LENGTH THEOREMS FOR THE GENERAL LINEAR GROUP
OF A MODULE OVER A LOCAL RING

ERICH W. ELLERS and HUBERTA LAUSCH

Communicated by R. Lidl

Abstract

Let R be a not necessarily commutative local ring, M a free R-module, and $\pi \in GL(M)$ such that $B(\pi) = \mathrm{im}(\pi - 1)$ is a subspace of M. Then $\pi = \sigma_1 \cdots \sigma_t \rho$, where σ_i are simple mappings of given types, ρ is a simple mapping, $B(\sigma_i)$ and $B(\rho)$ are subspaces, and $t \leq \dim B(\pi)$.

1. Introduction

Every transformation in the general linear group is a product of simple mappings. The minimal number of factors needed in any factorization of a given transformation is called its length. Recently the length of a transformation in general linear groups over commutative local rings has been determined (see [6]). Here we are going to extend these investigations to classical groups over noncommutative local rings.

The main results in [6] involve determinants which are no longer available in our more general setting. A suitable substitute for the determinant is the type of a simple mapping (see [4] and [2]). In order to introduce the type, we need that the path of each simple mapping is a subspace. Then the factorization

into simple mappings with given types follows a similar pattern to that over skewfields (see [2]), except for one special case where the induced mapping is a homothety. This situation remains partly unresolved.

As an application to modules over commutative local rings we determine the lengths of transformations of determinant ± 1, using only transvections or reflections.

In general the transfer from the commutative to the more general noncommutative setting hinges on two observations: any free left module M over a local ring has invariant basis number; and every direct summand of M is free (see [1]).

2. The length of a linear transformation

Let R be a not necessarily commutative local ring, I the proper ideal of R containing all nonunits, and R^* the set of units of R. Then R/I is a field by [1, Proposition 0.3.2]. The coset $r + I$ and the field R/I will be denoted by $\bar{r}$ and $\overline{R}$, respectively.

Since the local ring R has a field as homomorphic image, it has invariant basis number (see [1, Proposition 0.2.1]), that is, the rank of every free left or right R-module is unique.

Now assume M is a finitely generated free left R-module of rank n (left R-module means that elements of M can be multiplied on the left by ring elements). Then IM is a submodule of M and M/IM is its quotient module.

For $\alpha + I \in R/I$ and $v + IM \in M/IM$ we define $(\alpha + I)(v + IM) = \alpha v + IM$. Then M/IM is a left vector space of dimension n over $\overline{R}$. We denote the coset $v + IM$ and the left vector space M/IM by $\bar{v}$ and $\overline{M}$, respectively.

By [1, Exercise 0.3.11] every projective module over a local ring is free. Since every direct summand of a free module is projective, we have that every direct summand of the free R-module M is free. A direct summand of M is called a subspace of M. The subspaces of M form the projective geometry associated with M (see [8]).

Since Nakayama's lemma holds even for noncommutative local rings [1, Exercise 0.3.1], we have $U = M$ for every submodule U of M with $\overline{U} = \overline{M}$. Furthermore, let U be a submodule of M and $\{x'_1, \ldots, x'_m\}$ be a basis for $\overline{U}$. Then there is a basis $\{x_1, \ldots, x_m, \ldots, x_n\}$ for M such that $\{x_1, \ldots, x_m\} \subset U$ and $\bar{x}_i = x'_i$ for $i = 1, \ldots, m$ (see [6, Lemmas 1, 2]).

Let $\text{Hom}(M)$ be the set of all R-linear mappings of M into M and let $GL(M)$ denote the group of all invertible mappings in $\text{Hom}(M)$.

Every linear mapping $\pi: M \to M$ induces a linear mapping $\overline{\pi}: \overline{M} \to \overline{M}: \bar{x} \to \overline{x^\pi}$. If $\pi \in GL(M)$, then $\overline{\pi} \in GL(\overline{M})$.

For every linear mapping π we define two submodules of M associated with π, namely $F(\pi) = \{x \in M | x^\pi - x = 0\}$, the fix of π, and $B(\pi) = \{x^\pi - x | x \in M\}$, the path of π. Clearly, $B(\overline{\pi}) = \overline{B(\pi)}$. If $B(\pi)$ is a subspace of M for $\pi \in \mathrm{Hom}(M)$, then $F(\pi)$ is also a subspace of M and $\mathrm{codim}\,\overline{F(\pi)} = \dim\,\overline{B(\pi)}$; in addition $\overline{F(\pi)} = F(\overline{\pi})$.

