Math. Proc. Camb. Phil. Soc. (1981), **90**, 495
Printed in Great Britain

The factorization of simple knots

BY E. BAYER, J. A. HILLMAN*† AND C. KEARTON†
University of Geneva and University of Durham

(*Received* 19 *December* 1980)

Abstract. For high-dimensional simple knots we give two theorems concerning unique factorization into irreducible knots, and provide examples to show that the hypotheses are necessary in each case.

0. *Introduction*

The purpose of this paper is to collate and extend the known results on the factorization of high dimensional knots. By an *n-knot* we mean an oriented smooth or locally flat PL pair (S^{n+2}, Σ^n), where Σ^n is homeomorphic to the n-sphere S^n. The sum $k+l$ of two n-knots k and l is obtained by excising the interior of a tubular neighbourhood of a point on each Σ^n and identifying the boundaries of the resulting knotted ball pairs so that the orientations match up. A knot k is *irreducible* if it cannot be written as the sum of two non-trivial knots. It is a result of H. Schubert (**16**) that for $n = 1$, every knot factorizes into finitely many irreducibles, and that factorization is unique (up to the order of the factors).

Given an n-knot k, the *exterior* K is the closed complement of a tubular neighbourhood of Σ^n. The knot k is *simple* if K has the homotopy $[(n-1)/2]$-type of a circle; that is $\pi_1(K) \cong \pi_1(S^1)$ for $1 \leqslant i \leqslant (n-1)/2$. For $n \geqslant 3$, this is the most that can be asked without making k trivial (see (**11**, **12**)). The knot k is *fibred* if K is fibred over the circle, and we let $\tilde{K}$ denote the infinite cyclic cover of K.

In Section 1 we give a short proof that every simple n-knot, $n \geqslant 3$, factorizes into finitely many irreducibles. A more general result was published by A. B. Sosinskii in (**18**), but note the assertion of T. Maeda in (**14**).

Let k be a simple $(2q-1)$-knot, $q \geqslant 2$. There are two ways of classifying such knots in terms of algebraic invariants. The first of these, due to J. Levine, is in terms of the S-equivalence class of the Seifert matrix of k; details may be found in (**12**). The second method uses the Blanchfield duality pairing, $\langle , \rangle$: $H_q(\tilde{K}) \times H_q(\tilde{K}) \to \Lambda_0/\Lambda$, where $\Lambda = \mathbb{Z}[t, t^{-1}]$, Λ_0 is the field of fractions of Λ, and $H_q(\tilde{K})$ is regarded as a Λ-module. Details of this method may be found in (**7**, **8**, **20**, **21**).

Each such knot k has associated with it a quadratic form, as outlined in Section 2. If this form is definite, then k is said to be *definite*. The knot k is fibred if and only if the leading coefficient of its Alexander polynomial is ± 1; this follows easily from the results of R. H. Crowell (**3**) and W. Browder and J. Levine (**2**). In Section 2 we show

* Supported by a Research Grant from the Science Research Council of Great Britain.
† Recipients of a European Short Visit Grant from the Science Research Council of Great Britain.

0305-0041/81/0000-8840 $03.50 © 1981 Cambridge Philosophical Society

that for $q \geqslant 3$, every fibred definite knot factorizes uniquely into irreducibles. Sections 3–6 are devoted to showing that each of the hypotheses $q \geqslant 3$, fibred, and definite are necessary for this result.

Next we turn our attention to simple $2q$-knots, $q \geqslant 4$, for which $H_q(\tilde{K})$ is finite of odd order. Such knots have been classified by S. Kojima (10) in terms of a quadratic pairing $[\,,\,]: H_q(\tilde{K}) \times H_q(\tilde{K}) \to \mathbb{Q}/\mathbb{Z}$ together with an isometry t; the pair $([\,,\,], t)$ is called the *Levine pairing* of k. In Section 7 we outline a unique factorization theorem for a certain subclass of these knots, details of which appear in (6), and in Section 8 we give examples to show that factorization is not in general unique.

1. *Finite factorization of simple knots*

Let k be a simple n-knot and define $g(k)$ in the following way. If $n = 2q-1$, then $g(k) = \dim_{\mathbb{Q}} H_q(\tilde{K};\mathbb{Q})$. If $n = 2q$, let $T_q(\tilde{K})$ denote the $\mathbb{Z}$-torsion submodule of $H_q(\tilde{K})$; by a result of M. A. Kervaire (9), $T_q(\tilde{K})$ is finite of order $|T_q(\tilde{K})|$. We set

$$g(k) = \dim_{\mathbb{Q}} H_q(\tilde{K};\mathbb{Q}),\ h(k) = |T_q(\tilde{K})|.$$

THEOREM 1·1. *Let k be a simple n-knot, $n \geqslant 3$. Then k factorizes into finitely many irreducible knots.*

Proof. If $n = 2q-1$, then $g(k) = 0 \Leftrightarrow H_q(\tilde{K};\mathbb{Q}) = 0 \Leftrightarrow H_q(\tilde{K};\mathbb{Z}) = 0$, since the latter is $\mathbb{Z}$-torsion-free (see (7)) $\Leftrightarrow k$ is unknotted (see (7, 8)).

If $n = 2q$, then $g(k) = 0$ and $h(k) = 1 \Leftrightarrow H_q(\tilde{K};\mathbb{Q}) = 0$ and

$$T_q(\tilde{K}) = 0 \Leftrightarrow H_q(\tilde{K};\mathbb{Z}) = 0 \Leftrightarrow H_q(\tilde{K};\mathbb{Z}) = 0 = H_{q+1}(\tilde{K};\mathbb{Z}) \Leftrightarrow K$$

is a homotopy circle $\Leftrightarrow k$ is unknotted (see (11)).

