Proc. Indian Acad. Sci. (Math. Sci.), Vol. 97, Nos 1–3, December 1987, pp. 179–188.

On endomorphisms of degree two

MAX KOECHER

Mathematisches Institut der Westfälischen-Wilhelms-Universität Münster, Einsteinstraße 62, 4400 Münster, FRG

Abstract. Let R be a commutative ring, $\Delta \in R$ and let $R\{\Delta\}$ be the set of conjugacy classes of R-module endomorphisms f satisfying $f \circ f = \Delta \cdot id$. Using a certain subspace of the tensor product of two endomorphisms a commutative and associative product on $R\{\Delta\}$ can be defined. For $R = \mathbb{Z}$ a generalization of the composition of quadratic forms arises as a special case.

Keywords. Composition of quadratic forms; commutative rings; tensor products; conjugacy class of endomorphism.

1. Introduction

Let R be a commutative ring with unit element $1 = 1_R$ and let Δ be an element of R. A pair (A, f) is called a *Δ-pair*, if A is an R-module and $f: A \to A$ is a linear mapping satisfying $f \circ f = \Delta \cdot i$, where $i: A \to A$ denotes the identity mapping.

Given two Δ-pairs (A, f) and (B, g) there is a natural way to construct a new Δ-pair $(A * B, f * g)$. This construction is compatible with homomorphisms of Δ-pairs and hence induces a commutative and associative composition on the set $R\{\Delta\}$ of isomorphism classes of Δ-pairs.

In the case of free $\mathbb{Z}$-modules of rank 2 the composition is isomorphic to the product of the ideal classes in the ring $\mathbb{Z}[\sqrt{\Delta}]$ provided that Δ is not a square in $\mathbb{Z}$. Hence we obtain a new description of the composition of binary quadratic forms over $\mathbb{Z}$ in the sense of C F Gauss.

2. Δ-pairs

Suppose that (A, f) and (B, g) are Δ-pairs. The elements of A resp. B are written as a, a_1, a_2 etc. resp. b, b_1, b_2 etc. A linear mapping $\varphi: A \to B$ is called a *homomorphism of the Δ-pairs*, if

$$\varphi \circ f = g \circ \varphi \tag{1}$$

holds. We also write $\varphi: (A, f) \to (B, g)$.

Now consider the tensor product $A \otimes B$ over R and the submodule

$$A * B := (f \otimes i + i \otimes g)(A \otimes B) \tag{2}$$

of $A\otimes B$. Clearly, $A*B$ is spanned by the elements

$$a*b:=f(a)\otimes b+a\otimes g(b), \quad \text{where} \quad a\in A \quad \text{and} \quad b\in B. \tag{3}$$

Using

$$(f\otimes i)(a*b)=\Delta a\otimes b+f(a)\otimes g(b)=(i\otimes g)(a*b) \tag{4}$$

a linear mapping $f*g\colon A*B\to A*B$ is defined by

$$f*g:=f\otimes i|_{A*B}=i\otimes g|_{A*B}. \tag{5}$$

PROPOSITION A.

Suppose that (A,f) *and* (B,g) *are* Δ*-pairs. Then* $(A,f)*(B,g):=(A*B,f*g)$ *becomes a* Δ*-pair, too.*

Proof. Clearly,

$$(f*g)\circ(f*g)=(f\otimes i)\circ(f\otimes i)|_{A*B}=(f\circ f)\otimes i|_{A*B}=\Delta\cdot i\otimes i|_{A*B}$$

in view of (5). □

Applying $i\otimes g$ to (4) yields

$$(f\otimes g)(x)=\Delta\cdot x, \quad \text{whenever} \quad x\in A*B. \tag{6}$$

PROPOSITION B.