A mapping $\sigma \in \mathrm{Hom}(M)$ is called simple if $\mathrm{codim}\,\overline{F(\sigma)} = 1$. Let $\pi \in \mathrm{Hom}(M)$ be a product of simple mappings σ_i, $\pi = \sigma_1 \cdots \sigma_t$. Then the smallest integer t with this property is called the length $l(\pi)$ of π. Clearly $\dim\,\overline{B(\pi)} \leq l(\pi)$.

Our first theorem generalizes Theorem 5 in [6] for not necessarily commutative local rings. Indeed, the proof of [6, Theorem 5] remains true in the noncommutative case.

THEOREM 1. *Let R be a local ring, M a free left R-module of rank n, $\pi \in GL(M)$. Then π is a product of simple mappings in $GL(M)$ and $l(\pi) \leq \mathrm{codim}\,\overline{F(\pi)}$.*

If σ is a simple mapping, then $F(\sigma)$ is in general not a subspace of M. But for local rings without zero divisors we get

LEMMA 2. *Let R be a local ring without zero divisors, M a free left R-module of rank n, $\sigma \in GL(M)$. Then σ is simple if and only if $F(\sigma)$ is a hyperplane (that is, a subspace of dimension $n - 1$) of M.*

For a proof see [6, Proof of Lemma 7].

3. Factors with given types

From now on we consider only transformations $\pi \in GL(M)$ for which $B(\pi)$ is a subspace of M.

If σ is a simple mapping in $GL(M)$ and $B(\sigma)$ is a subspace of M, then there is some $a \in M \setminus IM$ such that $B(\sigma) = Ra$. Obviously $a^\sigma = \lambda a$ for some $\lambda \in R^*$. The conjugacy class $\tilde{\lambda}$ of λ is uniquely determined by σ. It will be called the type of σ.

We intend to obtain factorizations of a transformation into simple mappings with given types.

LEMMA 3. *Let R be a local ring and M a free left R-module of rank n. Let $\pi \in GL(M)$ such that $B(\pi)$ is a subspace of M, $\dim B(\pi) \geq 2$, and $\overline{\pi}$ is not a homothety modulo $\overline{F(\pi)}$. Then for any unit $\lambda \in R$ there is some simple mapping $\sigma \in GL(M)$ such that $B(\sigma)$ and $B(\pi\sigma^{-1})$ are subspaces of M, type $\sigma = \tilde{\lambda}$, and*

$\dim F(\pi) + 1 = \dim F(\pi\sigma^{-1})$. *Further, if $3 \leq \operatorname{codim} F(\pi)$, then σ can be chosen such that $\overline{\pi\sigma^{-1}}$ is not a homothety modulo $\overline{F(\pi\sigma^{-1})}$.*

PROOF. Assume $\dim F(\pi) = r - 1$. Then there is a basis $\{x_1, \ldots, x_{r-1}\}$ for $F(\pi)$. Let $\{b_r, \ldots, b_n\}$ be a basis for $B(\pi)$. Clearly there are $x_i \in M \setminus IM$, $r \leq i \leq n$, such that $x_i^\pi - x_i = b_i$, and $\overline{x}_i \notin \langle \overline{x}_1, \ldots, \overline{x}_{r-1}, \overline{x}_r, \ldots, \overline{x}_{i-1}\rangle$. Thus $X = \{x_1, \ldots, x_{r-1}, x_r, \ldots, x_n\}$ is a basis for M.

Then $x_i^\pi = \sum_{j=1}^n \alpha_{ij} x_j$ for some $\alpha_{ij} \in R$, $i = 1, \ldots, n$. In addition we may assume that α_{rs} is a unit for some $s > r$, as we shall see now. If $\overline{\alpha_{ij}} = \delta_{ij} \overline{\alpha_{rr}}$ for $r \leq i, j \leq n$, where δ_{ij} is the Kronecker delta, then $\overline{\alpha_{rr}}$ lies in the center $Z(\overline{R} \setminus \{\overline{0}\})$ of $\overline{R} \setminus \{\overline{0}\}$ and $\overline{\pi}$ is a homothety modulo $\overline{F(\pi)}$, which contradicts our assumption. Therefore either $\overline{\alpha_{kl}} \neq \overline{0}$ or $\overline{\alpha_{kk}} \neq \overline{\alpha_{ll}}$ for some k, l with $k \neq l$, $r \leq k, l \leq n$. If $\overline{\alpha_{ij}} = \overline{0}$ for all $i \neq j$ and $r \leq i, j \leq n$, then we choose a new basis $X' = \{x_i' | x_i' = x_i$ for $i = 1, \ldots, l-1, l+1, \ldots, n$ and $x_l' = x_k + x_l\}$. Calculating modulo $\overline{F(\pi)}$ we obtain the following congruences:

