Knot cobordism and amphicheirality.

Comment. Math. Helvetici 58 (1983) 601–616
0010–2571/83/040601–16\$01.50 + 0.20/0

Knot cobordism and amphicheirality

DANIEL CORAY and FRANÇOISE MICHEL

Introduction

Let C_n denote the cobordism group of n-dimensional knots. Cameron Gordon has asked the following question ([Ha], problem 16):

Can every element of order 2 *in* C_1 *be represented by a* (-1)*-amphicheiral knot?*

A knot is called (-1)-amphicheiral if it is isotopic to its obvious cobordism inverse (see §1 for a precise definition). Hence it is clear that the cobordism class of any (-1)-amphicheiral knot has order two. Gordon's question is about a partial converse of this statement.

Actually the problem makes sense in any odd dimension. (We recall that $C_n = 0$ for n even [K].) But, for $n = 2q-1$, we show:

STATEMENT 1. *The answer is negative for every* $q \geq 2$. *More precisely, some Alexander polynomials* γ *have the following property: the cobordism class of every knot whose Alexander polynomial is* γ *has order two, but contains no* (-1)*-amphicheiral knot.*

STATEMENT 2. *For* $q = 1$ *the same polynomials provide many examples of algebraic cobordism classes of order* 2 *which contain no* (-1)*-amphicheiral knot. Since they are exceedingly numerous, it seems reasonable to expect that Gordon's question should have a negative answer also in the classical case.*

For the proof we work with the algebraic invariants already used in [T], [Mic] and [Hi]. One of the main features is a new (-1)-amphicheirality criterion, which is considerably more general than those previously obtained. In particular it is invariant under cobordism and applies to knots of any odd dimension.

We thank J. Hillman, who pointed out the interest of studying Gordon's problem in higher dimensions.

§1. Statements of the results

We begin with some definitions:

1. An *n-knot* Σ is a smooth, oriented submanifold of S^{n+2} which is homeomorphic to S^n.

2. Let $\sigma: S^{n+2} \to S^{n+2}$ be the reflection in some equatorial plane, $(\sigma(\Sigma))^-$ the image of Σ with the opposite orientation. By $-\Sigma$ we shall denote $(\sigma(\Sigma))^-$ regarded as a submanifold of S^{n+2}. We call it the *inverse of* Σ. As $\Sigma \# -\Sigma$ is null-cobordant, the cobordism class of $-\Sigma$ is the inverse of the cobordism class of Σ.

3. Σ is said to be (-1)-*amphicheiral* ("involutory" in the terminology of J. Conway) if it is isotopic to $-\Sigma$.

4. For $\varepsilon = \pm 1$, let $C^{\varepsilon}(\mathbb{Z})$ be the cobordism group of ε-forms (cf. [L₁] or [K]). Associating a Seifert form to a $(2q-1)$-knot induces a homomorphism φ_{2q-1} from C_{2q-1} to $C^{(-1)^q}(\mathbb{Z})$. The *algebraic cobordism class* of a $(2q-1)$-knot Σ is the image by φ_{2q-1} of the cobordism class of Σ. We recall that φ_{2q-1} is injective if and only if $q \geqslant 2$ ([L_1] and [C–G]). It is the reason why our results do not answer Gordon's question when $q = 1$.

5. For any polynomial $\Delta \in \mathbb{Z}[X]$, of degree d (say), we define $\Delta^* \in \mathbb{Z}[X]$ by the formula:

$$\Delta^*(X) = X^d \Delta(X^{-1}).$$

We recall that Δ is *reciprocal* if $\Delta = \Delta^*$.

6. Given an irreducible reciprocal polynomial $\gamma \in \mathbb{Z}[X]$, we define K to be the number field $\mathbb{Q}[X]/(\gamma)$, and $\mathcal{O}_K$ its ring of algebraic integers. As γ is reciprocal, mapping X into X^{-1} induces an involution on K. We write $\bar{\alpha}$ for the image of $\alpha \in K$ under this involution. Finally we set $a = \gamma(0)$ and adopt the following terminology:

γ *has property* P_1 if $\alpha\bar{\alpha} = -1$ for some α in K;

γ *has property* P_2 if $\alpha\bar{\alpha} = -1$ for some α in the ring $\mathcal{O}_K[1/a]$;

γ *has property* P_3 if $\eta\bar{\eta} = -1$ for some unit η in $\mathcal{O}_K$.

We are now in a position to give the precise statements that we shall prove. In what follows, q is any positive integer, and Σ a $(2q-1)$-knot. If Δ is the Alexander polynomial of Σ, we have $\Delta = \Delta^*$. Hence we can write:

$$\Delta = \delta\delta^* \prod_{i=1}^{l} \gamma_i,$$

where the γ_i are distinct irreducible reciprocal polynomials. (The γ_i are those reciprocal polynomials which appear with odd multiplicity among the irreducible factors of Δ.)

THEOREM 1. *If Σ is (-1)-amphicheiral then γ_i has property P_2, for every $i \leq l$.*

This (-1)-amphicheirality criterion is proved in §2. In practice, property P_3 is a lot more convenient to work with than P_2. This makes the interest of the following two propositions, where *γ is assumed to be an irreducible reciprocal polynomial such that $\gamma(1) = \pm 1$.*

PROPOSITION 1. *Suppose $|\gamma(0)|$ is a prime p and $\mathbb{Z}[X, X^{-1}]/(\gamma) = \mathcal{O}_K[1/p]$. Then γ has property P_2 if and only if it has P_3.*

PROPOSITION 2. *Suppose $|\gamma(0)|$ is a prime p and K is a Galois extension of $\mathbb{Q}$. Then γ has property P_2 if and only if it has P_3.*

For Proposition 1 we give a topological argument, while Proposition 2 is established by purely algebraic means.

Remark. Proposition 2 will be used in §4 in constructing the appropriate examples.

