THÉORIE DES NOMBRES
BESANÇON

Années 1996/97-1997/98

Algebraic construction of bilinear forms over $\mathbb{Z}$

M. KRÜSKEMPER

Algebraic construction of bilinear forms over $\mathbb{Z}$

Martin Krüskemper

Abstract. Chapter 8 in [CS] gives algebraic constructions for certain lattices. Some of these constructions used the trace map. In this note we want to show that by applying [S],[W], any bilinear form over $\mathbb{Z}$ with nonzero determinant can be constructed as a scaled trace form of some algebra $A = \mathbb{Z}[X]/(f(X))$ where $f(X) \in \mathbb{Z}[X]$ is monic, irreducible.

Let R be a commutative ring with 1. A bilinear form over R is a pair (M, b) where M is a finitely generated projective R–module and $b : M \times M \to R$ is symmetric bilinear. If M is free and $e_1, \ldots, e_n$ is a basis for M then b can be described by the symmetric $n \times n$ matrix $B = (b(e_i, e_j))$ over R. Conversely any $B \in Sym(n, R)$ defines the bilinear form (R^n, B). The determinant $det(M, b)$ is defined as $det(M, b) = det\,B$. (M, b) is called regular if $det(M, b)$ is a unit in R. We call two forms (M, b) and (M', b') with matrices $B, B' \in Sym(n, R)$ isometric if there exists an invertible $M \in Mat(n, R)$ such that $B = M^t B' M$.

If $\beta : R \to A$ is a ringmorphism such that A is a finitely generated projective R–module and $s \in Hom_R(A, R)$, then the map $(x, y) \in A \times A \to s(xy)$ defines a bilinear form (A, s) over R. More generally, if $\mathcal{I}$ is an ideal in A such that $\mathcal{I}$ is a finitely generated projective R–module then $(x, y) \in \mathcal{I} \times \mathcal{I} \to s(xy)$ defines a bilinear form $(\mathcal{I}, s)$ over R. We call $(\mathcal{I}, s)$ scaled trace form of A/R.

Let $f(X) \in \mathbb{Z}[X]$ be a monic separable polynomial of degree n (in one variable X). Then $A := \mathbb{Z}[X]/(f(X))$ is a free $\mathbb{Z}$–module of rank n with basis $1, X, \ldots, X^{n-1}$. We set $A_{\mathbb{Q}} := A \otimes \mathbb{Q}$. If f is irreducible then $A_{\mathbb{Q}} = Q(A)$ denotes the quotient field of A. Let $Tr : A_{\mathbb{Q}} \to \mathbb{Q}$ denote the trace map which is non–zero. Euler's lemma (see [L] III–1, proposition 2, corollary) implies that we have:

$$A^{\#} := \{c \in A_{\mathbb{Q}} \mid Tr(cA) \subset \mathbb{Z}\} = 1/(f'(X))A.$$

Any $c \in A^{\#}$ defines a symmetric bilinear form (A, Tr_c) where Tr_c maps $(a_1, a_2) \in A \times A$ to $Tr(ca_1a_2)$. Let $N : A_{\mathbb{Q}} \to \mathbb{Q}$ denote the norm map. It is well known (compare [L] III–1) that if $c = c_0/f'(X) \in A^{\#}$, where $c_0 \in A$, then we have $det(A, Tr_c) = (-1)^{n(n-1)/2} N(c_0)$. In particular, if $c \neq 0$ then $det(A, Tr_c) \neq 0$ and the form (A, Tr_c) is regular if c_0 is a unit in the integral closure. More generally, let $\mathcal{I} \subset A$ be an ideal in A and let $c \in (\mathcal{I}^2)^{\#}$. Then we obtain a symmetric bilinear form $(\mathcal{I}, Tr_c)$ if Tr_c maps $(a_1, a_2) \in \mathcal{I} \times \mathcal{I}$ to $Tr(ca_1a_2)$. Note that if $\mathcal{B}$ is an ideal in A then $\mathcal{B}^{\#} = \mathcal{B}^{-1}A^{\#} = 1/(f'(X))\mathcal{B}^{-1}$. If $c = c_0/f'(X)$ where $c_0 \in \mathcal{I}^{-2}$ we have $det(\mathcal{I}, Tr_c) = (-1)^{n(n-1)/2} N(c_0) N(\mathcal{I})^2$. (Compare [CS] page 226.)