$$\overline{x}_l'^{\overline{\pi}} \equiv (\overline{x}_k + \overline{x}_l)^{\overline{\pi}} \equiv \overline{\alpha_{kk} x_k} + \overline{\alpha_{ll} x_l}$$
$$\equiv (\overline{\alpha_{kk}} - \overline{\alpha_{ll}})\overline{x}_k + \overline{\alpha_{ll}}(\overline{x}_k + \overline{x}_l) \equiv (\overline{\alpha_{kk}} - \overline{\alpha_{ll}})\overline{x}_k' + \overline{\alpha_{ll}}\overline{x}_l'.$$

Obviously $\{b_i' = x_i'^\pi - x_i' | i = r, \ldots, n\}$ is a basis for $B(\pi)$. Now let $x_i'^\pi = \sum_{j=1}^n \alpha_{ij}' x_j'$, $\alpha_{ij}' \in R$, $i = 1, \ldots, n$. Then $\overline{\alpha_{lk}'} \neq \overline{0}$. Therefore (returning to our original notation and renumbering if necessary) we may assume that $\overline{\alpha_{rs}} \neq \overline{0}$, that is, α_{rs} is a unit for some $s > r$ as claimed.

Now $Y_1 = \{x_1, \ldots, x_{r-1}, x_r, x_{r+1}, \ldots, x_{s-1}, b_r, x_{s+1}, \ldots, x_n\}$ and $Y_2 = \{x_1, \ldots, x_{r-1}, x_r^\pi, x_{r+1}, \ldots, x_{s-1}, \lambda b_r, x_{s+1}, \ldots, x_n\}$ for any unit $\lambda \in R$ are bases for M.

We define a simple mapping σ by $x_i^\sigma = x_i$ for $i \neq r, s$; $b_r^\sigma = \lambda b_r$; $x_r^\sigma = x_r^\pi$. Then $\sigma \in GL(M)$ since $Y_1^\sigma = Y_2$, and $B(\sigma) = Rb_r$. Using the basis Y_1 we get

$$B(\pi\sigma^{-1}) = \left\{ \sum_{\substack{i=r+1 \\ i \neq s}}^n \gamma_i(x_i^{\pi\sigma^{-1}} - x_i) + \gamma_s(b_r^{\pi\sigma^{-1}} - b_r) \Big| \gamma_i \in R, \ i = r+1, \ldots, n \right\}$$

$$= \left\{ \sum_{\substack{i=r+1 \\ i \neq s}}^n \gamma_i(b_i + \beta_i b_r) + \gamma_s((b_r^\pi - b_r) + \beta_s b_r) \Big| \gamma_i \in R, \ i = r+1, \ldots, n \right\}$$

for suitable $\beta_i \in R$, $i = r+1, \ldots, n$, and $\{b_i + \beta_i b_r | r+1 \leq i \leq n, i \neq s\} \cup \{b_r^\pi - b_r + \beta_s b_r\}$ is a basis for $B(\pi\sigma^{-1})$ since $\{b_i | r \leq i \leq n, i \neq s\} \cup \{b_r^\pi - b_r\}$ is a basis for $B(\pi)$. Thus $B(\pi\sigma^{-1})$ is a subspace of M and $\dim F(\pi\sigma^{-1}) = r = \operatorname{codim} B(\pi\sigma^{-1}) = \dim F(\pi) + 1$.

