathfrak{N}_*(\text{Iso})$  comes from a diffeomorphism, using a proof by Charles Giffen. Finally it is noted that algebraically trivial diffeomorphisms need not be boundaries, as diffeomorphisms. For  $n \geq 3$  there is a non-trivial kernel.

The author is indebted to Professors Charles Giffen and Gordon Keller for their assistance, and to the National Science Foundation for financial support during this work.

**2. Dimension zero.** The preliminaries and precise definitions for Poincaré algebras and Lefschetz algebras were first given by Brown and Peterson [1]. We will not insult the reader by repeating all of the formalism. The reader may also find it convenient to look at [6] Section 5 and at [7].

All Poincaré algebras considered here will be over the field  $Z_2$ . An

isomorphism of a Poincaré or Lefschetz algebra will be a homomorphism  $f$  of algebras, commuting with the Steenrod algebra action and such that if  $\mu: M^n \rightarrow Z_2$  is the fundamental class homomorphism, then  $\mu \circ f = \mu$ .

Two Poincaré algebras of dimension  $n$  with isomorphisms  $(M, f)$  and  $(M', f')$  will be cobordant if there are Lefschetz algebras with isomorphism  $(V, g)$  and  $(V', g')$  so that

$$(M, f) \oplus \partial(V, g) \cong (M', f') \oplus \partial(V', g').$$

The resulting set of equivalence classes forms an abelian group under direct sum, and will be denoted  $\mathfrak{N}_n(\text{Iso})$ .

It is not at all difficult to characterize when a Poincaré algebra with isomorphism is a boundary. One has

LEMMA 2.1. *If  $(M, f)$  is a Poincaré algebra with isomorphism, then  $(M, f)$  is a boundary if and only if there is a homogeneous subalgebra  $R \subset M$  closed under the action of the Steenrod algebra, containing the characteristic classes of  $M$ , which is its own annihilator and is invariant under  $f$ .*

PROOF. If  $R$  exists, let  $V = R$ ,  $g$  the restriction of  $f$ ,  $V/\partial V = M/R$  with the isomorphism induced by  $f$ . Then

$$\begin{array}{ccc} & \overline{\phantom{M}} & \\ \downarrow & & \downarrow \\ V \hookrightarrow & M & \rightarrow V/\partial V \end{array}$$

may be given the structure of a Lefschetz algebra with isomorphism. Conversely if  $(M, f)$  is the boundary of  $(V, g)$ , the image of  $V$  in  $M$  has the properties given for  $R$ . q.e.d.

NOTE. Here characteristic class refers to the Stiefel-Whitney classes defined via the Steenrod algebra action: i.e.,  $w_i = \sum Sq^{i-j} v_j$  where  $\mu(v_j x) = \mu(Sq^j x)$  for all  $x$ .

The zero dimensional case behaves much differently from the positive dimensional cases, and is relatively simpler. Geometrically, it is easy to compute the 0-dimensional bordism group of diffeomorphisms. Any diffeomorphism of a zero dimensional manifold is a union of orbits  $\{x, fx, \dots, f^{n-1}x\}$  with  $f^n x = x$  with a cyclic permutation. If  $n$  is even,  $n = 2k$ , this bounds the union of  $k$ -intervals joining  $f^i x$  to  $f^{i+k} x$  with the diffeomorphism  $g$  mapping the interval joining  $f^i x$  to  $f^{i+k} x$  linearly to that joining  $f^{i+1} x$  and  $f^{i+k+1} x$ . Clearly two copies of any orbit bounds. Thus any diffeomorphism of a zero dimensional manifold is bordant to a union of cycles with distinct odd lengths. If such an action  $(M, f)$  is a boundary of some  $(V, g)$ , then  $V$  is a union of intervals. If  $I$  joins

$x$  and  $y$  and  $f^n x = x$ , then  $f^n y = y$ , and thus each orbit separately must bound, which is impossible since they have odd numbers of points. This proves

**PROPOSITION 2.1.** *The zero dimensional cobordism group of diffeomorphisms is the  $Z_2$  vector space with base the actions  $\{x, fx, \dots, f^{n-1}x\}$ ,  $f^n x = x$ , with  $n$  odd.*

Now turning to the algebraic case, let  $M$  be a zero dimensional Poincaré algebra with isomorphism  $f$ . Since  $x = Sq^0 x = x^2$  ( $Sq^0 = 1$  and  $Sq^i x = x^2$  if  $\dim x = i$ ), every element is idempotent. One says  $e \leq f$  if  $e = ef$ , and then  $M$  has a base  $e_1, \dots, e_n$  consisting of the minimal idempotents, with  $1 = e_1 + \dots + e_n$ . Since  $\mu(e_i \cdot e_j) = \mu(0) = 0$  for  $j \neq i$ ,  $\mu(e_i) = \mu(e_i \cdot e_i)$  must be 1, and  $\mu$  is determined.