An obvious question is the following: Let (M, b) be a scaled trace form of $A/\mathbb{Z}$. If (N, b') is symmetric bilinear such that $(M, b) \otimes \mathbb{Q}$ is isometric to $(N, b') \otimes \mathbb{Q}$, then is

(N, b') also a scaled trace form of $A/\mathbb{Z}$? The following examples show, that the answer to this question is negative:

Examples. (a) Let $d \in \mathbb{Z}$ be not a square and set $A = \mathbb{Z}[\sqrt{d}]$. Let (M, b) be a two-dimensional symmetric bilinear form over $\mathbb{Z}$. Then there exists some $c \in A^{\#}$ such that $(M, b) = (A, Tr_c)$ if and only if there exists a $\mathbb{Z}$-basis m_1, m_2 of M such that the matrix of b with respect to m_1, m_2 is in

$$\{\begin{pmatrix} a & b \\ b & ad \end{pmatrix} | a, b \in \mathbb{Z}, a \neq 0 \text{ or } b \neq 0\}.$$

Proof. Set $\tau := \frac{a\sqrt{d}+b}{2\sqrt{d}}$. We obtain as matrix of (A, Tr_τ) with respect to the $\mathbb{Z}$-basis $1, \sqrt{d}$,

$$\begin{pmatrix} a & b \\ b & ad \end{pmatrix}.$$

□

(b) We consider the field extension $A = \mathbb{Q}[\sqrt{d}]/\mathbb{Q}$. It is easy to chek that a two-dimensional symmetric bilinear form (M, b) over $\mathbb{Q}$ is scaled trace form of $A/\mathbb{Q}$ if and only if $0 \neq -det(M, b)$ is a norm.

(c) Let $A = \mathbb{Z}[\sqrt{-1}]$. Since A is a principal ideal domain, example (a) describes all scaled trace forms of $A/\mathbb{Z}$: A two-dimensional form of determinant -4 is a scaled trace form of $A/\mathbb{Z}$ if and only if it is given by a matrix of the followig type

$$\{\begin{pmatrix} a & b \\ b & -a \end{pmatrix} | a = \pm 2, b = 0 \text{ or } a = 0, b = \pm 2\}.$$

These matrices describe only two different isometry classes of forms over $\mathbb{Z}$. It is well known that there exists more than two different isometry classes of symmetric bilinear forms over $\mathbb{Z}$ with determinant -4 (See [CS] page 362.); more precisely, the form given by the matrix

$$\begin{pmatrix} 0 & 2 \\ 2 & 1 \end{pmatrix}$$

is not a scaled trace form of $A/\mathbb{Z}$. Since over $\mathbb{Q}$ there exists only one isometry class of forms with determinant -4 we see that the answer to the above question is negative.

The following problem remains open: Let $d \in \mathbb{Z}$ be not a square and $A = \mathbb{Z}[\sqrt{d}]$. Then determine all isometry classes of scaled trace forms of $A/\mathbb{Z}$. Let $D \in Mat(n, \mathbb{Z})$. Let $\chi_D(X) = det(XE_n - D) \in \mathbb{Z}[X]$ be the characteristic polynomial of D. The next lemma was shown in [T]. Other proofs and generalisations of this result can be found in [CP], [IS], [W].

Lemma 1. *(Taussky) Let $B \in Sym(n, \mathbb{Z})$ such that $\det B \neq 0$. Suppose there exists some $M \in Mat(n, \mathbb{Z})$ such that $BM^t = MB$ and $\chi_M(X)$ is irreducible. Let $A :=$*

$\mathbb{Z}[X]/(\chi_M(X))$. *Then there exists some* $c \in A_{\mathbb{Q}}$ *and* $b_1, \ldots, b_n \in A$ *such that* $\mathbb{Z}b_1 + \ldots + \mathbb{Z}b_n$ *is an ideal in* A *and* $B = (Tr(cb_ib_j))$. *Furthermore* $(b_1, \ldots, b_n) \in Q(A)^n$ *is an eigenvector of* $M \in Mat(n, Q(A))$.

Note that the above c is in $(\mathbb{Z}b_1 + \ldots + \mathbb{Z}b_n)^{\#}$. Given some $B \in Sym(n, \mathbb{Z})$ we can always find some M such that $BM^t = MB$: Choose any $S \in Sym(n, \mathbb{Z})$ and set $M := BS$. Then $BM^t = B(SB) = MB$ (Compare ([CP]).