In §3 we prove:

THEOREM 2. *Let Σ be a $(2q-1)$-knot whose Alexander polynomial γ is irreducible. Then:*

(1) *γ has property P_1 if and only if the algebraic cobordism class of Σ has order two;*
(2) *if Σ is cobordant to some (-1)-amphicheiral knot then γ has property P_2.*

SCHOLIUM. *If $q \geq 2$ and γ has property P_1 then the geometric cobordism class of Σ is also of order two, as follows from* [L_1].

COROLLARY. *To prove statements 1 and 2 of the introduction it is enough to produce some irreducible, reciprocal polynomials γ with the following properties:*

(1) *γ is the Alexander polynomial of some $(2q-1)$-knot;*
(2) *γ has property P_1;*
(3) *γ fails to have property P_2.*

In §4 we show how to construct infinitely many irreducible Alexander polynomials having property P_1 but not P_2. As a matter of fact there are some examples already in degree 2, but recall:

Levine's criterion [L_1]. *A reciprocal polynomial $\gamma \in \mathbb{Z}[X]$, with degree d, is the Alexander polynomial of some $(2q-1)$-knot if and only if $\gamma(1)=\varepsilon^{d/2}$ and $\gamma(\varepsilon)$ is a perfect square, where $\varepsilon=(-1)^{q+1}$.*

Now, if γ is any reciprocal polynomial of degree 2 such that $\gamma(1)=-1$, we observe that $\gamma(-1)$, being the discriminant of γ, can be a perfect square only if γ is reducible! Therefore, by Levine's criterion, no example with q even can be obtained in degree 2. That is why we shall give two series of examples:

I. *The quadratic case* (*which occurs only for odd values of q*)

$$\gamma(X)=-pX^2+(2p+1)X-p,$$

where p runs through a certain set of primes: $p=367, 379, 461, 751, 991, \cdots$ (61 examples for $p<10{,}000$).

Remark. In [T], H. F. Trotter already observed that the knots with Alexander polynomial $\gamma(X)=-367X^2+735X-367$ are not (-1)-amphicheiral.

II. *The biquadratic case* (*which occurs for any q*)

In §4 we prove the following theorem:

THEOREM 3. *Let p be an odd prime and*

$$\gamma(X)=-pX^4+(2p+1)X^2-p.$$

Then γ is irreducible. Moreover:

(1) *γ has property P_1;*

(2) *γ fails to have property P_2 if and only if p is congruent to* 3 *modulo* 4 *and the fundamental unit of $\mathbb{Q}(\sqrt{4p+1})$ has norm* $+1$.

Remark. This yields infinitely many examples. Indeed the fundamental unit of $\mathbb{Q}(\sqrt{4p+1})$ has norm $+1$ whenever $4p+1$ has a prime factor with odd multiplicity which is congruent to 3 modulo 4 (e.g. $p=19, 23$, etc.), and also in certain other cases, like $p=367, 379, 751, 991, \cdots$ etc.

Other examples. The following polynomials:

$$\gamma(X)=X^4-2\lambda X^3+(4\lambda-1)X^2-2\lambda X+1,$$

with $\lambda=36, 45, \cdots$ (an infinity of examples), satisfy all three properties of the above corollary. This is proved in [C] with the techniques that we use in the proof of Theorem 3. The particular interest of these examples is that they can be realized as Alexander polynomials of some *fibered* knots.

§2. An amphicheirality criterion

Proof of Theorem 1. We recall that Σ is a (-1)-amphicheiral $(2q-1)$-knot with Alexander polynomial Δ. To prove Theorem 1, we must show: if $\Delta = \gamma^{2l+1}\cdot\mu$, where γ is reciprocal, irreducible and prime to μ, then γ has property P_2.

Let $\tilde{X}$ be the infinite cyclic covering of the complement of Σ. Put $M = H_q(\tilde{X})$; this is a torsion module over $\mathbb{Z}[X, X^{-1}]$. Let $B: M\times M \to \mathbb{Q}(X)/\mathbb{Z}[X,X^{-1}]$ be the Blanchfield pairing associated with Σ (cf. [L_3], p. 15). If we write ε for $(-1)^{q+1}$, the Blanchfield pairing is ε-hermitian and unimodular (i.e. the adjoint of B yields a $\mathbb{Z}[X, X^{-1}]$-isomorphism between M and $\mathrm{Hom}_{\mathbb{Z}[X,X^{-1}]}(M, \mathbb{Q}(X)/\mathbb{Z}[X,X^{-1}])$) (cf. [$L_3$]). We recall that B can be constructed as follows ([L_3], Proposition 14.3, p. 44):

Let A be an $r\times r$ matrix which represents a Seifert pairing of Σ (see, for example, [K]). We denote by A^t the transpose of A. Now M is isomorphic to

$$(\mathbb{Z}[X, X^{-1}])^r/(AX-\varepsilon A^t)$$

and, with this presentation of M, the form B corresponds to $(1-X)(AX-\varepsilon A^t)^{-1}$.

As $-A$ is a Seifert matrix for $-\Sigma$, it follows from the above that $(M, -B)$ is the Blanchfield pairing of $-\Sigma$. Now the isomorphism class of (M, B) is an invariant of the isotopy class of Σ. Hence the (-1)-amphicheirality of Σ yields a $\mathbb{Z}[X, X^{-1}]$-automorphism F of M such that $B(F(\alpha), F(\beta)) = -B(\alpha, \beta)$ for all α and β in M.

Let A_0 be any non-degenerate Seifert matrix in the S-equivalence class of A (cf. [T]). Then $\Delta(X) = \det(A_0X - \varepsilon A_0^t)$ is independent of the choice of A_0, and $\Delta(0) = \det(A_0) \neq 0$.