The isomorphism  $f$  then acts by permutation of the minimal idempotents, which will form cycles, as in the geometric case. In fact,  $(M, f)$  is the cohomology of a diffeomorphism on a 0-dimensional manifold.

If  $R \subset M$  is a subalgebra satisfying the conditions of the lemma, so that  $(M, f)$  bounds, then every  $r \in R$  has the form  $e_{i_1} + \dots + e_{i_{2j}}$ , i.e., is a sum of an even number of minimal idempotents.  $R$  also has a base consisting of minimal idempotents, which are then disjoint sums of an even number of  $e$ 's. Since  $R$  is its own annihilator,  $\dim R = (1/2) \dim M$ , and the base of  $R$  consists of terms  $e_i + e_j$ . Clearly  $e_i$  and  $e_j$  must belong to cycles of the same length in the action of  $f$  on  $R$ , which gives

**PROPOSITION 2.2.**  *$\mathfrak{R}_0(\text{Iso})$  is isomorphic to the zero dimensional cobordism group of diffeomorphisms.*

### 3. Positive dimensions.

**LEMMA 3.1.** *If  $f$  is an isomorphism of the Poincaré algebra  $M$ , then  $f$  is the identity on the characteristic classes of  $M$ .*

**PROOF.** For any  $x \in M$ ,  $x = f(y)$  for some  $y$ , and  $\mu(f(v_i)x) = \mu(f(v_i)f(y)) = \mu f(v_i, y) = \mu(v_i, y) = \mu(Sq^i y) = \mu f(Sq^i y) = \mu(Sq^i f(y)) = \mu(Sq^i x) = \mu(v_i, x)$ , so  $f(v_i) = v_i$ . Since  $f$  commutes with Steenrod operations and algebra operations, the result follows. q.e.d.

**PROPOSITION 3.1.** *For  $n$  odd,  $(M, f)$  bounds if and only if all the Stiefel-Whitney numbers of  $M$  are zero; i.e.,  $\mathfrak{R}_n(\text{Iso}) \cong \mathfrak{R}_n$ .*

**PROOF.** If  $(M, f)$  bounds, clearly  $M$  does, and the Stiefel-Whitney numbers are zero. If the Stiefel-Whitney numbers of  $M$  are zero, let  $R^i \subset M^i$  be the set of characteristic classes of  $M$  for  $i < \dim M/2$  and let  $R^i \subset M^i$  be the annihilator of  $R^{n-i}$  if  $i > \dim M/2$ ,  $\dim M = n$ . This  $R$

satisfies the conditions of Lemma 2.1.

q.e.d.

**PROPOSITION 3.2.** *For  $n = 2k > 0$ ,  $(M, f)$  bounds if and only if all the Stiefel-Whitney numbers of  $M$  are zero and there is an  $f$  invariant subspace  $B \subset M^k$  containing the characteristic classes which is its own annihilator.*

**PROOF.** If  $(M, f)$  bounds, then  $M$  bounds and  $B = R^k$  suffices. Conversely, let  $R^i$  be the characteristic classes for  $i < k$ ,  $B$  for  $i = k$ , and the annihilator of the characteristic classes if  $i > k$ . q.e.d.

In order to determine when such a subspace exists, one may apply the theory of canonical forms. Let  $M$  be an  $n$ -dimensional Poincaré algebra with isomorphism  $f$  where  $n = 2k > 0$ . Then  $f: M^k \rightarrow M^k$  is an isomorphism preserving the non-singular bilinear form  $\langle x, y \rangle = \mu(xy)$  i.e.,  $\langle fx, fy \rangle = \langle x, y \rangle$ .

For each prime polynomial  $p \in Z_2[x]$ , the subspace  $Vp$  of  $M^k$  consisting of all  $x$  such that  $p(f)^r(x) = 0$  for some  $r$  is an  $f$  invariant subspace.