Furthermore, it is clear that $g(k+l) = g(k) + g(l)$ and $h(k+l) = h(k)h(l)$.

The result follows at once.

2. *Unique factorization of fibred definite simple $(2q-1)$-knots, $q \geqslant 3$*

Let k be a simple $(2q-1)$-knot, and let A be a Seifert matrix of k. By a result of Trotter (19), A is S-equivalent to a non-singular matrix, and so we may assume that A is non-singular. Furthermore, any non-singular matrix which is S-equivalent to A is congruent to A over the rational numbers. Set $S = A + A'$, $T = A^{-1}A'$, and note that $T'ST = AA'^{-1}(A+A')A^{-1}A' = A' + A = S$. If $A_1 = P'AP$, then

$$S_1 = A_1 + A_1' = P'SP, \quad \text{and} \quad T_1 = A_1^{-1}A_1' = P^{-1}TP.$$

Thus k determines a quadratic space V together with an isometry τ, represented by the pair (S, T). The knot is *definite* if V is definite.

If k is fibred, then $\det A = \pm 1$, since $\det A$ is the leading coefficient of the Alexander polynomial $\det(tA + (-1)^q A')$. If $q \geqslant 3$, then the converse is true by the results of R. H. Crowell (4) and W. Browder and J. Levine (2). Moreover, any non-singular matrix which is S-equivalent to A is congruent to A over the integers. Thus a fibred knot gives rise to a quadratic lattice L and isometry τ represented by (S, T).

Note that

$$S = A + A' = A + AT = A(I+T),$$

so $A = S(I+T)^{-1}$. Thus given (S, T) we can recover the Seifert matrix A.

By the results of J. Levine (12), the isotopy class of k determines and is determined by the S-equivalence class of A, when $q \geqslant 2$. If k is fibred, this reduces to the integral congruence class of A (where A is non-singular).

THEOREM 2·1. *Let k be a fibred definite simple $(2q-1)$-knot, $q \geqslant 3$. Then k factorizes uniquely into irreducible knots.*

Proof. Let L be the quadratic lattice of k. Since L is definite, it has a unique orthogonal decomposition into indecomposable sublattices by a theorem of Eichler (see (3), p. 363). Say $L = L_1 \perp \ldots \perp L_r$. Now L can be regarded as a Λ-module via the action of the isometry τ. (Recall that $\Lambda = \mathbb{Z}[t, t^{-1}]$.) But $L = \tau L = \tau L_1 \perp \ldots \perp \tau L_r$ is another orthogonal splitting of L into indecomposable sublattices, so the action of t is to permute the L_i. Thus L splits orthogonally as $L = L'_1 \perp \ldots \perp L'_m$, where each L'_i is a Λ-module which is irreducible in the sense that it cannot be written as the orthogonal sum of two non-trivial Λ-modules. Moreover, this splitting is unique.

Choosing $\mathbb{Z}$-bases of each L'_i we can assume that S, T have block diagonal form:

$$S = \begin{pmatrix} S_1 & & \\ & \ddots & \\ & & S_m \end{pmatrix}, \quad T = \begin{pmatrix} T_1 & & \\ & \ddots & \\ & & T_m \end{pmatrix}$$

and hence

$$A = \begin{pmatrix} A_1 & & \\ & \ddots & \\ & & A_m \end{pmatrix}$$

also has block diagonal form. Now

$$\det(A + (-1)^q A') = \prod_{i=1}^{m} \det(A_i + (-1)^q A'_i),$$

and so for each i we see that $A_i + (-1)^q A'_i$ is unimodular. Thus by (12), A_i is a Seifert matrix of a simple $(2q-1)$-knot k_i, and $k = k_1 + \ldots + k_m$. Because L'_i is unique and indecomposable, k_i is unique and irreducible, and the result is proved. ∎

3. *Non-unique factorization of fibred simple $(2q-1)$-knots), $q \geqslant 3$*

We shall reformulate the proof of [(1); Section 1] using Blanchfield forms instead of Seifert matrices. There is a bijection between the isotopy classes of simple $(2q-1)$-knots, $q \geqslant 3$, and the isometry classes of $(-1)^{q+1}$-Blanchfield forms (see (7, 8)). Therefore it suffices to prove that factorization is not unique for $(-1)^{q+1}$-Blanchfield forms.

Let $\lambda \in \mathbb{Z}[t]$ be such that $\lambda(1) = \pm 1$, $\lambda(t) = t^{\deg \lambda} \lambda(t^{-1})$. Let $R = \Lambda/(\lambda) = \mathbb{Z}[\tau, \tau^{-1}]$, where τ is a root of λ. Define an involution $\bar{t} = t^{-1}$ in Λ, which induces the involution $\bar{\tau} = \tau^{-1}$ in R.

Let H be the standard hyperbolic $(+1)$-Blanchfield form:

$$H: (Re \oplus Rf) \times (Re \oplus Rf) \to R$$

$$H(e, e) = H(f, f) = 0, \quad H(e, f) = H(f, e) = 1.$$

Let u be a unit of R such that $\bar{u} = u$. We denote by $\langle u\rangle \perp \langle -u\rangle$ the $(+1)$-Blanchfield form

$$(Rx \oplus Ry) \times (Rx \oplus Ry) \to R$$

$$x\cdot x = u, \quad y\cdot y = -u, \quad x\cdot y = y\cdot x = 0.$$

Then we claim that $\langle u\rangle \perp \langle -u\rangle \cong H$.