Now assume $\operatorname{codim} F(\pi) \geq 3$ and $\overline{\pi\sigma^{-1}}$ is a homothety modulo $\overline{F(\pi\sigma^{-1})}$. Since $\overline{(\pi\sigma^{-1})} = \overline{F(\pi)} \oplus \overline{R}\overline{x}_r$, there is some t, $t \geq r+1$, $t \neq s$, such that

$\overline{x}_t \notin \overline{F(\pi\sigma^{-1})}$. We define a simple mapping σ' by $x_i^{\sigma'} = x_i$ for $i \neq r, s, t$; $x_t^{\sigma'} = x_t + b_r$; $b_r^{\sigma'} = \lambda b_r$; $x_r^{\sigma'} = x_r^\pi$. Then $\sigma \in GL(M)$ since $Y_1^{\sigma'} = Y_3 = \{x_1, \ldots, x_{r-1}, x_r^\pi, x_{r+1}, \ldots, x_{t-1}, x_t + b_r, x_{t+1}, \ldots, x_{s-1}, \lambda b_r, x_{s+1}, \ldots, x_n\}$ which is a basis for M. We have $B(\sigma') = Rb_r$ and

$$
B(\pi\sigma'^{-1}) = \left\{ \sum_{\substack{i=r+1 \\ i \neq s,t}}^n \gamma_i(x_i^{\pi\sigma'^{-1}} - x_i) + \gamma_s(b_r^{\pi\sigma'^{-1}} - b_r) + \gamma_t(x_t^{\pi\sigma'^{-1}} - x_t)| \right.
$$
$$
\left. \gamma_i \in R, i = r+1, \ldots, n \right\}
$$

$$
= \left\{ \sum_{\substack{i=r+1 \\ i \neq s,t}}^n \gamma_i(b_i + \beta_i b_r) + \gamma_s((b_r^\pi - b_r) + \beta_s b_r) + \gamma_t(b_t + \beta_t b_r)| \right.
$$
$$
\left. \gamma_i \in R, i = r+1, \ldots, n \right\}
$$

for suitable $\beta_i \in R$, $i = r+1, \ldots, n$. Hence $B(\pi\sigma'^{-1})$ is a subspace of M.

Since $\overline{\pi\sigma^{-1}}$ is a homothety modulo $\overline{(F(\pi\sigma^{-1}))}$, there are $\delta \in R \setminus I$ and $z \in M$ with $\overline{z} \in \overline{F(\pi\sigma^{-1})}$ such that $\overline{x}_t^{\pi\sigma^{-1}} = \overline{\delta}\overline{x}_t + \overline{z}$. Hence $\overline{x}_t^\pi = \overline{\delta}\overline{x}_t^\sigma + \overline{z}^\sigma$. Since $t \neq r, s$, we have $x_t^\sigma = x_t$. Now let $z \in Rx_1 \oplus \cdots \oplus Rx_r$, that is, $z = \sum_{i=1}^r \alpha_i x_i$ where $\alpha_i \in R$. Then $z^\sigma = \sum_{i=1}^{r-1} \alpha_i x_i + \alpha_r x_r^\pi$. Thus $\overline{x}_t^\pi = \overline{\delta}\overline{x}_t + \sum_{i=1}^{r-1} \overline{\alpha}_i \overline{x}_i + \overline{\alpha}_r \overline{x}_r^\pi$ and therefore $\overline{x}_t^{\pi\sigma'^{-1}} = \overline{\delta}\overline{x}_t^{\sigma'^{-1}} + \sum_{i=1}^r \overline{\alpha}_i \overline{x}_i = \overline{\delta}(\overline{x}_t + \overline{\lambda^{-1}b_r}) + \overline{z}$. Since $\overline{z} \in \overline{F(\pi\sigma^{-1})} = \overline{F(\pi\sigma'^{-1})}$, we get $\overline{x}_t^{\pi\sigma'^{-1}} \equiv \overline{\delta}(\overline{x}_t - \overline{\lambda^{-1}b_r})$ modulo $\overline{F(\pi\sigma'^{-1})}$. But $\overline{\lambda^{-1}b_r} \notin \overline{F(\pi\sigma'^{-1})}$, hence $\overline{\pi\sigma'^{-1}}$ is not a homothety modulo $\overline{F(\pi\sigma'^{-1})}$.

LEMMA 4. *Let R be a local ring, M a free left R-module of rank n, and $\pi \in GL(M)$ such that $B(\pi)$ is a subspace of M and $\dim B(\pi) \geq 2$. Suppose $\overline{\pi}$ is a homothety η_ε modulo $F(\overline{\pi})$, where $\varepsilon \in Z(\overline{R} \setminus \{\overline{0}\})$. Assume $\varepsilon = \overline{1}$ or $\varepsilon \neq \overline{\lambda^{-1}}$ for some unit $\lambda \in R$. Then there is some simple mapping $\sigma \in GL(M)$ such that $B(\sigma)$ and $B(\pi\sigma)$ are subspaces of M, type $\sigma = \tilde{\lambda}$, $\dim B(\overline{\pi}) = \dim B(\overline{\pi\sigma})$, and $\overline{\pi\sigma}$ is not a homothety modulo $F(\overline{\pi\sigma})$.*

PROOF. Let $\{x_1, \ldots, x_{r-1}\}$ and $\{b_r, \ldots, b_n\}$ be bases for $F(\pi)$ and $B(\pi)$, respectively. Then there is a basis $X = \{x_1, \ldots, x_n\}$ for M such that $x_i^\pi - x_i = b_i$ for $i = r, \ldots, n$.