If  $p(x) = x^m + a_1x^{m-1} + \dots + a_{m-1}x + 1$  is a prime, so is  $p'(x) = x^m + a_{m-1}x^{m-1} + \dots + a_1x + 1$ . If  $q$  is another prime not equal to  $p'$ , with  $x \in Vp$  and  $y \in Vq$  and  $p(f)^r(x) = 0$  then

$$0 = \langle p(f)^r(x), y \rangle = \langle x, p(f^{-1})^r(y) \rangle = \langle x, f^{-mr}p'(f)^r(y) \rangle$$

and since  $q \neq p'$ ,  $f^{-mr}p'(f)^r$  is an isomorphism of  $Vq$  onto itself. Thus, for  $q \neq p'$ ,  $Vq$  annihilates  $Vp$ , and in particular, if  $p \neq p'$ , the spaces  $Vp$  and  $Vp'$  are dually paired under the form, each being self-annihilating.

If a subspace  $B$  exists, then  $B$  similarly decomposes and is the direct sum of its subspaces  $B \cap Vp$ ; in particular  $B$  exists if and only if for each prime  $p$  which is symmetric (i.e.,  $p = p'$ )  $Vp$  contains an invariant subspace which is its own annihilator, with the additional proviso that if  $p(x) = x + 1$ , the subspace must also contain the characteristic classes.

**CLAIM.** *If all Stiefel-Whitney numbers of  $M$  are zero, then for  $p(x) = x + 1$ ,  $Vp$  contains an invariant subspace which is its own annihilator and which contains the characteristic classes.*

**PROOF.** Choose a maximal subspace of  $Vp$ ,  $W$ , which is invariant, is self-annihilating, and contains the characteristic classes (such spaces exist for the characteristic classes have this list of properties). Let  $W^\perp$  be the annihilator of  $W$ . Then  $W^\perp$  is  $f$  invariant, so that  $W^\perp/W$  has an isomorphism  $\bar{f}$  induced by  $f$ , and an invariant non-singular form induced by  $\langle, \rangle$ , denoted  $[\cdot, \cdot]$ . Maximality of  $W$  implies that  $W^\perp/W$  has no invariant self-annihilating subspace. If  $W^\perp/W \neq 0$ , there is a  $w \in W$

for which  $[w] \neq 0$ , where  $[w]$  denotes the class in  $W^\perp/W$ , and for which  $\bar{f}([w]) = [w]$ , for  $\bar{f}$  belongs to  $p(x) = x + 1$  type. Then  $[[w], [w]] = \langle w, w \rangle = \mu(w^2) = \mu(Sq^k w) = \mu(v_k w) = \langle v_k, w \rangle = 0$  for  $v_k \in W$  and  $w \in W^\perp$ . The span of  $[w]$  is then an invariant self-annihilating subspace. Thus  $W^\perp/W = 0$ , and  $W$  is its own annihilator. q.e.d.

Now consider a symmetric prime  $p(x) \neq x + 1$ . Then  $p(x)$  must have even degree, so

$$p(x) = x^{2j} + a_1 x^{2j-1} + \dots + a_{2j-1} x + 1$$

with  $a_{2j-i} = a_i$  and  $a_j = 1$ . Using the rational canonical form  $f: Vp \rightarrow Vp$   $f$  may be expressed by a matrix with  $2j \times 2j$  blocks down the diagonal. Thus the degree of  $p$  divides the dimension of  $Vp$ .

CLAIM. For  $p(x) \neq x + 1$  symmetric,  $Vp$  contains an invariant subspace which is its own annihilator if and only if  $(\dim Vp)/(\deg p)$  is even.

The proof of this requires a number of steps. If  $Vp$  has an invariant subspace  $P$  which is its own annihilator, then  $(\dim Vp)/(\deg p)$  is twice  $(\dim P)/(\deg p)$ , so the condition is necessary.

Before looking at the other implication, note that for  $x \in Vp$ ,  $\langle x, x \rangle = \mu(x^2) = \mu(Sq^k x) = \mu(v_k x) = \langle v_k, x \rangle = 0$  for  $v_k$  is in the subspace for  $x + 1$  and so annihilates  $Vp$ .

Now suppose  $(\dim Vp)/(\deg p)$  is even, and let  $W$  be a maximal invariant self-annihilating subspace of  $Vp$ . If  $W^\perp$  is the annihilator of  $W$ , then  $W^\perp$  is  $f$  invariant, so  $W^\perp/W$  inherits an isomorphism and a non-singular invariant bilinear form which is even ( $\langle x, x \rangle = 0$ ). Further,  $(\dim W^\perp/W)/(\deg p)$  is even, for  $\dim W^\perp/W = \dim Vp - 2 \dim W$ , and  $W^\perp/W$  has no invariant self-annihilating subspace other than  $\{0\}$ .