To see this, note that $1 = \alpha + \bar{\alpha}$ with $\alpha = 1/(1-\tau) \in R$; $1-\tau$ is a unit of R because $\lambda(1) = \pm 1$.

Let $e = x+y, f' = y$. Then $e\cdot e = 0, e\cdot f' = f'\cdot e = -u, f'\cdot f' = -u$. Set $f'' = f' - \alpha e$; we have $e\cdot f'' = f''\cdot e = -u$, and $f''\cdot f'' = -u + \alpha u + \bar{\alpha} u = 0$. Finally, let $f = -u^{-1} f''$; then $e\cdot f = f\cdot e = 1$. So $\langle u\rangle \perp \langle -u\rangle$ is isometric to H.

Therefore $\langle 1\rangle \perp \langle -1\rangle$ is isometric to $\langle u\rangle \perp \langle -u\rangle$ for any unit u of R such that $\bar{u} = u$.

In order to get a counter-example to unique factorization, it suffices to find a unit u such that $\langle 1\rangle \ncong \langle u\rangle$, $\langle -1\rangle \ncong \langle u\rangle$. Such an example is given in [(1); Section 1] for $\lambda = \phi_{15}$, the cyclotomic polynomial corresponding to the 15th roots of unity, and $u = \tau + \tau^{-1}$.

For the (-1)-Blanchfield form case, note that in $R = \Lambda/(\phi_{15})$, $v = \tau - \bar{\tau}$ is a unit. Therefore $\langle v\rangle \perp \langle -v\rangle$ is a (-1)-Blanchfield form, and we have

$$\langle v\rangle \perp \langle -v\rangle \cong \langle vu\rangle \perp \langle -vu\rangle$$

$$\langle v\rangle \ncong \langle vu\rangle, \quad \langle -u\rangle \ncong \langle vu\rangle,$$

with $u = \tau + \tau^{-1}$.

In each case, the Alexander polynomial of the corresponding simple $(2q-1)$-knot is ϕ_{15}^2, of which the leading coefficient is 1. Thus, as in Section 2, these knots are fibred.

4. *Non-unique factorization of definite simple* $(4q+1)$*-knots*, $q \geqslant 1$

As in Section 3, it will suffice to give an example of a suitable Blanchfield form with several distinct factorizations. In fact our example will rely upon the possible non-uniqueness of factorization of the underlying knot module as a direct sum of modules. (The examples above were a little more subtle in that the underlying modules were all free as modules over the ring $\Lambda/(\phi_{15})$, as this ring is a principal ideal domain.)

Let $\theta = 13t - 25 + 13t^{-1}$. The ring $R = \Lambda/(\theta)$ is isomorphic to $\mathbb{Z}[\gamma, \frac{1}{13}]$ where $\gamma = (-1+\sqrt{-51})/2$ is the image of $13(t-1)$. Since $\theta(t^{-1}) = \theta(t)$, the involution of Λ induces an involution of R, which is just complex conjugation, and which we denote by an overbar. Since $\theta(1) = 1$, any finitely generated R-module which supports a non-singular ϵ-Hermitian pairing may be regarded as a knot module, and an ϵ-Hermitian pairing on such a module determines an ϵ-Hermitian form via the inclusion

$$R = \Lambda/(\theta) \cong \theta^{-1}\Lambda/\Lambda \subset \Lambda_0/\Lambda.$$

Let J be the R-ideal generated by 3 and $\sqrt{-51}$. Then $J = \bar{J}$ and $J\bar{J} = J^2 = (3)$, so $b_J(j,k) = j\bar{k}/3$ for all j, k in J determines a $(+1)$-Blanchfield form on the knot module J.

Let $B = b_J \perp b_J$, and let

$$e = ((18+\sqrt{-51})/13,\quad (9+\sqrt{-51})/13)$$
$$f = ((9-\sqrt{-51})/13,\quad (-18+\sqrt{-51})/13).$$

Then $B(e,e) = B(f,f) = 1$ and $B(e,f) = 0$, so B is isometric to $b \perp b$, where $b\colon R \times R \to R$ is the $(+1)$-Blanchfield form on the knot module R given by $b(r,s) = r\bar{s}$ for all r,s in R. We shall show that J is not a principal ideal, so that it is not isomorphic to R, and hence that these factorizations of B are distinct.

Suppose that J is principal. Then we may suppose that it is generated by an element $\alpha = A + B\gamma$ of $S = \mathbb{Z}[\gamma]$, the ring of integers of $\mathbb{Q}(\sqrt{-51})$, and that α is not divisible in S by γ or $\bar{\gamma}$, since they are units in R. Since 3 belongs to J, α divides 3 in R and so divides $3 \cdot 13^k$ in S, for some large k. Similarly α divides $\sqrt{-51}\cdot 13^l$ in S, for some large l. Therefore $\alpha\bar{\alpha} = A^2 + AB + 13B^2$ divides $9\cdot 13^{2k}$ and $51 \cdot 13^{2l}$ in $\mathbb{Z}$, and hence divides $3\cdot 13^m$ in $\mathbb{Z}$ for some large m. If 13 divides $\alpha\bar{\alpha}$ in $\mathbb{Z}$ then either γ or $\bar{\gamma}$ divides α in S, since $13 = \gamma\bar{\gamma}$ and (γ) is a prime ideal as $S/(\gamma) \cong \mathbb{Z}/(13)$. As we have assumed this is not the case, $\alpha\bar{\alpha}$ must divide 3. Since $R/J \cong \mathbb{Z}/(3)$, J is a proper ideal, and so

$$A^2 + AB + 13B^2 = \alpha\bar{\alpha} = 3.$$

This is clearly impossible and so J cannot be principal. (This example was discussed in greater detail in (5), where it was indicated how other examples with knot module annihilated by an irreducible knot polynomial δ might be sought whenever δ is such that $\delta = \bar{\delta}$ and $\Lambda/(\delta)$ contains a non-principal ideal I such that $I\bar{I}$ is principal.)