By assumption, $\Delta = \gamma^{2l+1}\cdot\mu$, with coprime γ and μ. Let us define:

$$M_\gamma = \mu(X)M \subset \mathrm{Ker}\,\gamma(X)^{2l+1} \quad \text{and} \quad M_\mu = \gamma^{2l+1}(X)M \subset \mathrm{Ker}\,\mu(X).$$

Clearly $M_\gamma \cap M_\mu = 0$. Since μ and γ are both reciprocal, the Blanchfield pairing B splits orthogonally on $M_\gamma \oplus M_\mu$. Moreover, the index of $M_\gamma \oplus M_\mu$ in M is finite; therefore the restriction, B_γ, of B to M_γ is non-degenerate. Furthermore the restriction, F_γ, of F to M_γ yields an isomorphism from (M_γ, B_γ) to $(M_\gamma, -B_\gamma)$.

We now define:

$$M^i = \{\alpha \in M_\gamma \mid \gamma^i(X)\alpha = 0\}$$
$$H^i = M^i/(M^{i-1} + \gamma(X)M^{i+1}).$$

Put $R = \mathbb{Z}[X, X^{-1}]/(\gamma)$. Then H^i is an R-module of finite rank e_i (say) and the $\mathbb{Q}[X, X^{-1}]$-module $M_\gamma \otimes_\mathbb{Z} \mathbb{Q}$ is isomorphic to:

$$\bigoplus_{i=1}^{\infty} (\mathbb{Q}[X, X^{-1}]/(\gamma)^i)^{e_i}.$$

As $\sum_{i=1}^{\infty} i \cdot e_i = 2l+1$, there is only a finite number of non-zero e_i; and one of them, say e_{i_0}, must be odd. We write: $n = e_{i_0}$, $H = H^{i_0}$, and denote by $[\alpha]$ the class in H of an element $\alpha \in M^{i_0}$. One can define a non-degenerate, ε-hermitian form $b: H \times H \to \mathbb{Q}(X)/\mathbb{Z}[X, X^{-1}]$ by setting, for any α and β in M^{i_0}:

$$b([\alpha], [\beta]) = B_\gamma(\gamma^{i_0-1}(X)\alpha, \beta).$$

That the form b is well-defined is proved in [Mil], where it is also shown that b is non-degenerate provided B_γ is.

As $\gamma(X)b(\alpha, \beta)$ is in $\mathbb{Z}[X, X^{-1}]$ for all α and β in H, it follows that $b(\alpha, \beta) = P(X)/\gamma(X)$, where $P(X)$ is some polynomial in $\mathbb{Z}[X, X^{-1}]$. Setting $b'(\alpha, \beta) = P(X)$ defines a non-degenerate ε-hermitian form $b': H \times H \to R$, and F_γ induces an R-isomorphism from (H, b') to $(H, -b')$. Since H is of rank n over R, we see that $\Lambda^n H$, the n-th exterior power of H, can be identified with an R-ideal I. In [B] (§1, no 9, p. 31) the n-th exterior power of b' is defined, and it is shown that $\Lambda^n b'$ is non-degenerate provided b' is. Let f be the isomorphism from $(I, \Lambda^n b')$ to $(I, \Lambda^n(-b'))$ which is induced by F_γ. We write R_I for the ring of coefficients of the R-ideal I, i.e. $R_I = \{\alpha \in K \mid \alpha I \subset I\}$. We recall that $a = \gamma(0)$; so $R \subset \mathcal{O}_K[1/a]$.

LEMMA 1. $R_I \subset \mathcal{O}_K[1/a]$.

Proof. Put $S = \mathcal{O}_K[1/a]$ and $J = I \cdot S$. Clearly the ring of coefficients, S_J, of J contains R_I. Hence it is enough to show that $S_J \subset S$. But S is a Dedekind ring; hence the ring of coefficients of any non-zero S-ideal is S itself. □

As f is an R-automorphism of I, there exists u in R_I, hence in $\mathcal{O}_K[1/a]$ (by the lemma), such that $f(\alpha) = u\alpha$ for all α in I. Now n is odd, hence $\Lambda^n(-b') = -\Lambda^n b'$.

Let us take α and β in I, both non-zero; then $(\Lambda^n b')(\alpha, \beta) \neq 0$; so the relations

$$(\Lambda^n b')(f(\alpha), f(\beta)) = u\bar{u}(\Lambda^n b')(\alpha, \beta) = -(\Lambda^n b')(\alpha, \beta)$$

imply $u\bar{u} = -1$. This completes the proof of Theorem 1. □

Proof of Proposition 1. Suppose γ has property P_2. Under the assumptions of Proposition 1, we show that γ also has property P_3. Let $M = \mathbb{Z}[X, X^{-1}]/(\gamma)$; we define a unimodular hermitian form $B: M \times M \to \mathbb{Q}(X)/\mathbb{Z}[X, X^{-1}]$ by setting $B(\alpha, \beta) = \alpha\bar{\beta}/\gamma(X)$ for any α and β in M.

As γ has property P_2 and $\mathcal{O}_K[1/\gamma(0)] = \mathbb{Z}[X, X^{-1}]/(\gamma)$, multiplication by an element u in $\mathcal{O}_K[1/\gamma(0)]$ such that $u\bar{u} = -1$ yields an isomorphism from (M, B) to $(M, -B)$. Now the form (M, B) is always the Blanchfield pairing of some $(2q-1)$-knot, provided we choose q odd (see Theorem 12.1 in [L$_3$]). Let A be a non-degenerate Seifert matrix associated with such a knot. Assuming $|\gamma(0)|$ is a prime number p, Trotter [T] (Corollary 4.7, p. 196) shows that (M, B) is isomorphic to $(M, -B)$ if and only if A is isomorphic to $-A$. (A word of caution: Trotter calls Seifert form what is usually called Blanchfield pairing, as here.)