Since  $W^\perp/W$  is associated to  $p$ , assuming it is non-zero, there is an  $x \neq 0$  with  $p(f)(x) = 0$ , and the span  $T$  of  $\{x, fx, \dots, f^{2j-1}x\}$  is an invariant subspace of  $W^\perp/W$ , having no proper invariant subspaces. Now  $\{y \in T \mid \langle y, z \rangle = 0 \text{ for any } z \in T\} = S$  is an invariant subspace of  $T$  and cannot be all of  $T$  since  $W^\perp/W$  has no non-trivial self-annihilating invariant subspaces. Thus,  $S = \{0\}$ , and the restriction of the form to  $T$  is non-singular. Thus  $W^\perp/W$  decomposes into the direct sum of  $T$  and its annihilator, each invariant under  $f$  with the form non-singular.

Proceeding inductively,  $W^\perp/W$  decomposes as the orthogonal direct sum of an even number of subspaces of dimension  $(\deg p)$  invariant under  $f$  and with invariant non-singular even form. Thus, one wishes to analyze such a space  $T$ .

To begin,  $T$  is an irreducible  $Z_2$  representation space for  $Z$ , so a module over the commutative ring  $Z_2[Z]$  and has the property that if  $x \neq 0$  is an element of  $T$ , then  $(Z_2[Z])x = T$ . For any  $x \neq 0$ ,  $Ix = \{\lambda \in Z_2[Z] \mid \lambda x = 0\}$  is a two sided ideal in  $Z_2[Z]$  and  $Z_2[Z]/Ix$  is a field. (Note. If  $\mu \notin Ix$ ,  $\mu x \neq 0$  so  $(Z_2[Z])\mu x = T$  and there is a  $\lambda \in Z_2[Z]$  with  $\lambda \mu x = x$ .) Further  $Ix$  is independent of  $x$ . One may then identify  $T$  with the field  $K = (Z_2[Z])/I$ . This is a finite extension of the field  $Z_2$  of dimension  $2j$  over  $Z_2$ , and is the Galois field with  $2^{2j}$  elements. In particular,  $K$  has a non-singular symmetric bilinear form given by  $\phi(u, v) = \text{trace}(uv)$ , the trace over  $Z_2$  of the linear map given by multiplication by  $uv$ . Writing  $Z$  as the cyclic group generated by  $f$ , the action of  $f$  on  $T$  is identifiable with multiplication by  $\lambda_f$  on  $K$ , where  $\lambda_f$  is the class of  $f$  in  $Z_2[Z] \text{ mod } I$ .

Now define an automorphism  $\sigma: Z_2[Z] \rightarrow Z_2[Z]$  by  $\sigma(\sum \alpha_r f^r) = \sum \alpha_r f^{-r}$ , so that the  $Z_2[Z]$  module structure on the dual of  $T$  is given by  $(\lambda\phi)(x) = \phi(\sigma(\lambda)x)$  for  $\phi \in \text{Hom}(T, Z_2)$ . If  $\psi: T \rightarrow T^*$  is an isomorphism of  $Z_2[Z]$  modules, then for  $v, v' \in T$ ,  $\lambda \in Z_2[Z]$ , one has

$$\psi(\lambda v)(v') = \{\lambda\psi(v)\}(v') = \psi(v)(\sigma(\lambda)v') ,$$

so if  $\lambda \in I$ ,  $\psi(v)(\sigma(\lambda)v') = 0$  for all  $v$  so  $\sigma(\lambda)v' = 0$  and hence  $\sigma(\lambda) \in I$ , while if  $\sigma(\lambda) \in I$ ,  $\psi(\lambda v)(v') = 0$  for all  $v'$  so  $\lambda v = 0$  and  $\lambda \in I$ . Thus if  $T \cong T^*$ ,  $\sigma(I) = I$ , and  $\sigma$  induces an automorphism  $\sigma: K \rightarrow K$ . (Note. Because  $p$  is a symmetric prime, the dual of  $T$  has minimal polynomial  $p' = p$  and hence is isomorphic to  $T$  as  $Z_2[Z]$  modules; thus  $\sigma(I) = I$ .)