Since any real quadratic space of rank 2 with an isometry whose characteristic polynomial has complex roots (such as $\theta(t)$) must be definite, any simple $(4q+1)$-knot with Blanchfield form $B = b \perp b = b_J \perp b_J$ is a definite knot with two distinct factorizations into irreducible knots.

5. *Non-unique factorization of definite simple* $(4q-1)$*-knots,* $q \geqslant 2$

As in Sections 3 and 4, it suffices to show that factorization is not unique for definite (-1)-Blanchfield forms. Let $\lambda(t) = 53t^8 - 105t^4 + 53$. Then λ is irreducible over $\mathbb{Q}$ (this can be checked by computing the roots of λ). Let

$$K = \mathbb{Q}[t]/(\lambda) = \mathbb{Q}(\tau),\quad R = \mathbb{Z}[t,t^{-1}]/(\lambda) = \mathbb{Z}[\tau,\tau^{-1}],$$

where τ is a root of λ. Note that R is integrally closed by ((13), Theorem 28·2, p. 93).

We shall follow the same idea as in Section 4. We shall begin by constructing a non-principal ideal I of R. We have

$$N_{K/\mathbb{Q}}(1-\tau) = \tfrac{1}{53}\lambda(1) = \tfrac{1}{53} \in R.$$

Therefore 53 is a unit of R. As $N_{K/\mathbb{Q}}(1-\tau^4) = 1/53^4$, $1-\tau^4$ is also a unit of R. Let $\omega = (1-\tau^4)^{-1} \in R$, and let I be the R-ideal generated by 5 and $\omega + 1$.

Claim 1. I is not principal.

Proof. Let $K_1 = \mathbb{Q}[t]/(53t^2 - 105t + 53) = \mathbb{Q}(\tau^4)$, $R_1 = \mathbb{Z}[\tau^4, \tau^{-4}]$. Then $\omega \in R_1$. Let $I_1 = (5, \omega + 1)$. It is straightforward to check that I_1 and I_1^2 are not principal (use the same method as in Section 4), and that $I_1^3 = (\omega - 9)R_1$: therefore I_1 is of order 3. (In fact, it suffices to prove that I_1 is not principal. The table on p. 101 of (13) implies that I_1 is then of order 3.)

Let $K_2 = \mathbb{Q}[t]/(53t^4 - 105t^2 + 53) = \mathbb{Q}(\tau^2)$, $R_2 = \mathbb{Z}[\tau^2, \tau^{-2}]$, and let $I_2 = (5, \omega + 1)$ be the extension of I_1 to R_2. Using ((13), Section 29, p. 95) we see that R_1 and R_2 are integrally closed. We have: $R \cap K_2 = R_2$, $R_2 \cap K_2 = R_1$. I is the extension of I_2 to R.

The following lemma shows that I_2 and I are also non-principal, of order 3.

LEMMA 5·1. *Let E/F be a quadratic extension of number fields, let A be an integrally closed subring of E which is sent into itself by* Gal(E/F), *and let $B = A \cap F$. Let b be an ideal of B such that $a = bA$ is principal. Then b^2 is principal.*

Proof: Let $\sigma: E \to E$ generate Gal(E/F). We have $a = bA$, therefore $\sigma(a) = a$. But a is principal by hypothesis, so there exists an $x \in E$ such that $a = xA$. Then

$$a^2 = a \cdot \sigma(a) = x \cdot \sigma(x) A.$$

Let $y = x \cdot \sigma(x)$. We have $\sigma(y) = y$, so $y \in F$. Then $b^2 = a^2 \cap F = yB$, so b^2 is principal.

Let $^-$ denote $\mathbb{Q}$-involution of K which sends τ to τ^{-1}. Then

$$I\bar{I} = (25, 5(\omega + 1), \quad 5(\bar{\omega} + 1), 55) = 5R.$$

Let $b_I: I \times I \to R$ be given by $b_I(x, y) = x\bar{y}/5$. Then b_I is a $(+1)$-Blanchfield form.

Let $L = I \oplus I \oplus I$, and define $b_L: L \times L \to R$ to be $b_L = b_I \perp b_I \perp b_I$.

Let $b: R \times R \to R$ be given by $b(x, y) = 53x\bar{y}$. As 53 is a unit of R, b is a $(+1)$-Blanchfield form.

Claim 2. b is an orthogonal summand of b_L.

Proof. Let $e = (10 + (\omega + 1), \omega + 1, 5) \in L$. Direct computation gives $b_L(e, e) = 53$. Then Re is a submodule of L such that $b_L|(Re \times Re) \cong b$ is unimodular, therefore b is an orthogonal summand of b_L.

So $b_L = b_I \perp b_I \perp b_I \cong b \perp b^{\perp}$, and $b_I \ncong b$ because I is not principal by Claim 1. Thus we have proved that the $(+1)$-Blanchfield form b_L has at least two non-equivalent factorizations.

Now we shall change b_L in order to get a definite (-1)-Blanchfield form.