On the other hand, since γ is irreducible, the isomorphism between A and $-A$ implies the existence of u in $\mathcal{O}_K$ such that $u\bar{u} = -1$ (cf. [Mic]). This completes the proof of Proposition 1. □

Proof of Proposition 2. We begin by showing that Proposition 2 can be deduced from the following lemma:

LEMMA 2. *Let F be a number field, $\mathcal{O}_F$ its ring of algebraic integers and $a \in \mathbb{N}^*$. Suppose there exists a Galois automorphism $\sigma: F \to F$ such that $\sigma^2 = \mathrm{id}$ (σ is an involution of F), and an element α in $\mathcal{O}_F[1/a]$ such that $\alpha \cdot \sigma(\alpha) = -1$. If, for some odd integer $\lambda \in \mathbb{N}^*$, every prime ideal $\mathfrak{p} \subset \mathcal{O}_F$ dividing a and distinct from $\sigma(\mathfrak{p})$ is such that $\mathfrak{p}^\lambda$ is principal, then there exists η in $\mathcal{O}_F$ such that $\eta\sigma(\eta) = -1$.*

Lemma 2 *implies Proposition* 2:

We recall that $p = |\gamma(0)|$ is prime. Consider the following polynomial:

$$\varphi(X) = \gamma(1)X^d\gamma\left(1 - \frac{1}{X}\right) = \gamma(1)(\gamma(1)X^d + \cdots + (-1)^d\gamma(0)),$$

where d is the degree of γ. As $\gamma(1) = \pm 1$, the polynomial φ is monic, and $\varphi(0) = \pm p$.

Let $\xi_1, \ldots, \xi_d$ be the roots of φ. Since φ is irreducible, they are all distinct. Moreover, K is Galois; hence they all lie in K. For every i, the ideal $\mathfrak{p}_i = (\xi_i)$ is prime (with degree one), since $N_{K/\mathbb{Q}}(\xi_i) = \pm p$. By construction it is principal and

$$(p) = \prod_{i=1}^{d} \mathfrak{p}_i.$$

(We do not claim that the $\mathfrak{p}_i$ are all distinct!) Therefore all prime ideals dividing p are principal. Thus Proposition 2 is a consequence of Lemma 2 (with $F = K$, $\sigma(\alpha) = \bar{\alpha}$, $a = p$ and $\lambda = 1$).

Proof of Lemma 2. Suppose $\alpha \cdot \sigma(\alpha) = -1$ for some α in $\mathcal{O}_F[1/a]$. We may write the fractional ideal (α) as a product of prime ideals:

$$(\alpha) = \prod \mathfrak{p}^{v_{\mathfrak{p}}(\alpha)} \tag{2.1}$$

Since $\alpha\sigma(\alpha) = -1$, we have:

$$v_{\mathfrak{p}}(\alpha) + v_{\sigma(\mathfrak{p})}(\alpha) = 0 \quad \forall \mathfrak{p}. \tag{2.2}$$

If $v_{\mathfrak{p}}(\alpha) \neq 0$, it follows from (2.2) that either $v_{\mathfrak{p}}(\alpha)$ or $v_{\sigma(\mathfrak{p})}(\alpha)$ is negative; hence $\mathfrak{p}$ divides a. The relation (2.2) shows also that $v_{\mathfrak{p}}(\alpha) = 0$ if $\mathfrak{p} = \sigma(\mathfrak{p})$.

Let us now consider the prime ideals $\mathfrak{p}_i \neq \sigma(\mathfrak{p}_i)$ which divide a. By assumption, we may write $\mathfrak{p}_i^{\lambda} = (\pi_i)$ for some $\pi_i \in F$. Then the relations (2.1) and (2.2) imply:

$$\alpha^{\lambda} = \eta \prod_i \left(\frac{\sigma(\pi_i)}{\pi_i}\right)^{\mu_i}, \tag{2.3}$$

with $\mu_i \in \mathbb{Z}$ and η a unit in $\mathcal{O}_F$. We see that $\alpha^{\lambda}\sigma(\alpha)^{\lambda} = \eta \cdot \sigma(\eta)$. Now λ is *odd*; hence $\eta \cdot \sigma(\eta) = -1$. This completes the proof of Lemma 2. $\square$

§3. Knot cobordism classes of order two

Proof of the first assertion of Theorem 2. Let Σ be a $(2q-1)$-knot whose Alexander polynomial γ is irreducible. Put $\varepsilon = (-1)^q$. We recall some definitions and basic facts about algebraic cobordism (for more details see [K]).

DEFINITION. An $n \times n$ integral matrix B *represents an* ε*-form* if the matrix $B + \varepsilon B^t$ is invertible over $\mathbb{Z}$.

If A is a Seifert matrix associated with Σ, then $A + \varepsilon A^t$ is the matrix of the intersection form on a Seifert surface of Σ. Since Σ is a sphere, this intersection form is unimodular [K]. Hence A represents an ε-form.

DEFINITION. An ε-form is *null-cobordant* if it is represented by a matrix of the form $\begin{pmatrix} 0 & A_1 \\ A_2 & A_3 \end{pmatrix}$, where the A_i are all square integral matrices.

Let $C^\varepsilon(\mathbb{Z})$ be the group of cobordism classes of ε-forms. On tensoring with $\mathbb{Q}$, we obtain an injective map from $C^\varepsilon(\mathbb{Z})$ to the group of cobordism classes of rational ε-forms, say, $C^\varepsilon(\mathbb{Q})$.

The first assertion of Theorem 2 can therefore be stated as follows: *Given a Seifert matrix A of Σ, then $A \oplus A$ is null-cobordant if and only if γ has property P_1.* This fact can be deduced from Levine's description of $C^\varepsilon(\mathbb{Q})$ [L_2] or from Stoltzfus's computation of $C^\varepsilon(\mathbb{Z})$ [St], but we shall give here a direct and elementary proof.