CLAIM. *The form  $\theta(u, v) = \text{trace}(u \cdot \sigma(v))$  is a non-singular symmetric bilinear form on  $K$  and is invariant under multiplication by  $\lambda_f$ . Further, the form is even.*

PROOF.  $\theta(v, u) = \text{trace}(v\sigma(u)) = \text{trace}(\sigma(u\sigma(v))) = \text{trace}(u\sigma(v)) = \theta(u, v)$  and

$$\theta(\lambda_f u, \lambda_f v) = \text{trace}(\lambda_f u \cdot \sigma(v) \cdot \lambda_f^{-1}) = \text{trace}(u\sigma(v)) = \theta(u, v) ,$$

while  $\{u \mid \theta(u, v) = 0 \text{ for all } v\}$  is a  $Z$  invariant subspace of  $T$  and is proper since  $\text{trace}(uv)$  is non-singular, hence is the zero subspace. Finally,  $1, \lambda_f, \dots, \lambda_f^{2j-1}$  is a base for  $K$  over  $Z_2$  and  $\theta(\lambda_f^i, \lambda_f^i) = \text{trace}(\lambda_f^i \lambda_f^{-i}) = \text{trace}(1) = 2j = 0$ , so the form is even. q.e.d.

Now let  $\langle, \rangle$  be any non-singular  $f$  invariant even form on  $T$ . This may be considered as a  $Z_2[Z]$  isomorphism  $T \rightarrow T^*$ , while  $\theta$  also gives such an isomorphism. The composite of one isomorphism with the inverse of the other is a  $Z_2[Z]$  isomorphism from  $K$  to itself, hence given by

multiplication by an element of  $K$ . Thus, on  $K$  the form  $\langle, \rangle$  is given by  $\langle u, v \rangle = \text{trace}(\xi u \sigma(v))$  for some  $\xi \in K, \xi \neq 0$ . This form is clearly non-singular and  $f$  invariant. Now  $\langle v, u \rangle = \text{trace}(\xi v \sigma(u)) = \text{trace}(\sigma(\xi) u \sigma(v))$ , so that  $\langle v, u \rangle = \langle u, v \rangle$  implies  $\text{trace}((\xi + \sigma(\xi)) u \sigma(v)) = 0$  for all  $u, v$ , and by non-singularity of the trace form,  $\xi = \sigma(\xi)$ .

Now  $\sigma$  is an automorphism of  $K$  fixing  $Z_2, \sigma(f^0) = f^0$ , and  $\sigma$  is an involution. Further  $\sigma(\lambda_f) = \lambda_f^{-1}$  and  $K - \{0\}$  consists of  $2^{2j} - 1$ 'st roots of unity so  $\lambda_f^{-1} \neq \lambda_f$ , and thus  $\sigma$  is non-trivial. The Galois group of  $K$  over  $Z_2$  is cyclic of order  $2j$  and is generated by the automorphism  $\alpha \rightarrow \alpha^2$ . Thus  $\sigma$  is the unique element of order 2 in the Galois group, and is given by  $\sigma(u) = u^{2^j}$ . Now  $K - O$  is a cyclic group of order  $2^{2j} - 1$  and  $\phi: K - O \rightarrow K - O: u \rightarrow u \sigma(u) = u^{2^j+1}$  is a homomorphism with kernel the  $2^j + 1$ 'st roots of unity. Thus the image of  $\phi$  contains at least  $2^j - 1$  elements, each invariant under  $\sigma$ ; i.e.,  $\sigma(u \sigma(u)) = u \sigma(u)$ . The fixed field of  $\sigma$  is the Galois field on  $2^j$  elements, and each element in this field has the form  $u \sigma(u)$  for some  $u$ . Since  $\sigma(\xi) = \xi$ , one then has  $\langle u, v \rangle = \text{trace}(\lambda \sigma(\lambda) u \sigma(v)) = \text{trace}(\lambda u \cdot \sigma(\lambda v))$ .

Thus, replacing  $x \in T$  by the point  $\lambda^{-1}x$  for some  $\lambda \in K$  makes the form  $\langle, \rangle$  equivalent to the trace form  $\theta$ . In particular  $W^\perp/W$  consists of an even number of summands of the same form. Since  $W^\perp/W$  can have no invariant self-annihilating subspaces, one must have zero copies and  $W^\perp/W = 0$ , completing the proof of our claim.

**PROPOSITION 3.3.** *For  $n = 2k > 0, \mathfrak{N}_n(\text{Iso}) \cong \mathfrak{N}_n \oplus A$  where  $A$  is a  $Z_2$  vector space with a basis in 1-1 correspondence with the irreducible symmetric polynomials of even degree.*

