INTERTWINING MATRICES FOR NUMBER FIELDS: SUPPLEMENT TO "INTERTWINERS AND THE K-THEORY OF COMMUTATIVE RINGS"

A. J. BERRICK AND M.-F. LIM

Since not all the matrices appearing in [1] Proposition 10.4 are intertwining matrices as claimed, we present a corrected version here. Moreover, with only a little extra work, we then generalize the result from quadratic to arbitrary number fields.

[1] **Proposition 10.4.** *Let A be the ring of integers in the quadratic number field $\mathbb{Q}(\sqrt{\delta})$ of discriminant δ $(\neq -3, -4)$. Suppose that there exist $\alpha, b, n \in \mathbb{Z}$ $(b^2 > 1,\ n \geq 3)$ such that*

$$\delta = \alpha^2 - 4b^n \qquad \text{and} \qquad (\alpha, b) = 1.$$

Thus we may define integers $x_1, x_2, \ldots$ coprime to b by

$$x_1 = 1,\ x_2 = \alpha,\ \ldots \quad x_{k+1} = \alpha x_k - b^n x_{k-1}\,,\ \ldots$$

and choose $r_0, r_{n-1} \in \mathbb{Z}$ to satisfy

$$r_0 x_n + r_{n-1} b^{n-1} = 1.$$

Then, with $u = (\alpha + \sqrt{\delta})/2$,
(a) *the matrix*

$$S_n = \begin{bmatrix} u & -b & 0 & \cdots & 0 & 0 \\ 0 & u & -b & \cdots & 0 & 0 \\ 0 & 0 & u & \ddots & 0 & 0 \\ \vdots & \vdots & \vdots & \ddots & \ddots & \vdots \\ 0 & 0 & 0 & \ddots & u & -b \\ r_0 x_{n-1} b & r_{n-1} b & 0 & \cdots & 0 & r_0 u \end{bmatrix}$$

is an element of $\mathrm{Int}_n A$; and
(b) *if further n is an odd integer, then the element of the ideal class group of A represented by S_n has order n, provided that either:*

- (i) *for every integer β and proper divisor m of n the number $\delta\beta^2 \pm 4b^m$ is not a perfect square; or*
- (ii) *$n | \delta$, and that moreover when $\delta > 0$ then the fundamental unit $(\varepsilon_1 + \varepsilon_2\sqrt{\delta})/2$ of A has $n | \varepsilon_2$.*

Proof. (a) From $u(\alpha - u) = (\alpha^2 - \delta)/4 = b^n$, we obtain inductively that

$$u^k = x_k u - x_{k-1} b^n.$$

That S_n is an intertwiner with determinant u follows readily from the proof of [1] Theorem 9.1 (where $r_1 = r_2 = \cdots = r_{n-2} = 0$).

(b) In the specified cases it is shown in [2] Propositions 1.9, 2.8 that the class obtained in (a) maps under the isomorphism of our Corollary 9.6 (b) to an element of order n. □

For determination of the order of the element of the ideal class group represented by an intertwining matrix, the following result is useful.

Lemma 1. *Let A be a Dedekind domain, and suppose that $S \in \mathrm{Int}_n(A)$. Let r be the greatest integer such that $\det(S)$ is associate in A to an r th power. Then the order of the element represented by S in the ideal class group of A is n/r.*

Proof. Writing $u = \det(S)$, we deduce from [1] Theorem 3.2 that $Au = (A\langle S\rangle)^n$. By definition, the class of the ideal $A\langle S\rangle$ generated by the entries of S has order dividing s in the class group if and only if for some $w \in A$ we have $(A\langle S\rangle)^s = Aw$. By unique divisibility of ideals, this is equivalent to $Au = Aw^r$, where $n = rs$. □

In order to generalize the proposition above, we recall the following notation from [2]. For a number field F with ring of integers A, let $l = [F : \mathbb{Q}]$, and for $u \in A$ let the characteristic equation for u over F be

$$(*) \qquad \sum_{j=0}^{l} (-1)^{l-j} N_j(u) u^j = 0.$$

for some $N_0(u), \ldots, N_l(u) \in \mathbb{Z}$. (In fact, $N_0(u)$ is the norm of u.)

Theorem 2. *Let A be a number ring.*

(a) *Suppose that there exists $u \in A$ such that:*

(i) *the integers $N_0(u)$, $N_1(u)$ are coprime; and*

(ii) *$|N_0(u)|$ is a proper power (say, $|N_0(u)| = b^n$).*

Then the $n \times n$ matrix S given by

$$\begin{bmatrix} u & -b \\ xb & yb + zu \end{bmatrix}$$

when $n = 2$; or, for $n > 2$:

$$S = \begin{bmatrix} u & -b & 0 & \cdots & \cdots & 0 \\ 0 & u & -b & \ddots & \ddots & \vdots \\ \vdots & 0 & u & \ddots & \ddots & \vdots \\ \vdots & \vdots & \vdots & \ddots & \ddots & 0 \\ 0 & 0 & \vdots & \ddots & u & -b \\ xb & yb & 0 & \cdots & 0 & zu \end{bmatrix}$$

(where $x, y, z \in A$ are constructible from the proof) is an intertwining matrix of determinant u.

(b) *The element represented by* S *in the ideal class group has order* n *if and only if* u *is not associate in* A *to a proper power (of exponent dividing* n*).*

Proof. (a) From hypotheses (i), (ii), we have, as ideals in A,

$$A = Ab^{n-1} + AN_1(u),$$

while from $(*)$ and (i)

$$AN_1(u)u \subseteq Ab^n + Au^2.$$

Then multiplying the former equality by u and combining gives

$$Au \subseteq Ab^n + Ab^{n-1}u + Au^2.$$

Iteration yields

$$Au \subseteq Ab^n + Ab^{n-1}u + Au^k$$

for all $k \geq 2$; and so, there are $x, y, z \in A$ with

$$u = xb^n + yb^{n-1}u + zu^n.$$

Thus S has determinant u, and that S is an intertwining matrix again follows from the proof of [1] Theorem 9.1.

(b) This is immediate from the lemma. □

Note that the necessary and sufficient condition in (b) of the above theorem weakens that found in [2] (1.8) (namely, that no lesser power of b than b^n be the norm of an element). Thus, in $\mathbb{Q}(\sqrt{-231})$ for instance, the above theorem detects a nontrivial class of order 3 with $u = (5 + \sqrt{-231})/2$, of norm 4^3; in $\mathbb{Q}(\sqrt{-455})$ the theorem detects a nontrivial class of order 5 with $u = (1 + 3\sqrt{-455})/2$, of norm 4^5. However, in both cases, $b = 4 = N(2)$.

References

[1] A. J. Berrick: Intertwiners and the K-theory of commutative rings, *J. reine angew. Math.* **569** (2004), 55–101.

[2] M. Karoubi & T. Lambre: Quelques classes caractéristiques en théorie des nombres, *J. reine angew. Math.* **543** (2002), 169-186.

Department of Mathematics, National University of Singapore, Singapore 117543, Republic of Singapore

E-mail address: berrick@math.nus.edu.sg

Department of Mathematics, McMaster University, Hamilton, Ontario, Canada

E-mail address: limmf@math.mcmaster.ca