As in §1, K is the number field $\mathbb{Q}[X]/(\gamma)$. Let $H^\varepsilon(K)$ be the Witt group of non-degenerate ε-hermitian forms $B: M \times M \to K$, where M runs through the finite-dimensional vector spaces over K.

LEMMA 3. *Suppose M is a one-dimensional vector space over K. Then the class of B in $H^\varepsilon(K)$ has order two if and only if γ has property P_1.*

Proof. If γ has property P_1, then $\alpha\bar{\alpha} = -1$ for some α in K. Multiplication by α yields an automorphism of M that carries B into $-B$. Thus $B \oplus B$ is isomorphic to $B \oplus (-B)$; therefore its Witt class is zero.

As B has rank one, if the Witt class of $B \oplus B$ is zero, this form is represented by a matrix of the form $\begin{pmatrix} 0 & \beta_1 \\ \varepsilon\bar{\beta}_1 & \beta_2 \end{pmatrix}$ with $\beta_i \in K$. If $\beta \in K^*$ is the determinant of B, then:

$$\beta = \varepsilon\bar{\beta}. \tag{3.1}$$

As the determinant is defined up to an element of K^* of the form $\eta \cdot \bar{\eta}$, we obtain the relation:

$$\det(B \oplus B) = \beta^2 = -\varepsilon\beta_1\bar{\beta}_1\eta\bar{\eta}. \tag{3.2}$$

If we write $\alpha = \beta^{-1}\beta_1\eta$, the relations (3.1) and (3.2) show that $\alpha \cdot \bar{\alpha} = -1$. This completes the proof of Lemma 3. $\square$

In the S-equivalence class of Seifert matrices corresponding to Σ, we can choose one which is non-degenerate [T]. Call it A. Then the rank of A is equal to the degree, d, of γ. Let M be a d-dimensional vector space over $\mathbb{Q}$. The matrix $T=-\varepsilon A^{-1}A^t$ represents an automorphism of M. Put $X \cdot \alpha = T(\alpha)$. This action of $\mathbb{Q}[X]$ induces on M the structure of a one-dimensional K-vector space. There exists an ε-hermitian form $B: M \times M \to K$ such that the relation:

$$(a\alpha)^t(A+\varepsilon A^t)(\beta) = \mathrm{trace}_{K/\mathbb{Q}}\, aB(\alpha, \beta) \tag{3.3}$$

is satisfied for all a in K and α, β in M (see [Mil]). Now, using (3.3), a direct computation shows that $A \oplus A$ is null-cobordant if and only if the Witt class of B has order two. By Lemma 3 this completes the proof of assertion (1).

Proof of the second assertion of Theorem 2. Suppose Σ is cobordant to Σ'. Then the Fox–Milnor relation shows that the Alexander polynomial of Σ' is of the form $\delta \cdot \delta^* \cdot \gamma$ for some integral polynomial δ (for a proof see [L_1], p. 237). If, moreover, Σ is (-1)-amphicheiral, it follows from Theorem 1 that γ has property P_2. This completes the proof of Theorem 2. □

§4. Explicit examples

In this section, which is purely number-theoretical, we show that there exist infinitely many irreducible Alexander polynomials of low degree having property P_1 but not P_2.

I. *The quadratic case*

PROPOSITION 3. *Let p be an odd prime, D the square-free part of* $4p+1$, *and*

$$\gamma(X) = -pX^2 + (2p+1)X - p.$$

Then γ is irreducible. Moreover:

(1) *γ has property P_1 if and only if all prime factors of D are congruent to* 1 *modulo* 4;
(2) *γ fails to have property P_2 if and only if the fundamental unit of $\mathbb{Q}(\sqrt{D})$ has norm* $+1$.

Proof. The discriminant $4p+1$ of γ is not a square, since it is congruent to 5 modulo 8. Hence γ is irreducible.

(1) As $K=\mathbb{Q}(\sqrt{D})$, it is clear that P_1 holds if and only if the equation

$$x^2-Dy^2=-1 \tag{4.1}$$

can be solved with $x, y\in\mathbb{Q}$. A local calculation and the Hasse–Minkowski theorem show that this is the case if and only if all prime factors of D are congruent to 1 modulo 4. (In fact this is a well-known result on sums of two squares.)

(2) This is an immediate consequence of Proposition 2, since $|\gamma(0)|=p$ and $K/\mathbb{Q}$ is Galois. □

EXAMPLES. As is well-known, the fundamental unit of $\mathbb{Q}(\sqrt{D})$ has norm $+1$ if and only if the period of the continued fraction expansion of $\sqrt{D}$ is even.

There is a very efficient algorithm for determining that period (see [Si], p. 296; and [P], §26, pp. 102–103, for a useful refinement). In point of fact the fundamental unit itself is detected by this procedure, which involves a computer calculation whose only difficulty is the number of digits to be handled (for $D=991$, already thirty digits are required!). The two smallest examples[(1)] illustrating Proposition 3 are:

$$p=367; \qquad D=13\cdot 113; \qquad \eta=56+3\delta$$

$$p=379; \qquad D=37\cdot 41; \qquad \eta=19+\delta$$

(We denote by η the fundamental unit of $\mathbb{Q}(\sqrt{D})$, and $\delta=(1+\sqrt{D})/2$.)

Remark. In these examples, D is never a prime. This follows from an elementary result, which will be used again later:

LEMMA 4. *Suppose D is a prime congruent to* 1 *modulo* 4. *Then equation* (4.1) *can be solved with $x, y\in\mathbb{Z}$. Hence the fundamental unit of $\mathbb{Q}(\sqrt{D})$ has norm* -1.

A proof can be found in [Mo], Chap. 8. The idea is to start from the fundamental solution of the Pell equation $t^2-Du^2=1$. The assumptions on D enable one to write

$$\frac{t-1}{2}=x^2 \quad\text{and}\quad \frac{t+1}{2}=Dy^2,$$

with $x, y\in\mathbb{Z}$. Then (x, y) is a solution of (4.1).