**PROOF.** Send  $(M, f)$  to the bordism class of  $M$  and the numbers  $(\dim V_p)/(\deg p)$  for  $p$  irreducible symmetric of even degree. This is clearly a homomorphism, and by the above discussion is monic. To see that it is epic,  $(M, \text{identity})$  clearly goes to the class of  $M$  in  $\mathfrak{N}_*$ . To get a class with all invariants other than  $(\dim V_p)/\deg p$  zero, one may form a Poincaré algebra of dimension  $n$  with

$$M^0 \cong M^n \cong Z_2$$

$$M^k \cong Z_2 \text{ vector space of dimension } (\deg p)$$

$$M^i = 0 \text{ otherwise}$$

with  $f$  the identity on  $M^0$  and  $M^n$  and having minimal polynomial  $p$  on  $M^k$ . The multiplicative structure is given by making the unit a base for  $M^0$  and by  $x \cdot y \neq 0$  for  $x, y \in M^k$  if and only if  $\langle x, y \rangle \neq 0$  where  $\langle x, y \rangle$  is an  $f$ -invariant, symmetric, even non-singular form on  $M^k$ . That

such forms exist was discussed above using the symmetry of  $p$ . q.e.d.

**4. Remarks.** The first obvious question is whether there are any symmetric irreducible polynomials, and in fact there are such polynomials of degree  $2j$  for each  $j$ . One has

**PROPOSITION 4.1.** *The number of irreducible symmetric polynomials of degree  $2j$  is*

$$\frac{1}{2j} \sum \phi(a)$$

*the sum being over all  $a$  dividing  $2^j + 1$  and not dividing  $2^b - 1$  for any  $b$  properly dividing  $2j$ , where  $\phi(a)$  is Euler's  $\phi$  function.*

**PROOF.** In the Galois field of order  $2^{2j}$ , every non-zero element is a  $2^{2j} - 1$ 'st root of unity and a primitive  $a$ 'th root for some  $a$  dividing  $2^{2j} - 1$ . If  $a$  does not divide  $2^b - 1$  for any  $b$  properly dividing  $2j$ , then primitive  $a$ 'th roots do not lie in a proper subfield. For any such primitive  $a$ 'th root  $\alpha$ , the Galois group acts freely and the smallest degree polynomial satisfied by  $\alpha$  is

$$(x - \alpha)(x - \alpha^2) \cdots (x - \alpha^{2^{2j-1}}) = p(x)$$

which is prime of degree  $2j$ . In order that  $p$  be symmetric, it is necessary and sufficient that  $\alpha^{-1}$  also be a root of  $p$ , and as noted in Section 3,  $\alpha^{-1} = \sigma(\alpha) = \alpha^{2^j}$ . Thus it is precisely when  $a$  divides  $2^j + 1$  that  $p(x)$  is symmetric. The number of symmetric primes is then the number of orbits of the Galois group action on the set of primitive  $a$ 'th roots of unity with  $a$  as given. q.e.d.

**ACKNOWLEDGMENT.** This result was obtained during a discussion with G. Keller, and considerable thanks are due him. C. Giffen independently obtained the result.

For convenience, the examples of least degree are

deg 2:  $x^2 + x + 1$

deg 4:  $x^4 + x^3 + x^2 + x + 1$

deg 6:  $x^6 + x^3 + 1$

deg 8:  $x^8 + x^7 + x^6 + x^4 + x^2 + x + 1$  and  $x^8 + x^5 + x^4 + x^3 + 1$ .

Next, one might ask about the multiplicative structure in  $\mathfrak{N}_*(\text{Iso})$  induced by the tensor product of Poincaré algebras, corresponding to the product of manifolds.

The product in  $\mathfrak{N}_0(\text{Iso})$  is relatively simple, for a product of a cycle



of length  $2n + 1$  with one of length  $2m + 1$  consists of orbits with length the least common multiple of  $2n + 1$  and  $2m + 1$  (with  $\gcd(2n + 1, 2m + 1)$  orbits).

The product of dimension zero classes with odd dimensional classes shows that there are many divisors of zero, since  $\mathfrak{N}_{2j+1}(\text{Iso})$  is finite dimensional.

The product of a zero dimensional class with anything of positive dimension can be zero. For example  $Z_7 \cup \text{pt}$  (a 7 cycle and a point) annihilates all positive dimensional classes for  $H^*(Z_7 \cup \text{pt}; Z_2)$  contains an invariant subspace which is its own annihilator. (Note. The subspace is not a subalgebra and hence  $Z_7 \cup \text{pt}$  does not bound.) This is very intimately related to some bad number theoretic questions and is the fact that  $x^7 - 1/x - 1$  is the product  $(x^3 + x^2 + 1)(x^3 + x + 1)$ .

It is clear then that the multiplicative structure of  $\mathfrak{N}_*(\text{Iso})$  is very ugly.

One might then consider the relationship between the cobordism of diffeomorphisms and  $\mathfrak{N}_*(\text{Iso})$ .