Claim 3. There exists an R-ideal J and a (-1)-Blanchfield form $B: J \times J \to R$ such that $B \otimes_R b_I: JI \times JI \to R$ is a definite (-1)-Blanchfield form.

Claim 3 implies the non-uniqueness of the factorization of definite (-1)-Blanchfield forms. Indeed,

$$B \otimes b_L = B \otimes b_I \perp B \otimes b_I \perp B \otimes b_I \simeq B \otimes b \perp B \otimes b^{\perp}.$$

We have seen that I is non-principal, therefore IJ is not isomorphic to J. So we have $B \otimes b_I \ncong B \otimes b$.

Proof of Claim 3. Let $\alpha = (1 - \tau)^{-1} \in R$. Let $\phi(t) = t^8 \lambda(1 - t^{-1}) \in \mathbb{Z}[t]$: ϕ is the minimal polynomial of α. We have

$$\phi(t) = t^8 - 4t^7 + 854t^6 - 2548t^5 + 3605t^4 - 53 \cdot 56t^3 + 53 \cdot 28t^2 - 8 \cdot 53t + 53.$$

Let

$$\delta = \phi'(\alpha)(1-2\alpha) = -3388\alpha^3(1-\alpha)^3 + 106{\cdot}56\alpha^2(1-\alpha)^2 - 53{\cdot}56\alpha(1-\alpha) + 8{\cdot}53.$$

Let $F = \{x \in K : \bar{x} = x\}$. F has 4 real embeddings $\sigma_1, \sigma_2, \sigma_3, \sigma_4$. It is straightforward to check that δ is positive at two of these embeddings, say σ_1 and σ_2, and negative at σ_3 and σ_4.

Let $\beta = (\tau - \bar{\tau})^2 \in F$: notice that $K = F(\tau - \bar{\tau})$. Denote the Hilbert symbol by $(,)_P$.

There exists an $a \in F$ such that

$$(a, \beta)_P = \begin{cases} -1 & \text{if } P = \sigma_3, \sigma_4 \\ +1 & \text{otherwise} \quad (\text{that is, for } P = \sigma_1, \sigma_2, \text{ or a discrete prime}). \end{cases}$$

To see this, apply Theorem 71:19 and Corollary 71:19*a* of (15) with $T = \{\sigma_3, \sigma_4\}$. Notice that $\beta = -(\tau - \bar{\tau})\overline{(\tau - \bar{\tau})}$, so β is negative at all real embeddings of F.

As $(a, \beta)_P = +1$ for P discrete, there exists an R-ideal J such that $B' : J \times J \to R$ given by $B'(x, y) = ax, \bar{y}$ is a $(+1)$-Blanchfield pairing (see ((13), lemma 2·4·3, p. 81)).

Now $1 - 2\alpha$ is a unit of R. Indeed, $1 - 2\alpha = (\tau + 1)/(\tau - 1)$, and

$$N_{K/\mathbb{Q}}(\tau + 1) = N_{K/\mathbb{Q}}(\tau - 1) = 1/53, \quad \text{so} \quad N_{K/\mathbb{Q}}(1 - 2\alpha) = 1.$$

Define $B : J \times J \to R$ by $B(x, y) = (1 - 2\alpha)^{-1}\, ax, \bar{y}$. We have seen that $1 - 2\alpha$ is a unit, and clearly $\overline{1 - 2\alpha} = -(1 - 2\alpha)$, therefore B is a (-1)-Blanchfield pairing.

It remains to prove that $h = B \otimes b_I$ is definite. To see this, it suffices to show that the extension h_K of h to K is definite. We have

$$h_K : K \times K \to K,\ h_K(x, y) = (1 - 2\alpha)^{-1}\ ax, \bar{y}/5.$$

Since $K = \mathbb{Q}(\alpha)$, we can write $x \in K$ in the form

$$x = \sum_{i=0}^{7} x_i \alpha^i,\ x_i \in \mathbb{Q},$$

and this expression is unique. Define $s : K \to \mathbb{Q}$ by $s(x) = x_7$, as in ((21), p. 239). We have $s(x) = Tr_{K/\mathbb{Q}}(x/\phi'(\alpha))$. (See (21), p. 239), and $s(h_K(x, y)) = S(x, y)$, where S^{-1} is the rational intersection form corresponding to h_K (see (21) and (20): Section 2)).

By definition, h_K is definite if and only if S^{-1} is a definite quadratic form. Clearly S^{-1} is definite if and only if S is definite. We have

$$S(x, x) = s(h_K(x, x)) = Tr_{K/\mathbb{Q}}(ax, \bar{x}/5\delta) > 0$$

if $x \neq 0$, (recall that $\delta = \phi'(\alpha)(1 - 2\alpha)$) because a/δ is totally positive by construction, and $x\bar{x}$ is also totally positive as the involution becomes complex conjugation at every $\mathbb{C}$-embedding of K.

Therefore $S(x, x) > 0$ if $x \neq 0$, so S is positive definite.

6. *Non-unique factorization of* 3-*knots*

Let k be a simple 3-knot, with Seifert matrix S-equivalent to the non-singular matrix A. If A is unimodular, then we say that k is *algebraically fibred*. (If k were a simple $(4q-1)$-knot, $q > 1$, then k would be fibred by the Browder–Levine theorem (2).)