Suppose that $\varphi\colon(A,f)\to(\bar{A},\bar{f})$ *and* $\psi\colon(B,g)\to(\bar{B},\bar{g})$ *are homomorphisms of the* Δ*-pairs. Then*

$$\chi\colon A*B\to\bar{A}*\bar{B}, \quad \chi:=\varphi\otimes\psi|_{A*B},$$

becomes a homomorphism of the Δ*-pairs.*

Proof. First of all, write $\bar{a}:=\varphi(a)$ resp. $\bar{b}=\psi(b)$, and obtain

$$\overline{f(a)}=\bar{f}(\bar{a}) \quad \text{resp.} \quad \overline{g(b)}=\bar{g}(\bar{b})$$

from (1). Hence

$$\chi(a*b)=\overline{f(a)}\otimes\bar{b}+\bar{a}\otimes\overline{g(b)}=\bar{f}(\bar{a})\otimes\bar{b}+\bar{a}\otimes\bar{g}(\bar{b})\in\bar{A}*\bar{B} \tag{$*$}$$

holds according to (3). In order to prove $\chi\circ(f*g)=(\bar{f}*\bar{g})\circ\chi$ it suffices to consider elements of the form (3). Hence one gets

$$\begin{aligned}\chi\circ(f*g)(a*b)&=\chi(f(a)*b)=\bar{f}(\overline{f(a)})\otimes\bar{b}+\overline{f(a)}\otimes\bar{g}(\bar{b})\\&=(\bar{f}\otimes i)(\bar{f}(\bar{a})\otimes\bar{b}+\bar{a}\otimes\bar{g}(\bar{b}))=(\bar{f}l*\bar{g})\circ\chi(a*b)\end{aligned}$$

using (5) and $(*)$. □

PROPOSITION C.

Suppose that (A, f) and (B, g) are Δ-pairs. Then the restriction φ of the mapping $A \otimes B \to B \otimes A$ given by $a \otimes b \mapsto b \otimes a$ to $A * B$ becomes an isomorphism of $A * B$ onto $B * A$ and satisfies $\varphi(a * b) = b * a$.

Proof. Clearly,

$$\varphi(a * b) = g(b) \otimes a + b \otimes f(a) = b * a$$

holds according to (3). Hence

$$\varphi \circ (f * g)(a * b) = \varphi(\Delta a \otimes b + f(a) \otimes g(b)) = \Delta \cdot b \otimes a + g(b) \otimes f(a),$$

$$(g * f) \circ \varphi(a * b) = (g * f)(b * a) = \Delta b \otimes a + g(b) \otimes f(a)$$

follow from (4) and (5). $\square$

In order to prove the associative law start with three Δ-pairs (A, f), (B, g), (C, h) and compute

$$\begin{aligned}(a * b) * c &= [(f * g)(a * b)] \otimes c + (a * b) \otimes h(c) \\ &= [\Delta \cdot a \otimes b + f(a) \otimes g(b)] \otimes c + [f(a) \otimes b + a \otimes g(b)] \otimes h(c) \\ &= \Delta \cdot [a \otimes b] \otimes c + [f(a) \otimes g(b)] \otimes c \\ &\quad + [f(a) \otimes b] \otimes h(c) + [a \otimes g(b)] \otimes h(c)\end{aligned}$$

according to (3), (4) and (5). With the aid of similar arguments one obtains

$$\begin{aligned}a * (b * c) &= \Delta \cdot a \otimes [b \otimes c] + f(a) \otimes [g(b) \otimes c] \\ &\quad + f(a) \otimes [b \otimes h(c)] + a \otimes [g(b) \otimes h(c)].\end{aligned}$$

Furthermore one calculates

$$\begin{aligned}([f * g] * h)([a * b] * c) &= \Delta \cdot (a * b) \otimes c + [(f * g)(a * b)] \otimes h(c) \\ &= \Delta \cdot [f(a) \otimes b] \otimes c + \Delta \cdot [a \otimes g(b)] \otimes c \\ &\quad + \Delta \cdot [a \otimes b] \otimes h(c) + [f(a) \otimes g(b)] \otimes h(c)\end{aligned}$$

and respectively.

$$\begin{aligned}&(f * [g * h])(a * [b * c]) \\ &= \Delta \cdot a \otimes [b * c] + f(a) \otimes [(g * h)(b * c)] \\ &= \Delta \cdot a \otimes [g(b) \otimes c] + \Delta \cdot a \otimes [b \otimes h(c)] + \Delta \cdot f(a) \otimes [b \otimes c] \\ &\quad + f(a) \otimes [g(b) \otimes h(c)].\end{aligned}$$

Now let χ be the restriction of the R-module isomorphism

$$(A\otimes B)\otimes C\to A\otimes(B\otimes C),\ (a\otimes b)\otimes c\mapsto a\otimes(b\otimes c),$$

to $(A*B)*C$. Hence one has

$$\chi(a*(b*c))=(a*b)*c$$

and

$$\chi\circ([f*g]*h)=(f*[g*h])\circ\chi$$

holds. A summary yields

PROPOSITION D.