PROPOSITION 4.2 (C. Giffen). *Every class in  $\mathfrak{N}_*(\text{Iso})$  can be realized as the cohomology of a manifold with diffeomorphism.*

PROOF. This has been observed for  $\mathfrak{N}_0(\text{Iso})$  and identity maps give the  $\mathfrak{N}_*$  terms. Now let  $p(x) = x^{2j} + \dots + 1$  be a symmetric prime. Then  $p(x)$  is the mod 2 reduction of an integral polynomial  $q(x) = x^j + \sum_{i=1}^j e_i x^{j-i} (1-x)^{2i}$  with  $e_j = 1$  or 0. By Burde [2],  $q(x)$  is the Alexander polynomial of a Neuwirth knot  $K \subset S^3$ . The knot complement then fibers over a circle and is of the form  $V \times R/(v, t) \sim (f(v), t + 1)$  where  $V$  is a compact 2 manifold with boundary a circle and  $f: V \rightarrow V$  is a diffeomorphism which is the identity on  $\partial V$ . By Milnor [5], the Alexander polynomial of the knot mod 2, i.e.,  $p(x)$ , is any generator of the ideal order in  $H_1(V \times R; Z_2)$  and is the characteristic polynomial of the covering transformation on  $H_1(V \times R; Z_2)$ . Thus letting  $M$  be the closed 2 manifold obtained from  $V$  by attaching  $D^2$  along the boundary, with the diffeomorphism given by  $f$  on  $V$  and by the identity on  $D^2$ , the induced transformation on  $H_1(M; Z_2)$  has characteristic polynomial  $p$ , and since  $p$  is symmetric the characteristic polynomial is the same in cohomology. This diffeomorphism has  $(\dim Vp)/(\deg p) = 1$  and all other invariants vanish.

To form examples of dimension  $2n$ ,  $n > 1$ , consider the product  $RP(2n - 2) \times M$ , with the product of the identity and the above diffeomorphism. This bounds since  $M$  does, and the middle dimensional re-

presentation involves only  $x + 1$  and  $p$ , with  $(\dim Vp)/(\deg p) = 1$ . q.e.d.

To see that there are diffeomorphisms which are trivial algebraically but which do not bound as diffeomorphisms, one notes that if  $(M, f) \cup (N, g) = \partial(V, h)$  then  $R \times M/(s, m) \sim (s+1, f(m)) \cup R \times N/(s, n) \sim (s+1, g(n))$  is the boundary of  $R \times V/(s, v) \sim (s + 1, h(v))$ . In fact, two diffeomorphisms are cobordant if and only if the mapping tori are cobordant as fibrings over  $S^1$ . Now consider  $CP(2)$  with the identity and with conjugation. These are identical algebraically but the mapping tori are  $S^1 \times CP(2)$ , which bounds, and the Dold manifold  $P(1, 2)$ , which does not bound.

There are many such examples, for any involution is algebraically equivalent to the identity map. Conner and Floyd [3] produced many examples with non-bounding mapping tori using involutions on manifolds of dimension 3 or more, and hence for  $n \geq 3$  there are non-bounding diffeomorphisms representing zero in  $\mathfrak{N}_n(\text{Iso})$ .

**5. Addendum.** There are many obvious questions which arise in studying diffeomorphisms. The object of this addendum is to describe a beautiful diffeomorphism, and to draw some observations from it. The specific results were worked out in discussion with Charles Giffen, to whom thanks are due.

One begins with a solid torus with three holes  $H$  i.e.,  $D^3 \cup 3$  copies of  $D^1 \times D^2$  attached along the copies of  $S^0 \times D^2$

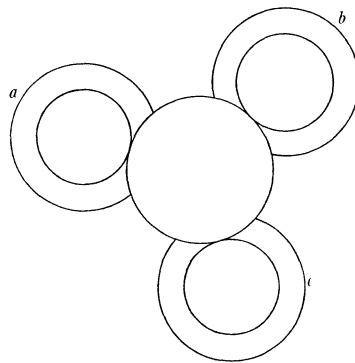


FIGURE 1

First one rotates through  $120^\circ$  to obtain

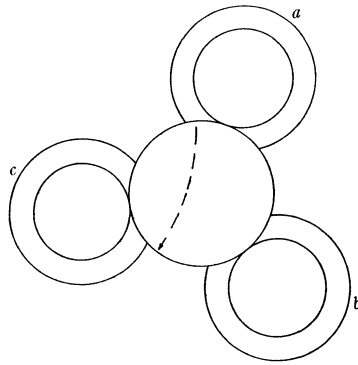


FIGURE 2

and then moves the handle *a* to obtain

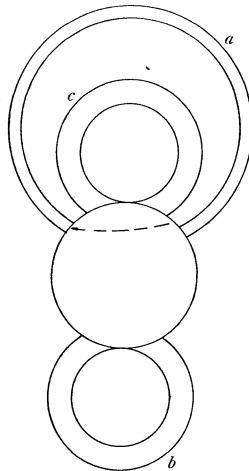


FIGURE 3

where the dotted lines indicate the path followed by the copy of  $D^2$  by which the handle is attached. One then thickens the area between two handles *a* and *c* to obtain