We define a simple mapping σ by $x_i^\sigma = x_i$, $i \neq r, s$ for some s with $r < s < n$; $x_r^\sigma = \lambda x_r$, $x_s^\sigma = x_s + x_r$. Then $\sigma \in GL(M)$, $B(\sigma) = Rx_r$ is a subspace of M, type $\sigma = \tilde{\lambda}$, and $F(\pi) \subset F(\sigma)$.

We intend to establish that $B(\pi\sigma)$ is a subspace of M. Now

$$B(\pi\sigma) = \left\{ \sum_{i=1}^{n} \beta_i (x_i^{\pi\sigma} - x_i) \mid \beta_i \in R, \ i = 1, \ldots, n \right\}$$

$$= \left\{ \sum_{\substack{i=r+1 \\ i \neq s}}^{n} \beta_i b_i^\sigma + \beta_r (b_r^\sigma + (\lambda - 1) x_r) + \beta_s (b_s^\sigma + x_r) \mid \beta_i = R, \ i = 1, \ldots, n \right\}$$

$$= \langle b_i^\sigma, b_r^\sigma + (\lambda - 1) x_r, b_s^\sigma + x_r \mid r < i \leq n, \ i \neq s \rangle.$$

Clearly $B(\pi\sigma)$ is a subspace of M if and only if $B(\pi\sigma)^{\sigma^{-1}}$ is a subspace of M. Now

$$B(\pi\sigma)^{\sigma^{-1}} = \langle b_i, b_r + (1 - \lambda^{-1}) x_r, b_s + \lambda^{-1} x_r \mid r < i \leq n, \ i \neq s \rangle.$$

If $\varepsilon = \bar{1}$, that is, $B(\bar{\pi}) \subset F(\bar{\pi})$, then $\{\bar{b}_i, \bar{x}_r \mid r \leq i \leq n\}$ is independent since $\bar{x}_r \notin F(\bar{\pi})$. Thus $B(\pi\sigma)^{\sigma^{-1}}$ is a subspace of M.

Now we assume $\varepsilon \neq \bar{1}$, that is, $B(\bar{\pi}) \cap F(\bar{\pi}) = \{\bar{0}\}$ and $\overline{\lambda^{-1}} \neq \varepsilon$. Then $x_r^\pi = \alpha_r x_r + z + v$, where $\alpha_r \in R$, $z \in F(\pi)$, $v \in IM$, and $\bar{\alpha}_r = \varepsilon$. Thus $b_r = (\alpha_r - 1) x_r + z + v$ and $\bar{b}_r = \overline{(\alpha_r - 1)} \bar{x}_r + \bar{z}$. From $B(\bar{\pi}) \cap F(\bar{\pi}) = \{\bar{0}\}$ we conclude that $\alpha_r - 1$ is a unit. Therefore $x_r = (\alpha_r - 1)^{-1}(b_r - z - v)$ and

$$B(\pi\sigma)^{\sigma^{-1}} = \langle b_i, b_r + (1 - \lambda^{-1})(\alpha_r - 1)^{-1}(b_r - z - v),$$
$$b_s + \lambda^{-1}(\alpha_r - 1)^{-1}(b_r - z - v) \mid r < i \leq n, \ i \neq s \rangle.$$