Suppose that (A,f), (B,g) and (C,h) are Δ-pairs. Then the mapping $\chi:(A*B)*C\to A*(B*C)$ becomes an isomorphism of the Δ-pairs.

Now let $R\{\Delta\}$ denote the set of isomorphism classes of Δ-pairs over the ring R. The isomorphism class of a Δ-pair (A,f) is denoted by

$$\mathfrak{a}=\prec A,f\succ. \tag{7}$$

According to Proposition A and B a product is defined in $R\{\Delta\}$ via

$$\mathfrak{a}*\mathfrak{b}:=\prec A*B,f*g\succ,\quad\text{whenever}\quad \mathfrak{a}=\prec A,f\succ,\quad \mathfrak{b}=\prec B,g\succ. \tag{8}$$

The propositions C and D lead to the

Lemma. The set $R\{\Delta\}$ of isomorphism classes of Δ-pairs forms a commutative semi-group.

3. Free modules

Let R^m denote the free R-module of column vectors with m entries. As an example consider a Δ-pair (A,f), where A is a free R-module of rank $m\geqslant 1$. Let $\mathscr{A}=(a_1,\dots,a_m)$ be a basis of A and put

$$h(a):=\begin{pmatrix}\alpha_1\\ \vdots\\ \alpha_m\end{pmatrix}, \tag{9}$$

whenever $a=\alpha_1a_1+\cdots+\alpha_ma_m$ and $\alpha_1,\dots,\alpha_m\in R$. Hence $h=h_{\mathscr{A}}:A\to R^m$ becomes a bijective linear mapping and there exists a matrix $F\in\mathrm{Mat}(m;R)$ such that

$$h\circ f=F\circ h,\quad F^2=\Delta\cdot I, \tag{10}$$

holds. Clearly, $h:(A,f)\to(R^m,F)$ becomes an isomorphism of the Δ-pairs.

Suppose further that (B,g) is a Δ-pair, where B is a free R-module of rank n and that $\mathscr{B}=(b_1,\dots,b_n)$ is a basis of B. How can the product $(A*B,f*g)$ be described?

Consider the diagram

$$\begin{array}{ccc} (A,f)\times(B,g) & \to (A*B, f*g), & (a,b)\mapsto a*b, \\ h_{\mathscr{A}} \downarrow \quad \downarrow h_{\mathscr{B}} & & \\ (R^m,F)\times(R^n,G) & \to (R^m*R^n, F*G). & \end{array} \tag{11}$$

In order to describe the module $A*B$, or better the module R^m*R^n, consider the isomorphism $\Phi\colon R^m\otimes R^n\to \mathrm{Mat}(m,n;R)$ induced by $\Phi(a\otimes b):=ab^t$, where b^t stands for the transpose of b.

Hence the subspace

$$R^m*R^n=(F\otimes I+I\otimes G)(R^m\otimes R^n)$$

of $R^m\otimes R^n$ is spanned by

$$z:=Fx\otimes y+x\otimes Gy,\quad \text{where}\quad x\in R^m,\quad y\in R^n, \tag{12}$$

and the map $F*G$ is given by

$$(F*G)(z):=\Delta\cdot x\otimes y+Fx\otimes Gy. \tag{12}$$

Now the image $\Phi(R^m*R^n)$ is spanned by the matrices

$$(Fx)y^t+x\cdot(Gy)^t=F\cdot xy^t+xy^t\cdot G^t.$$

Hence

$$\Phi(R^m*R^n)=\{FM+MG^t;\,M\in\mathrm{Mat}(m,n;R)\} \tag{13}$$

holds. In addition, the map $F*G$ is given via

$$FM+MG^t\mapsto F(FM+MG^t)=\Delta\cdot M+FMG^t \tag{13'}$$

in view of (4). A summary yields the

Lemma. Suppose that (A,f) and (B,g) are Δ-pairs, where A resp. B are free R-modules of rank m resp. n. Then the Δ-pair $(A*B, f*g)$ is isomorphic to the Δ-pair (C,h), where