Consider the following matrices.

$$B = \begin{bmatrix} 1 & 0 & -1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & -1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & -1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & -1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & -1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & -1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & -1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \end{bmatrix}$$

$$C = \begin{bmatrix} 1 & -1 & -2 & -3 & -3 & -3 & -2 & -1 \\ 2 & 1 & -1 & -2 & -3 & -3 & -3 & -2 \\ 3 & 2 & 1 & -1 & -2 & -3 & -3 & -3 \\ 3 & 3 & 2 & 1 & -1 & -2 & -3 & -3 \\ 3 & 3 & 3 & 2 & 1 & -1 & -2 & -3 \\ 2 & 3 & 3 & 3 & 2 & 1 & -1 & -2 \\ 1 & 2 & 3 & 3 & 3 & 2 & 1 & -1 \\ 0 & 1 & 2 & 3 & 3 & 3 & 2 & 1 \end{bmatrix}$$

Each matrix possesses the following properties:

(i) $\det(A+A') = 1$;

(ii) $\operatorname{signature}(A+A') = 8$.

In addition we have

(iii) $\det(tB+B') = 1+t-t^3-t^4-t^5+t^7+t^8 = \phi_{30}(t)$;

(iv) $\det(tC+C') = 1-t+t^3-t^4+t^5-t^7+t^8 = \phi_{15}(t)$.

By (12) there exist unique 3-knots k, l, m with Seifert matrices S-equivalent to

$$\begin{pmatrix} B & 0 \\ 0 & B \end{pmatrix}, \quad \begin{pmatrix} C & 0 \\ 0 & C \end{pmatrix}, \quad \begin{pmatrix} B & 0 \\ 0 & C \end{pmatrix}$$

respectively. By (12), we have $k+l = m+m$. Because the signature of a 3-knot must be divisible by 16 (see (12)), it is clear that each of the knots k, l, m is irreducible. All three knots are distinguished by their Alexander polynomials, these being $\phi_{30}(t)\,\phi_{30}(t)$, $\phi_{15}(t)\,\phi_{15}(t)$, $\phi_{30}(t)\,\phi_{15}(t)$ respectively. Finally, the knot $k+l$ is definite and algebraically fibred. Thus the analogue of Theorem 2·1 fails for 3-knots.

7. *Unique factorization of odd semisimple finite 2q-knots, $q \geqslant 4$*

In this section we shall sketch a proof of the following theorem, given in (6).

THEOREM 7·1. *If k is an odd simple $2q$-knot, $q \geqslant 4$, whose knot module $H_q(\tilde{K};\mathbb{Z})$ is semisimple and such that either q is even or $t+1$ acts invertibly, then k has a unique factorization into irreducible knots.*

By means of Kojima's classification of odd simple $2q$-knots, $q \geqslant 4$, we may reduce the proof of this theorem to an argument about the factorization of certain ϵ-Levine pairings (for $\epsilon = (-1)^{q+1}$). We shall first explain the term 'semisimple'.

A finite Λ-module M is the direct sum of its localizations M at the various maximal ideals $\mathfrak{m}$ of Λ. The localization $M_{\mathfrak{m}}$ may be regarded as a module over the $\mathfrak{m}$-adic completion $\Lambda_{\hat{\mathfrak{m}}} = \varprojlim \Lambda/\mathfrak{m}^n$. Let $\mathfrak{m} = (p, g(t))$ where p is a rational prime and $g(t)$ is a monic polynomial in $\mathbb{Z}[t]$ whose image in $\mathbb{Z}/p\mathbb{Z}[t]$ is irreducible. Then the completion $\Lambda_{\hat{\mathfrak{m}}}$ is isomorphic to $S[[T]]$ where $S = \mathbb{Z}_{\hat{p}}[\xi]$ is an unramified extension of the p-adic integers $\mathbb{Z}_{\hat{p}}$, generated by a root of unity ξ such that $g(\xi) \equiv 0$ modulo (p), and where t has image $\xi(1-T)$. (That such an isomorphism exists is a special case of I. S. Cohen's structure theorem for complete regular local rings ((17): p. V–16).) The localization M is semisimple if $T \cdot M_{\mathfrak{m}} = 0$; the module M is semisimple if each such localization is semisimple. Semisimple modules may be recognized by the following criterion. A finite Λ-module M is semisimple if and only if $\operatorname{Ann} M = \Pi_{i=1}^{r}(p_i^{e_i}, g_i)$ where p_i is a rational prime and g_i is congruent modulo $(p_i^{e_i})$ to an irreducible factor of a cyclotomic polynomial in $\mathbb{Z}/p_i^{e_i}[t]$ for $1 \leqslant i \leqslant r$, and where the maximal ideals (p_i, g_i) are all distinct. (This fact is not used in proving the theorem.)

Suppose that the finite knot module M supports an ϵ-Levine pairing

$$[\,,]: M \times M \to \mathbb{Q}/\mathbb{Z}.$$

Then the localizations $M_{\mathfrak{m}}$ and $M_{\mathfrak{n}}$ are orthogonal unless $\mathfrak{n} = \bar{\mathfrak{m}}$. If $\mathfrak{m} \neq \bar{\mathfrak{m}}$ the pairing on $M_{\mathfrak{m}} \oplus M_{\bar{\mathfrak{m}}}$ is determined uniquely by the module structure of $M_{\mathfrak{m}}$. If $\mathfrak{m} = \bar{\mathfrak{m}}$ then the involution of Λ induces involutions on $\Lambda_{\hat{\mathfrak{m}}}$ and S mapping ξ to ξ^{-1} and T to $T/(T-1)$, and the pairing $[\,,]$ determines a pairing

$$\{\,,\}: M_{\hat{\mathfrak{m}}} \times M_{\hat{\mathfrak{m}}} \to S \otimes \mathbb{Q}/\mathbb{Z} = S_0/S$$