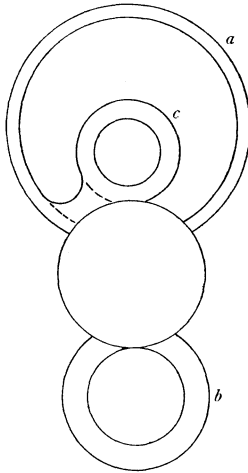


FIGURE 4

and continuing to thicken

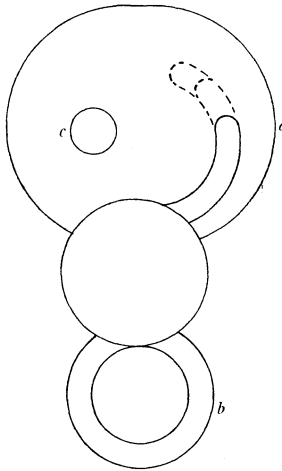


FIGURE 5

which is  $H$  again.

The composite of these maps gives a diffeomorphism from  $H$  to itself, sending boundary to boundary. The effect in mod 2 homology, given by  $H_0(H) = \mathbb{Z}_2$ ,  $H_1(H) = \mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_2$ ,  $H_i(H) = 0$  if  $i > 1$  sends the cycle represented by the handle  $b$  to that of  $c$ , of  $c$  to  $a$ , and of  $a$  to something wrapping around both  $a$  and  $b$  once. This is the identity of dimension 0 homology, and in dimension 1 is represented by the matrix (mod 2).

$$\begin{pmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & 0 & 1 \end{pmatrix}$$

with characteristic polynomial  $x^3 + x^2 + 1$ . In cohomology the polynomial is  $x^3 + x + 1$ , given by the dual.

In particular, the boundary is a diffeomorphism of the connected sum of 3 copies of  $S^1 \times S^1$  with a 2 sphere. The mod 2 cohomology is  $Z_2$  in dimensions 0 and 2, 6 copies of  $Z_2$  in dimension 1 and zero otherwise, and the diffeomorphism has characteristic polynomial  $(x^3 + x^2 + 1)(x^3 + x + 1) = (x^7 - 1)/(x - 1)$  in dimension 1.

Similar constructions may be made with more handles, and one may form the product with  $D^m$ . This shows many facts, or curiosities.

OBSERVATION 1. Up to cobordism the subspaces of mod 2 cohomology with minimal polynomial  $p(x)$  with  $p$  a non-symmetric prime carry no information.

OBSERVATION 2. One of the most obvious cobordism invariants is the Euler characteristic, and its diffeomorphism analogue is the Lefschetz number. The Lefschetz number is non-zero for this bounding diffeomorphism, and hence is not a cobordism invariant for diffeomorphisms. The problem arises from the fact that the trace of a matrix and its inverse are not the same.

#### REFERENCES

- [1] E. H. BROWN, JR. AND F. P. PETERSON, Algebraic bordism groups, *Annals of Math.*, 79 (1964), 616-622.
- [2] G. BURDE, Alexanderpolynome Neuwirthscher Knoten, *Topology*, 5 (1966), 321-330.
- [3] P. E. CONNER AND E. E. FLOYD, Fibring within a cobordism class, *Michigan Math. J.*, 12 (1965), 33-47.
- [4] M. KRECK, Bordism of diffeomorphisms, *Bull. Amer. Math. Soc.*, 82 (1976), 759-761.
- [5] J. W. MILNOR, Infinite cyclic coverings, in "Conference on the Topology of Manifolds" edited by J. G. Hocking, Prindle, Weber, and Schmidt, Inc., Boston, 1968.
- [6] R. E. STONG, Bilinear forms on manifolds, *Math. Ann.*, 205 (1973), 249-263.
- [7] R. E. STONG, Poincaré algebras modulo an odd prime, *Comm. Math. Helv.*, 49 (1974), 382-407.

DEPARTMENT OF MATHEMATICS  
UNIVERSITY OF VIRGINIA  
CHARLOTTESVILLE, VIRGINIA  
22903 U.S.A.