$$C:=C_{F,G}:=\{FM+MG^t;\,M\in\mathrm{Mat}(m,n;R)\} \tag{14}$$

and where

$$h(X):=FX=XG^t,\quad \textit{whenever}\quad X\in C. \tag{14'}$$

Consider the Δ-pair (R^2,e), where $e\colon R^2\to R^2$ is given by

$$e(a):=Ea,\quad E:=\begin{pmatrix}0 & \Delta\\ 1 & 0\end{pmatrix}. \tag{15}$$

COROLLARY.

Suppose that (A,f) is a Δ-pair, where A is a free R-module. Then the Δ-pair $(A,f)*(R^2,e)$ is isomorphic to (A,f).

Proof. Without restriction suppose $A = R^m$ and $f(a) = Fa$, where $F \in \mathrm{Mat}(m; R)$ and $F^2 = \Delta \cdot I$. Hence according to (14), one has

$$C = \{FM + ME^t; M \in \mathrm{Mat}(m, 2; R)\}$$
$$= \{(Fa + \Delta b, Fb + a); a, b \in R^m\}$$
$$= \{(Fc, c); c \in R^m\} \cong R^m$$

and the mapping $h: C \to C$ corresponds to the endomorphism $c \mapsto Fc$ of R^m. □

The isomorphisms of (R^m, F) onto $(R^m, \tilde{F})$ clearly are given by matrices $W \in GL(m; R)$ such that $WF = \tilde{F}W$. Hence the isomorphism class $\langle\!\langle R^m, F \rangle\!\rangle$ in $R\{\Delta\}$ coincides with the conjugacy class of the matrix F with respect to the group $GL(m; R)$.

PROPOSITION.

Suppose that R is a field of characteristic $\neq 2$ and suppose that Δ is a square in R. Then $R\{\Delta\}$ is isomorphic to the multiplicative semi-group $\mathbb{N} \times \mathbb{N}$.

Proof. A set of representatives of conjugacy classes of matrices $F \in \mathrm{Mat}(m; R)$ satisfying $F^2 = \Delta \cdot I$ is given by

$$F_{p,q} := \sqrt{\Delta}\begin{pmatrix} I^{(p)} & 0 \\ 0 & -I^{(q)} \end{pmatrix}, \tag{16}$$

where $p + q = m$, and it is parametrized by $(p, q) \in \mathbb{N} \times \mathbb{N}$. Hence

$$F_{p,q}M + MF_{r,s} = 2\sqrt{\Delta}\begin{pmatrix} A & 0 \\ 0 & -D \end{pmatrix}, \tag{$*$}$$

where

$$M = \begin{pmatrix} A^{(p,r)} & B^{(p,s)} \\ C^{(q,r)} & D^{(q,s)} \end{pmatrix}.$$

Clearly, the dimension of $(R^m, F_{p,q}) * (R^n, F_{r,s})$ becomes $pr + qs$ and multiplication of $(*)$ from the left hand side by $F_{p,q}$ produces the identity on $A \in \mathrm{Mat}(p, r; R)$ and minus the identity on $B \in \mathrm{Mat}(q, s; R)$. □

4. An obvious generalization

In order to generalize Δ-pairs consider a monic polynomial $\pi \in R[X]$ of degree $r \geq 1$

$$\pi(X) = \pi_0 + \pi_1 X + \cdots + \pi_{r-1}X^{r-1} + X^r, \tag{17}$$

where $\pi_0, \ldots, \pi_{r-1} \in R$. A pair (A, f) is now called a *π-pair*, if A is an R-module and if $f: A \to A$ is a linear mapping satisfying

$$\pi(f) = \pi_0 i + \pi_1 f + \cdots + \pi_{r-1} f^{r-1} + f^r = 0. \tag{18}$$

Suppose that (A, f) and (B, g) are π-pairs. Define a linear mapping $F_{f,g}\colon A\otimes B\to A\otimes B$ via

$$F_{f,g} := \sum_{k=0}^{r-1} \pi_{k+1} \sum_{\nu+\mu=k} f^{\nu}\otimes g^{\mu}, \quad \pi_r = 1. \tag{19}$$