which is non-singular, S-linear in its first argument, ϵ-conjugate symmetric

$$(\{n, m\} = \epsilon\overline{\{m, n\}} \text{ for all } m,\, n \text{ in } M)$$

and such that

$$\{Tm, n\} = \{m, (T/(T-1))n\} \quad \text{for all } m,\, n \text{ in } M.$$

If now M is assumed semisimple each localization $M_{\mathfrak{m}}$ is a module over a discrete valuation ring $S = \Lambda_{\hat{\mathfrak{m}}}/(T)$, and so has an essentially unique factorization as a direct sum of (irreducible) cyclic modules. By the remarks above we may assume that M is annihilated by some power of a maximal ideal $\mathfrak{m}$ such that $\bar{\mathfrak{m}} = \mathfrak{m}$.

An ϵ-Levine pairing on such a module is equivalent to a non-singular ϵ-conjugate symmetric pairing into S_0/S which is S-linear in its first argument. For brevity, we shall refer to such a pairing on a finite S-module as an (ϵ-torsion) form. We recall that $S = \mathbb{Z}_{\hat{p}}[\xi]$ where ξ is a root of unity which is not congruent to 1 modulo (p) (since M is a knot module). The extension $S/\mathbb{Z}_{\hat{p}}$ is unramified, so the unique maximal ideal of S is generated by p, and S has an involution which maps ξ to $\bar{\xi} = \xi^{-1}$. The involution is the identity if and only if $\xi = -1$, and in this case p must be odd.

Let $\epsilon - S(p^k)$ denote the ϵ-torsion form with underlying module $S/(p^k)$, generated by $e = 1 + (p^k)$, and with pairing determined by

$$\{e, e\} = 1/p^k \quad \text{if} \quad \epsilon = +1$$

$$\{e, e\} = (\xi - \bar{\xi})/p^k \quad \text{if} \quad \epsilon = -1 \text{ and the involution is nontrivial.}$$

(If $\epsilon = -1$, p is odd, and the involution is trivial then there is no cyclic ϵ-torsion form.)

PROPOSITION 7·2. *If the involution on S is nontrivial then any ϵ-torsion form $M, \{,\}$ is an orthogonal direct sum of copies of $\epsilon - S(p^j)$, for various $j \geqslant 1$.*

COROLLARY 7·3. *If the involution on S is nontrivial, then any ϵ-torsion form is determined up to isometry by its underlying module, and has an essentially unique decomposition into irreducible forms.*

Now let us suppose that the involution on S is trivial, so that $\xi = -1$, $S = \mathbb{Z}_{\hat{p}}$ and p is odd. Let r be the smallest positive integer which is not congruent to a square modulo (p). (In fact we could use any non-quadratic residue instead of r.) Let

$$\widetilde{+1} - S/(p^k)$$

denote the $+1$-torsion form over S whose underlying module is $S/(p^k)$, generated by $f = 1 + (p^k)$, and with pairing determined by $\{f, f\} = r/p^k$. Let H_k denote the -1-torsion form over S whose underlying module is $(S/(p^k))^2$, generated by h and h', and with pairing determined by $\{h, h'\} = 1/p^k$.

PROPOSITION 7·4. *If the involution on S is trivial then any $+1$-torsion form $M, \{,\}$ is an orthogonal direct sum of copies of $+1 - S/(p^j)$ and $\widetilde{+1} - S/(p^j)$ for various $j \geqslant 1$; moreover $+1 - S/(p^j)$ and $\widetilde{+1} - S/(p^j)$ are distinct, but $(+1 - S/(p^j)) \oplus (+1 - S/(p^j))$ is isomorphic to $(\widetilde{+1} - S/(p^j)) \oplus (\widetilde{+1} - S/(p^j))$ for each $j \geqslant 1$. Any -1-torsion form is an orthogonal direct sum of copies of H_j for various j; moreover H_j is irreducible.*

COROLLARY 7·5. *If the involution on S is trivial, any -1-torsion form is determined by its underlying module, and has an essentially unique decomposition into irreducible forms.* ∎

Let $M, \{,\}$ be a $+1$-torsion form whose underlying module is freely generated over $S/(p^k)$ by the elements $m_1, \ldots, m_d$ with $d \geqslant 1$, and suppose that $\{m_i, m_j\} = S_{ij}/p^k$ for some element S_{ij} in S (not necessarily a unit). Let DET$\{,\}$ be the image of det $[S_{ij}]$ in $(S/(p^k))^*/((S/(p^k))^*)^2 = \mathbb{Z}/2\mathbb{Z}$.

COROLLARY 7·6. *There are up to isomorphism two $+1$-torsion forms on a non-trivial free $S/(p^k)$-module M distinguished by the value of* DET$\{,\}$. *Each of these factors is an orthogonal direct sum of cyclic forms and the number of essentially distinct such factorizations is the number of factorizations of* DET$\{,\}$ *as a product of d elements in the group $\mathbb{Z}/2\mathbb{Z}$ (where d is the minimal number of generators of M).*

Theorem 7·1 is an immediate consequence of Corollary 7·3 and Corollary 7·5.