Lemma 2. *For any* $B \in Sym(n, \mathbb{Z})$, $\det B \neq 0$ *there exists* $M \in Mat(n, \mathbb{Z})$ *such that* $BM^t = MB$ *and* $\chi_M(X) \in \mathbb{Z}[X]$ *is irreducible. Furthermore we may assume that* $\chi_M(X)$ *is totally real, that is all zeros of* $\chi_M(X)$ *are real.*

Proof. Let $N = (X_{ij})$ be the symmetric $n \times n$ matrix where the coefficients $X_{ij} = X_{ji}$ are new indeterminates. Choose $C \in GL(n, \mathbb{Q})$ such that C^tBC is a diagonal matrix. Since we may view $C^{-1}N(C^{-1})^t$ as a symmetric matrix with independent indeterminates as coefficients, by [S] or [W] the characteristic polynomial of $(C^tBC)C^{-1}N(C^{-1})^t$ is irreducible and it is also the characteristic polynomial of BN. By Hilbert's irreducibility theorem, there exist $a_{ij} = a_{ji} \in \mathbb{Q}$ such that $\chi_{B(a_{ij})}(X)$ is irreducible. If we choose $a \in \mathbb{Z}$ such that all $aa_{ij} \in \mathbb{Z}$, then $\chi_{B(aa_{ij})}(X) = a^n\chi_{B(a_{ij})}(a^{-1}X)$ is irreducible. Hence we set $M := B(aa_{ij})$. We have $BM^t = B(aa_{ij})^tB^t = MB$.

By [S], we may choose the a_{ij} above, such that $\chi_{B(a_{ij})}(X)$ is totally real. But then $\chi_{B(aa_{ij})}(X)$ is totally real as well. □

Using the above notations we have shown:

Theorem. *Let* (M, b) *be a bilinear form over* $\mathbb{Z}$ *such that* $det(M, b) \neq 0$. *Then there exist a monic, irreducible* $f(X) \in \mathbb{Z}[X]$, *some ideal* $\mathcal{I} \subset A := \mathbb{Z}[X]/(f(X))$, *and* $c \in (\mathcal{I}^2)^{\#}$ *such that* $(M, b) = (\mathcal{I}, Tr_c)$. *We may assume that* $f(X)$ *is totally real.*

Remarks. (a) The result holds more generally for (M, b) over R, $det(M, b) \neq 0$ where R is the integral closure of $\mathbb{Z}$ in some finite field extension $F/\mathbb{Q}$ and M is finitely generated free. We can also choose $R = k[X]$ where k is a field.

(b) Let $B \in Sym(n, \mathbb{Z})$ such that $\det B \neq 0$ and there exists some $c \in A_{\mathbb{Q}}$ and $b_1, \ldots, b_n \in A$ such that $B = (Tr(cb_ib_j))$. Let $B' \in Sym(n, \mathbb{Z})$ such that there exists $C \in Mat(n, \mathbb{Z})$ with $\det C = \pm 1$ and $B' = C^tBC$. Then there exists some $c' \in A_{\mathbb{Q}}$ and $a_1, \ldots, a_n \in A$ such that $B' = (Tr(c'a_ia_j))$. Furthermore, for the ideals we have $\mathbb{Z}b_1 + \ldots + \mathbb{Z}b_n = \mathbb{Z}a_1 + \ldots + \mathbb{Z}a_n$.

Proof. By [CP] III 5.2, there exists $M \in Mat(n, \mathbb{Z})$ such that $BM^t = MB$ and $A = \mathbb{Z}[X]/(\chi_M(X))$. Then

$$(C^tM(C^t)^{-1})(C^tBC) = C^tBM^tC = (C^tBC)(C^tM(C^t)^{-1})^t.$$

□

Question. Let (M, b) be a bilinear form over R, where R is the integral closure of $\mathbb{Z}$ in some finite field extension $F/\mathbb{Q}$, such that M is not a free but a projective R-module. Can we realize (M, b) as scaled trace form of some R-algebra A?

REFERENCES

[CP] Conner, P. E. , Perlis, R. , A survey of trace forms of algebraic number fields. World Scientific, Singapore, 1984.

[CS] Conway, J. H. , Sloane, N. J. A . Sphere packings, lattices and groups. Berlin, Heidelberg, New York, Springer 1988.

[IS] Ischebeck, F. , Scharlau, W. , Hermitesche und orthogonale Operatoren über kommutativen Ringen. Math. Ann. 200, 327–334 (1970).

[L] Lang, S. , Algebraic number theory. Reading, Massachusetts, Addison Wesley 1970.

[S] Scharlau, W. , On trace forms of algebraic number fields. Math. Z. 196, 125–127 (1987).

[T] Taussky, O. , On the similarity transformation between an integral matrix with irreducible characteristic polynomial and its transpose. Math. Ann. 166, 60–63 (1966).

[W] Waterhouse, W. C. , Scaled trace forms over number fields. Arch. Math. 47, 229–231 (1986).

February 1997

Mathematisches Institut der Universität
Einsteinstraße 62
D-48149 Münster
e–mail–adress: kruskem@math.uni-muenster.de