In particular, one has

r	$F_{f,g}$
1	$i\otimes i$
2	$f\otimes i + i\otimes g + \pi_1\cdot i\otimes i$
3	$f^2\otimes i + f\otimes g + i\otimes g^2 + \pi_2\cdot(f\otimes i + i\otimes g) + \pi_1\cdot i\otimes i.$

A verification using (18) leads to

$$(f\otimes i)\circ F_{f,g} = F_{f,g}\circ(f\otimes i) = F_{f,g}\circ(i\otimes g) = (i\otimes g)\circ F_{f,g}. \tag{20}$$

Now writing

$$A * B := F_{f,g}(A\otimes B), \tag{21}$$

and respectively

$$f * g\colon A * B\to A * B, \quad (f * g)(x) := (f\otimes i)(x), \tag{21'}$$

we obtain a π-pair $(A * B, f * g)$

This construction (and a more general set up) will be discussed elsewhere (cf. [2]).

5. The classical case

Suppose now $R=\mathbb{Z}$ and consider the case $m=n=2$. Start with an integer Δ and let $\mathbb{Z}_\Delta$ be the set of matrices $F\in\mathrm{Mat}(2;\mathbb{Z})$ satisfying

$$\operatorname{trace} F = 0 \quad\text{and}\quad \det F = -\Delta.$$

Hence $F^2 = \Delta\cdot I$ follows and $(\mathbb{Z}^2, F)$ is a Δ-pair. Let $M\{\Delta\}$ denote the subset of $\mathbb{Z}\{\Delta\}$ consisting of the equivalence classes

$$\mathfrak{a} = \langle\!\langle F\rangle\!\rangle := \langle\!\langle \mathbb{Z}^2, F\rangle\!\rangle,$$

where $F\in\mathbb{Z}_\Delta$. Recall that $\langle\!\langle(F)\rangle\!\rangle$ depends only on the conjugacy class over $\mathbb{Z}$ of F.

Proposition.

$M\{\Delta\}$ is a monoid under the composition $(\mathfrak{a},\mathfrak{b})\mapsto\mathfrak{a}*\mathfrak{b}$.

Proof. Put $\mathfrak{a} = \langle\!\langle F\rangle\!\rangle$ resp. $\mathfrak{b} = \langle\!\langle G\rangle\!\rangle$ and consider the $\mathbb{Z}$-module $C_{F,G}$ according to (14). Hence $C_{F,G}$ is a free $\mathbb{Z}$-module and $C_{F,G}\otimes\mathbb{C}$ has rank 2 over $\mathbb{C}$ in view of Proposition 3. Therefore the $\mathbb{Z}$-module $C_{F,G}$ has rank 2, too, and $\mathfrak{a}*\mathfrak{b}$ belongs to $M\{\Delta\}$. Clearly, the unit element $\mathfrak{e} = \langle\!\langle E\rangle\!\rangle$ (cf. (15)) belongs to $M\{\Delta\}$. □

Suppose that Δ is not a square in $\mathbb{Z}$, put $\Theta := \sqrt{\Delta}$ and consider the ring $\mathbb{Z}[\Theta]$. Let $\mathscr{I} \neq \{0\}$ be an ideal in $\mathbb{Z}[\Theta]$. Then there exists $0 \neq a \in \mathbb{Z}^2$ and $F = F_{\mathscr{I}} \in \mathbb{Z}_\Delta$ such that

$$\mathscr{I} = \{a^t(F + \Theta I)g; g \in \mathbb{Z}^2\} \tag{22}$$

holds. Note that F is uniquely determined up to conjugation over $\mathbb{Z}$. Hence a mapping

$$\mathscr{I} \mapsto \prec F_{\mathscr{I}} \succ \tag{23}$$

of the ideals of $\mathbb{Z}[\Theta]$ into $M\{\Delta\}$ is well-defined. But $F_{\mathscr{I}}$ depends only on the ideal class $\langle \mathscr{I} \rangle$ of $\mathscr{I}$ and consequently the mapping (23) induces a mapping ψ of the set $C(\Delta)$ of ideal classes of $\mathbb{Z}[\Theta]$ into $M\{\Delta\}$, which is bijective according to a classical result of R Dedekind (cf. [1], § 187).