8. *Non-unique factorization of odd finite 2q-knots, $q \geqslant 4$.*

Corollary 7·6 implies that for each odd $q \geqslant 5$ there is an odd finite $2q$-knot k with $H_q(\tilde{K}; \mathbb{Z})$ semisimple and which has more than one factorization into irreducible knots. The example given in (1) (for q odd) is of this nature, having knot module isomorphic to $(\Lambda/(5, t+1))^2$. There is only one maximal ideal to consider, and we may take $p = 5$ and $\xi = -1$. The involution is trivial, and $(\Lambda/(5, t+1))^2$ admits one $(+1)$-torsion form with DET $= [\pm 1]$, the class of a square, and one with DET $= [\pm 2]$, the class of a nonsquare. The example of (1) is the first of these, and has two factorizations as a direct sum of two cyclic forms since $[\pm 1] = [\pm 1]^2 = [\pm 2]^2$; the second has unique factorization since $[\pm 2] = [\pm 1][\pm 2]$.

Uniqueness of factorization can also fail for an odd simple $2q$-knot for each even $q \geqslant 4$, but no such knot can have semisimple knot module. The example given for this case in (1) is as follows. Let e be a fixed generator for the cyclic module $E = \Lambda/(5, (t+1)^2)$ and let $[\,,]$ and $[\,,]'$ be the (-1)-Levine pairings on E determined by $[e, te] = \frac{1}{5} \bmod \mathbb{Z}$ and $[e, te]' = \frac{2}{5} \bmod \mathbb{Z}$ respectively. Suppose that $\phi: E \to E$ is an isometry from $[\,,]$ to $\pm[\,,]'$, sending e to $\phi(e) = ae + bte$ with a, b in $\mathbb{Z}$. Then, mod $\mathbb{Z}$,

$$\begin{aligned}\tfrac{1}{5} &= [e, te] \\ &= \pm[\phi(e), \phi(te)]' \\ &= \pm[ae+bte, ate+bt^2e]' \\ &= \pm[ae+bte, ate-be-2bte]' \\ &= \pm([ae, (a-2b)te]' + [bte, -be]') \\ &= \pm(a^2-2ab+b^2)\cdot\tfrac{2}{5},\end{aligned}$$

which implies that ± 2 is a perfect square modulo 5, which is false. Therefore $[\,,]$ is not isometric to either $[\,,]'$ or $-[\,,]'$.

But the map $\Phi: E^2 \to E^2$, given in matrix form with respect to the basis $\{(e, 0), (0, e)\}$ by

$$\begin{pmatrix} 2 & 2 \\ -2 & 2 \end{pmatrix}$$

is an isometry between $[\,,] \perp -[\,,]$ and $[\,,]' \perp -[\,,]'$. Thus there is a (-1)-Levine pairing on the finite knot module $E^2 = (\Lambda/(5, (t+1)^2))^2$ which has more than one factorization as a sum of irreducible pairings. Of course the underlying knot module is not semisimple, as $T = t+1$ does not act as the zero endomorphism.

REFERENCES

(1) Bayer, E. Factorisation is not unique for higher dimensional knots. *Comm. Math. Helv.* **55** (1980), 583–592.

(2) Browder, W. and Levine, J. Fibering manifolds over a circle. *Comm. Math. Helv.* **40** (1965), 153–160.

(3) Cassels, J. W. S. *Rational quadratic forms*. Academic Press (1978). LMS monograph no. 13.

(4) Crowell, R. The group G'/G'' of a knot group G. *Duke Math. Jour.* **30** (1963), 349–354.

(5) Hillman, J. A. Blanchfield pairings with squarefree Alexander polynomials. *Math. Zeit.* **176** (1981), 551–563.

(6) Hillman, J. A. Finite knot modules and the factorisation of certain simple knots. *Math. Ann.* (to appear).

(7) Kearton, C. Classification of simple knots by Blanchfield duality. *Bull. Amer. Math. Soc.* **79** (1973), 952–955.

(8) Kearton, C. Blanchfield duality and simple knots. *Trans. Amer. Math. Soc.* **202** (1975), 141–160.

(9) Kervaire, M. A. Les nœuds de dimensions supérieures. *Bull. Soc. Math. France.* **93** (1965), 225–271.

(10) Kojima, S. Classification of simple knots by Levine pairings. *Comm. Math. Helv.* **54** (1979), 356–367.

(11) Levine, J. Unknotting spheres in codimension two. *Topology* **4** (1965), 9–16.

(12) Levine, J. An algebraic classification of some knots of codimension two. *Comm. Math. Helv.* **45** (1970), 185–198.

(13) Levine, J. *Algebraic structure of knot modules* (Springer, Lecture Notes in Mathematics, no. 772 (1980)).

(14) MAEDA, T. On a composition of knot groups. II. Algebraic bridge index. *Mathematics Seminar Notes Kobe University* **5** (1977), 457–464.
(15) O'MEARA, O. T. Introduction to quadratic forms. (Springer, 1971).
(16) SCHUBERT, H. Die eindeutige Zerlegbarkeit eines knotens in Primknoten. *S.-B. Heidelberger Akad. Wiss. Math. Nat. Kl.* **3** (1949), 57–104.
(17) SERRE, J. P. *Algèbre locale-multiplicités* (Springer, Lecture Notes in Mathematics, no. 11, 1965).
(18) SOSINSKII, A. B. Decomposition of knots. *Math. USSR-Sb.* **10** (1970), 139–150.
(19) TROTTER, H. F. Homology of group systems with applications to knot theory. *Annals of Math.* **76** (1962), 464–498.
(20) TROTTER, H. F. On *S*-equivalence of Seifert matrices. *Invent. Math.* **20** (1973), 173–207.
(21) TROTTER, H. F. *Knot modules and Seifert matrices* (Springer, Lecture Notes in Mathematics, no. 685, Knot Theory (1978)), pp. 291–299.