---

(1) A complete list with $p\leq 50{,}000$ is available on request.

II. *Proof of Theorem* 3

Let τ be any root of the polynomial

$$\gamma(X) = -pX^4 + (2p+1)X^2 - p.$$

As the other roots are $-\tau$ and $\pm 1/\tau$, we see that $K = \mathbb{Q}(\tau)$ is a Galois extension of $\mathbb{Q}$. Moreover, K contains $\mathbb{Q}(\tau^2) = \mathbb{Q}(\sqrt{D})$, where as above *we denote by D the square-free part of* $4p+1$. Since p is odd, $4p+1$ is congruent to 5 modulo 8, hence $D \neq 1$. the fixed field of the involution $\tau \mapsto 1/\tau$ is the field $\mathbb{Q}(\sigma)$, with $\sigma = \tau + 1/\tau = \sqrt{(4p+1)/p}$. From this we see that $K/\mathbb{Q}$ is an extension of degree 4 (whence γ is irreducible), with Galois group $\mathbb{Z}/2 \times \mathbb{Z}/2$. Therefore K contains three quadratic subfields:

$$\begin{tikzcd}
 & K = \mathbb{Q}(\tau) \arrow[dl, dash] \arrow[d, dash] \arrow[dr, dash] & \\
k_1 = \mathbb{Q}(\sqrt{p}) \arrow[dr, dash] & k_2 = \mathbb{Q}(\sqrt{D}) \arrow[d, dash] & k_3 = \mathbb{Q}(\sigma) \arrow[dl, dash] \\
 & \mathbb{Q} &
\end{tikzcd}$$

It is useful to observe that the involution $\tau \mapsto 1/\tau$ induces the ordinary conjugation on k_1 and on k_2: $\sqrt{p} \mapsto -\sqrt{p}$, resp. $\sqrt{D} \mapsto -\sqrt{D}$.

(1) *We wish to prove that γ has property P_1.* Now an element $\alpha \in K$ can be written in the form $\alpha = x + y\sqrt{p}$ with $x, y \in \mathbb{Q}(\sigma)$. Therefore we have to show that the equation

$$x^2 - py^2 = -1 \tag{4.2}$$

can be solved with $x, y \in \mathbb{Q}(\sigma)$. Equivalently, we are reduced to showing that the homogeneous equation

$$x^2 - py^2 + z^2 = 0 \tag{4.3}$$

has a non-trivial solution in $\mathbb{Q}(\sigma)$.

By the Hasse–Minkowski theorem for the number field $\mathbb{Q}(\sigma)$ (see for example [C–F], ex. 4.8, p. 359), it will suffice to show that (4.3) can be solved non-trivially in all completions of $\mathbb{Q}(\sigma)$. Since the quadratic form in (4.3) is defined over $\mathbb{Q}$, it is indefinite for each of the two real embeddings of $\mathbb{Q}(\sigma)$. Therefore it suffices to consider the non-archimedean valuations.

If $p \equiv 1 \pmod 4$, we know that p is a sum of two squares; hence (4.3) is already solvable over $\mathbb{Q}$. (By Lemma 4 we know that (4.2) is even solvable over $\mathbb{Z}$.) Thus we may assume without loss of generality that $p \equiv 3 \pmod 4$. Then $pD \equiv 3 \pmod 4$; hence the ideal (2) ramifies in $\mathbb{Q}(\sigma) = \mathbb{Q}(\sqrt{pD})$. *Therefore it is enough to prove that* (4.3) *has a non-trivial solution in all non-archimedean completions of* $\mathbb{Q}(\sigma)$ *whose residue field is of characteristic* $\neq 2$. Indeed, by the product formula ([C–F], ex. 4.5, p. 358), the number of places where a quadratic form in three variables does not represent zero is even; but there is only one prime ideal above (2).

By a well-known result (a special case of the Chevalley–Warning theorem), (4.3) has non-trivial solutions in every finite field. By Hensel's lemma (cf. [C–F], p. 83), these solutions can be lifted over the corresponding completions, provided the characteristic of the residue field is not equal to 2 or p. In addition, the ideal (p) ramifies in $\mathbb{Q}(\sigma) = \mathbb{Q}(\sqrt{pD})$; therefore all we have to show is that (4.3) can be solved $\mathfrak{p}$-adically, where $\mathfrak{p}$ denotes the unique ideal above (p).

Since $(p) = \mathfrak{p}^2$, locally we can write $p = \pi^2\eta$, where π is a uniformizing element and η a $\mathfrak{p}$-adic unit. Now, if we write $Y = \pi y$, we are reduced to showing that

$$x^2 - \eta Y^2 + z^2 = 0$$

has a non-trivial $\mathfrak{p}$-adic solution. Since now η is a unit, the above argument with Hensel's lemma applies. This completes the proof that γ has property P_1.

(2) *Let us examine under what conditions* γ *has property* P_2. In each quadratic subfield k_i of K there is a fundamental unit ε_i. Now since the involution $\tau \mapsto 1/\tau$ acts as the ordinary conjugation on k_1 and k_2, it is clear that γ has property P_3 (a fortiori P_2) if either ε_1 or ε_2 has norm -1. As we saw in Lemma 4, ε_1 has norm -1 if $p \equiv 1 \pmod 4$; and only then, since obviously (4.2) has no rational solution for $p \equiv 3 \pmod 4$. This proves one of the implications in the second assertion of Theorem 3. In order to establish the converse, we first note that the two properties P_2 and P_3 are in fact equivalent in our case, as follows from Proposition 2. Therefore we are reduced to proving the following lemma:

LEMMA 5. *Suppose* ε_1 *and* ε_2 *have norm* $+1$. *Then* γ *fails to have property* P_3.