Clearly, the product $\mathscr{I}_1\mathscr{I}_2$ of two ideals $\mathscr{I}_1, \mathscr{I}_2$ of $\mathbb{Z}[\Theta]$ induces a product $\langle \mathscr{I}_1\rangle\langle \mathscr{I}_2\rangle := \langle \mathscr{I}_1\mathscr{I}_2\rangle$ of the corresponding ideal classes. Hence $C(\Delta)$ is a commutative monoid.

Lemma. The mapping $\psi: C(\Delta) \to M\{\Delta\}$ is an isomorphism.

Proof. Let $\mathscr{I}_1$ and $\mathscr{I}_2$ be non-zero ideals of $\mathbb{Z}[\Theta]$. Hence there exist $a, b \in \mathbb{Z}^2\backslash\{0\}$ and $F, G \in \mathbb{Z}_\Delta$ such that

$$\mathscr{I}_1 = \{a^t(F + \Theta I)g; g \in \mathbb{Z}^2\} \quad \text{resp.} \quad \mathscr{I}_2 = \{b^t(G + \Theta I)h; h \in \mathbb{Z}^2\}$$

in view of (22). The elements of $\mathscr{I}_1\mathscr{I}_2$ are spanned by elements of the form

$$a^t(F + \Theta I)gh^t(G^t + \Theta I)b, \quad \text{where} \quad g, h \in \mathbb{Z}^2,$$

hence equal

$$a^t X_M b, \quad \text{where} \quad X_M := (F + \Theta I)M(G^t + \Theta I)$$

and where $M \in \mathrm{Mat}(2; \mathbb{Z})$. But one has

$$X_M = (FMG^t + \Delta M) + \Theta(FM + MG^t) = (F + \Theta I)Y_M,$$

where $Y_M := FM + MG^t$ holds. The use of (14) leads to

$$\mathscr{I}_1\mathscr{I}_2 = \{a^t(h(Y) + \Theta Y)b; Y \in C_{F,G}\},$$

where $\prec C_{F,G}, h \succ = \prec F \succ * \prec G \succ$. Now choose a basis of $C_{F,G}$ and compute

$$\mathscr{I}_1\mathscr{I}_2 = \{c^t(H + \Theta I)g; g \in \mathbb{Z}^2\}$$

for some $c \in \mathbb{Z}^2$ and $H \in \mathrm{Mat}(2; \mathbb{Z})$ such that $\prec C_{F,G}, h \succ = \prec H \succ$. $\square$

Note that $C(\Delta)$ and hence $M\{\Delta\}$ in general fail to be groups, because $\mathbb{Z}[\Theta]$ in general fails to be the maximal order of the quadratic field $\mathbb{Q}[\Theta]$. However, $M\{\Delta\}$ acts on $\mathbb{Z}\{\Delta\}$ in view of Lemma 2.

In addition, using the map

$$S \mapsto JS, \quad \text{where} \quad J = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix},$$

from the set of symmetric 2×2 matrices over $\mathbb{Z}$ of determinant-Δ onto $\mathbb{Z}_\Delta$ the composition of integral binary quadratic forms in the sense of C F Gauss is mapped onto the product in $M\{\Delta\}$.

6. The $\mathbb{Z}$-module $D_{F,G}$

Suppose that the integer Δ is not a square. Given $F \in \mathrm{Mat}(m;\mathbb{Z})$ resp. $G \in \mathrm{Mat}(n;\mathbb{Z})$ satisfying

$$F^2 = \Delta \cdot I \quad \text{resp.} \quad G^2 = \Delta \cdot I,$$

consider the $\mathbb{Z}$-modules $C_{F,G}$ (cf. (14)) and

$$D_{F,G} = \{N \in \mathrm{Mat}(m,n;\mathbb{Z}); FN = NG^t\}. \tag{24}$$

Hence

$$C_{F,G} \subset D_{F,G} \tag{25}$$

holds according to (14').