Proof. The general theory of units in biquadratic fields is fairly well understood (cf. [Kur], [Kub], [N]); but the special shape of the polynomial γ yields some further information, which will be needed. Let U_K be the group of units in the ring of integers $\mathcal{O}_K$. As K is totally real, we choose once for all a real embedding and denote by U_K^+ the free $\mathbb{Z}$-module of rank 3 consisting of all positive units. Correspondingly, we agree that ε_1, ε_2 and ε_3 are elements of U_K^+.

(**a**) A classical argument [Kur] shows that the sub-$\mathbb{Z}$-module $R \subset U_K^+$ generated by ε_1, ε_2 and ε_3 is of finite index in U_K^+. *For if $\eta \in U_K$ is any unit then $\eta^2 \in R$.* Indeed, let η' be the conjugate of η above k_1. Then

$$N_{K/k_1}(\eta) = \eta\eta' = \pm\varepsilon_1^a,$$

and similarly:

$$\eta\bar{\eta}' = \pm\varepsilon_2^b, \qquad \eta\bar{\eta} = \pm\varepsilon_3^c \quad (a, b, c \in \mathbb{Z}).$$

Hence $\eta^2 = \pm\, \eta^2(\eta\eta'\bar{\eta}\bar{\eta}') = \; = \varepsilon_1^a\varepsilon_2^b\varepsilon_3^c \in R$.

Remark. This argument shows that the index $J = [U_K^+ : R]$ is in fact a divisor of 8. Kuroda [Kur] has shown that, in the general case, there are seven essentially distinct possibilities and that every divisor of 8 can occur. In our present case, however, J is always equal to 2, since we prove below that U_K^+ *is generated by* ε_1, ε_2 *and* $\sqrt{\varepsilon_3}$.

(**b**) *Suppose now $\eta\bar{\eta} = \pm 1$ for some unit η; then η^2 belongs to the submodule $R' \subset R$ which is generated by ε_1 and ε_2.* Indeed, we have just seen that $\eta^2 = \varepsilon_1^a\varepsilon_2^b\varepsilon_3^c$; in addition $\varepsilon_3 = \bar{\varepsilon}_3$. From the assumption $\eta\bar{\eta} = \pm 1$ we therefore get: $1 = \eta^2\bar{\eta}^2 = \varepsilon_3^{2c}$, which is possible only if $c = 0$.

(**c**) Suppose γ has property P_3, i.e. there exists a unit $\eta \in U_K^+$ such that $\eta\bar{\eta} = -1$. Then $\eta \notin R'$, since by assumption $\varepsilon_1\bar{\varepsilon}_1 = \varepsilon_2\bar{\varepsilon}_2 = +1$. Further we know, by (**b**) above, that η^2 is of the form $\varepsilon_1^a\varepsilon_2^b$ with $a, b \in \mathbb{Z}$. Since $\eta \notin R'$, we see that a and b are not both even. This implies that at least one of the numbers ε_1, ε_2 and $\varepsilon_1\varepsilon_2$ is a square in K. *Therefore the lemma will be proved once we show that none of the numbers ε_1, ε_2 and $\varepsilon_1\varepsilon_2$ is a square in K.*

(**d**) We consider first ε_2. If it were a square in K, there would exist $\alpha, \beta \in k_2$ such that $\varepsilon_2 = (\alpha + \beta\sqrt{p})^2 = (\alpha^2 + p\beta^2) + 2\alpha\beta\sqrt{p}$. Of course $\beta \neq 0$, since ε_2 is not a square in k_2. But the coefficient of $\sqrt{p}$ must vanish, hence $\alpha = 0$. Thus we get: $\varepsilon_2 = p\beta^2$, with $\beta \in k_2$. This is impossible, since p does not ramify in $k_2 = \mathbb{Q}(\sqrt{4p+1})$. (One can also proceed as in (**g**) below: β is in fact an element of $\mathcal{O}_{k_2}$, and p does not divide the unit ε_2.) We have shown that ε_2 *is not a square in K.*

(**e**) Let us examine ε_1. As $p \equiv 3 \pmod 4$, we can write $\varepsilon_1 = a_1 + b_1\sqrt{p}$ with $a_1, b_1 \in \mathbb{Z}$. *We claim that b_1 is odd.* To see that, it suffices to repeat the argument by which one proves Lemma 4: if b_1 were even, the equality $a_1^2 - pb_1^2 = 1$ would imply

$$uv = p\left(\frac{b_1}{2}\right)^2,$$

where

$$u = \frac{|a_1| - 1}{2} \quad \text{and} \quad v = \frac{|a_1| + 1}{2}$$

are coprime integers. Since p is a prime, either u or v is a square. In either case we get a contradiction: if $u=s^2$ and $v=pt^2$, then $s^2-pt^2=u-v=-1$; hence $s+t\sqrt{p}\in k_1$ would be a unit of norm -1. If $v=s^2$ and $u=pt^2$, then $s^2-pt^2=v-u=1$, and $1<|s|<|a_1|$. This is impossible, for the fundamental unit ε_1 corresponds to a solution of the Pell equation $s^2-pt^2=1$ for which $|s|>1$ is minimal.

(f) We put $\rho=\sqrt{p}$, $\delta=(1+\sqrt{D})/2$. As $D\equiv 1 \pmod 4$, one checks easily that $\mathcal{O}_K$ is the free $\mathbb{Z}$-module with basis $\{1, \rho, \delta, \rho\delta\}$. (This follows also from [L], chap. 3, §3, prop. 17.) Thus any element $\xi\in\mathcal{O}_K$ can be written in the form $\xi=\alpha+\beta\rho$ with $\alpha, \beta\in\mathcal{O}_{k_2}$. Then ξ^2 takes the form $(\alpha^2+p\beta^2)+2\alpha\beta\rho$. On writing $\alpha\beta=a+b\delta$ with $a, b\in\mathbb{Z}$, we reach the following conclusion: *when ξ^2 is expressed in the $\mathbb{Z}$-base $\{1, \rho, \delta, \rho\delta\}$, the coefficients of ρ and $\rho\delta$ are even.*

(g) Putting **(e)** and **(f)** together, it is immediate that $\varepsilon_1=a_1+b_1\rho$ *is not a square in K*, since b_1 is odd. Finally, let us write $\varepsilon_2=a_2+b_2\delta$, with $a_2, b_2\in\mathbb{Z}$; the coefficients of ρ and $\rho\delta$ in the product $\varepsilon_1\varepsilon_2$ are then respectively b_1a_2 and b_1b_2. If $\varepsilon_1\varepsilon_2$ were a square in K, these integers would have to be even. But b_1 is odd; hence both a_2 and b_2 should be even. This is clearly not the case, since ε_2 is not divisible by 2. This shows that $\varepsilon_1\varepsilon_2$ *is not a square in K* and completes the proof of the lemma. □

Remark. In **(a)** above it is claimed that U_K^+ is generated by ε_1, ε_2 and $\sqrt{\varepsilon_3}$. In view of the results gathered so far, it is enough to prove that ε_2 is a square. Now the situation we are in is quite exceptional in that the fundamental unit ε_3 is given by an explicit formula! Indeed let

$$\eta_3=(8p+1)+4\sqrt{p(4p+1)}. \tag{4.4}$$

It is a simple exercise to show that $(8p+1, 4)$ is the fundamental solution of the Pell equation $x^2-p(4p+1)y^2=1$. Hence $\eta_3=\varepsilon_3$ if $4p+1$ is square-free; otherwise $\eta_3=\varepsilon_3^{\nu}$ for some $\nu\in\mathbb{N}$. Moreover, η_3 is the square of

$$\sqrt{\eta_3}=2\sqrt{p}+\sqrt{4p+1}\in K \tag{4.5}$$

Furthermore, ν is necessarily odd, since $\sqrt{\eta_3}$ does not lie in k_3. Hence in all cases ε_3 is a square, and $J=2$.

It is a firmly established tradition that unit computations in a number field culminate in the determination of the class number. As $J=2$, one has the following formula, ([Kub], Satz 5, p. 80):

$$H=\tfrac{1}{2}h_1h_2h_3, \tag{4.6}$$

in which h_i (resp. H) denotes the class number of the field k_1 (resp. K). We see that the product $h_1h_2h_3$ is always even. This is not surprising; indeed, using (4.4) or (4.5), one shows easily that every prime factor of D is the square of a non-principal ideal of k_3, and therefore accounts for a factor 2 in h_3.

Note. The proof of Theorem 3 shows that there exist infinitely many polynomials of degree four having the required properties. For the quadratic case we do not know whether the constructed family of polynomials is infinite (but we believe so).

REFERENCES

[B] BOURBAKI. *Algèbre.* Chapitre 9, Hermann, Paris, 1959.

[C–F] J. W. S. CASSELS and A. FRÖHLICH, *Algebraic Number Theory*, Academic Press, London, 1967.

[C–G] A. J. CASSON and C. McA. GORDON, *On slice knots in dimension three*, Proc. Symp. Pure Math. *32* (1978), 39–54.

[C] D. CORAY, *Polynômes d'Alexander de terme constant 1*, notes manuscrites, Genève 1981.

[Ha] J. C. HAUSMANN, *Knot Theory*, Springer Lecture Notes no 685, 1977.

[Hi] J. A. HILLMAN, *Reflections and Hyperbolic Concordance of Simple Knots*, Preprint, 1981.

[K] M. KERVAIRE, *Knot cobordism in codimension two*, Springer Lecture Notes no 197, Manifolds Amsterdam 1970.

[Kub] T. KUBOTA, *Über den bizyklischen biquadratischen Zahlkörper*, Nagoya Math. J., *10* (1956), 65–85.

[Kur] S. KURODA, *Über den Dirichletschen Körper*, J. Faculty Sci. Imp. Univ. Tokyo, section I, Vol. *4*, part. 5 (1943), 383–406.

[L] S. LANG, *Algebraic Number Theory*, Addison-Wesley, Reading, 1970.

[L_1] J. LEVINE, *Knot cobordism groups in codimension two*, Comment. Math. Helv. *44* (1969) 229–244.

[L_2] J. LEVINE, *Invariants of knot cobordism*. Inventiones Math. *8* (1969), 98–110.

[L_3] J. LEVINE, *Knot Modules I*, Transactions A.M.S., Vol. 229, pp. 1–50.

[Mic] F. MICHEL, *Inversibilité des noeuds et idéaux ambiges*, C.R. Acad. Sc. Série A, *290* (1980), 909–912.

[Mil] J. MILNOR, *On isometries of inner product spaces*, Inventiones Math. *8* (1969), 83–97.

[Mo] L. J. MORDELL, *Diophantine Equations*, Academic Press, London, 1969.

[N] T. NAGELL, *Sur quelques questions dans la théorie des corps biquadratiques*, Arkiv för Matematik, *4* (1962), 347–376.

[P] O. PERRON, *Die Lehre von den Kettenbrüchen*, Teubner, Leipzig, 1913.

[Si] W. SIERPIŃSKI, *Elementary Theory of Numbers*, Państwowe Wydawnictwo Naukowe, Warsaw, 1964.

[St] N. W. STOLTZFUS, *Unraveling the integral knot concordance group*, Memoirs of the A.M.S. no 192, (1977).

[T] H. F. TROTTER, *On S-equivalence of Seifert matrices*, Inventiones Math. *20* (1973), 173–207.

Université de Genève
Section de Mathématiques
Case Postale 124
CH-1211 Genève 24

Received May 24, 1982