PROPOSITION.

The $\mathbb{Z}$-modules $C_{F,G}$ and $D_{F,G}$ have the same rank.

Proof. Since $C := C_{F,G}$ and $D := D_{F,G}$ are free $\mathbb{Z}$-modules, it suffices to prove that the $\mathbb{C}$-ranks of $\mathbb{C} \otimes C$ and $\mathbb{C} \otimes D$ coincide. Without restriction assume $F \sim F_{p,q}$ resp. $G \sim F_{r,s}$, where $F_{p,q}$ is given by (16). Hence a computation leads to $\mathbb{C} \otimes C = \mathbb{C} \otimes D$. □

COROLLARY.

The index $i_{F,G}$ of $C_{F,G}$ in $D_{F,G}$ is finite.

Now consider a matrix

$$H := \begin{pmatrix} F & N \\ 0 & -G^t \end{pmatrix}, \tag{26}$$

where $N \in \mathrm{Mat}(m,n;\mathbb{Z})$. A computation leads to

$$N \in D_{F,G} \Leftrightarrow H^2 = \Delta \cdot I \tag{27}$$

and to

$$\begin{pmatrix} I & M \\ 0 & I \end{pmatrix} H \begin{pmatrix} I & -M \\ 0 & I \end{pmatrix} = \begin{pmatrix} F & N - (FM + MG^t) \\ 0 & -G^t \end{pmatrix}. \tag{28}$$

Lemma. The number of conjugacy classes of matrices (26) satisfying $H^2 = \Delta \cdot I$ does not exceed $i_{F,G}$.

Proof. The matrices N in (26) can be reduced modulo $C_{F,G}$ according to (28). □

This result can be extended to arbitrary matrices $M \in \mathrm{Mat}(m; \mathbb{Z})$ satisfying $M^2 = \Delta \cdot I$, because M is conjugate to a matrix of the form

$$\begin{pmatrix} F_1 & F_{12} & \cdots & F_{1n} \\ 0 & F_2 & & \vdots \\ \vdots & & \ddots & \\ 0 & \cdots & 0 & F_n \end{pmatrix} \tag{29}$$

where $m = 2n$ and where all F_i's belong to $\mathbb{Z}_\Delta$ and where all F_{ij}'s belong to $\mathrm{Mat}(2; \mathbb{Z})$ according to Theorem III.12 in [3]. Since $F_{ij} \in D_{F,G}$ holds, where $F := F_i$ and $G := -F_j^t$, the matrices F_{ij} can be reduced modulo $C_{F,G}$. In particular, *suppose that $C_{F,G} = D_{F,G}$ holds for all $F, G \in \mathbb{Z}_\Delta$. Then every $M \in \mathrm{Mat}(m; \mathbb{Z})$ satisfying $M^2 = \Delta \cdot I$ is over $\mathbb{Z}$ conjugate to a block diagonal matrix with diagonal blocks from $\mathbb{Z}_\Delta$.*

Given $F, G \in \mathbb{Z}_\Delta$,

$$F = \begin{pmatrix} f_1 & f_2 \\ f_3 & -f_1 \end{pmatrix}, \quad G = \begin{pmatrix} g_1 & g_2 \\ g_3 & -g_1 \end{pmatrix},$$

let

$$e_{F,G} := gcd(f_1 + g_1, f_1 - g_1, f_2, g_2, f_3, g_3).$$

Without proof we mention that

$$C_{F,G} = e_{F,G} \cdot D_{F,G}$$

holds. In particular, $e_{F,G} = 1$ for $F, G \in \mathbb{Z}_\Delta$, whenever Δ is square free and $\Delta \not\equiv 1 \pmod 4$.

References

[1] Dirichlet P G L and Dedekind R, *Vorlesungen über Zahlentheorie*, Vieweg (1894)

[2] Koecher M, On endomorphisms satisfying a given polynomial identity (to appear)

[3] Newman M, Integral matrices (New York: Academic Press) (1972)