In order to see that $B(\pi\sigma)^{\sigma^{-1}}$ is a subspace, we show that the following set W is independent. Put

$$W = \{\bar{b}_i, \bar{b}_r + \overline{(1 - \lambda^{-1})(\alpha_r - 1)^{-1}}(\bar{b}_r - \bar{z}), \bar{b}_s + \overline{\lambda^{-1}(\alpha_r - 1)^{-1}}(\bar{b}_r - \bar{z}) \mid$$
$$r < i \leq n, \ i \neq s\}$$

$$= \{\bar{b}_i, \overline{(\alpha_r - \lambda^{-1})(\alpha_r - 1)^{-1}}\bar{b}_r + \overline{(1 - \lambda^{-1})(\alpha_r - 1)^{-1}}\bar{z}, \bar{b}_s + \overline{\lambda^{-1}(\alpha_r - 1)^{-1}}(\bar{b}_r - \bar{z}) \mid$$
$$r < i \leq n, \ i \neq s\},$$

where $\overline{\alpha_r - \lambda^{-1}} \neq \bar{0}$ since $\bar{\alpha}_r - \overline{\lambda^{-1}} = \varepsilon - \overline{\lambda^{-1}} \neq \bar{0}$. The set W is independent since $\{\bar{b}_r, \ldots, \bar{b}_n\}$ is independent, and if $\bar{z} \neq \bar{0}$, also $\{\bar{b}_r, \ldots, \bar{b}_n, \bar{z}\}$ is independent. Clearly $\dim B(\bar{\pi}\bar{\sigma}) = \dim B(\bar{\pi})$.

Finally we shall show that $\bar{\pi}\bar{\sigma}$ is not a homothety modulo $F(\bar{\pi}\bar{\sigma})$. Obviously $x_s^\pi = \alpha_s x_s + t + w$, where $\alpha_s \in R$, $t \in F(\pi)$, $w \in IM$, and $\bar{\alpha}_s = \varepsilon$. Then $x_s^{\pi\sigma} = \alpha_s x_s^\sigma + t^\sigma + w^\sigma = \alpha_s(x_s + x_r) + t + w^\sigma$. Thus $\bar{x}_s^{\bar{\pi}\bar{\sigma}} = \varepsilon(\bar{x}_s + \bar{x}_r) + \bar{t} \not\equiv \varepsilon\bar{x}_s$ modulo $F(\bar{\pi}\bar{\sigma})$ since $F(\pi\sigma) \supset F(\pi)$, $\dim B(\pi\sigma) = \dim B(\pi)$, and $\bar{x}_r \notin F(\bar{\pi}) = F(\bar{\pi}\bar{\sigma})$.

Now we are ready to state and prove our main factorization result in this section.

THEOREM 5. *Let R be a local ring, M a free left R-module of rank n, and $\pi \in GL(M)$ such that $B(\pi)$ is a subspace of M with $\dim B(\pi) = d \geq 2$. Suppose ε_i are units in R for $i = 1, \ldots, d$. If $\overline{\pi}$ is not a homothety modulo $F(\overline{\pi})$, then there are simple mappings $\sigma_i, \rho \in GL(M)$ such that $B(\sigma_i)$, $B(\rho)$ are subspaces of M, type $\sigma_i = \tilde{\varepsilon}_i$ for $i = 1, \ldots, d-1$, and $\pi = \sigma_1 \cdots \sigma_{d-1}\rho$. If $\overline{\pi}$ is a homothety η_ε modulo $F(\overline{\pi})$, where $\varepsilon \in Z(\overline{R} \setminus \{\overline{0}\})$, and if either $\varepsilon = \overline{1}$ or $\overline{\varepsilon}_i \neq \varepsilon$ for some $i \leq d$, then there are simple mappings σ_i, $\rho \in GL(M)$ such that $B(\sigma_i)$, $B(\rho)$ are subspaces of M, type $\sigma_i = \tilde{\varepsilon}_i$ for $i = 1, \ldots, d$, and $\pi = \sigma_1 \cdots \sigma_d \rho$. If $\pi = \sigma_1 \cdots \sigma_d$, then $\overline{\varepsilon}_i = \varepsilon$ for $1 \leq i \leq d$.*

PROOF. If $\overline{\pi}$ is not a homothety modulo $F(\overline{\pi})$, then we apply Lemma 3 and use induction. If $\overline{\pi}$ is a homothety modulo $F(\overline{\pi})$, then we apply Lemma 4 and proceed as before. Finally suppose $\pi = \sigma_1 \cdots \sigma_d$, where type $\sigma_i = \tilde{\varepsilon}_i$, $\varepsilon_i \in R^*$, for $i = 1, \ldots, d$. Then $\overline{\pi} = \overline{\sigma}_1 \cdots \overline{\sigma}_d$ and type $\overline{\sigma}_i = \tilde{\overline{\varepsilon}}_i$. Now [2, Lemma 4] implies that $\overline{\varepsilon}_i = \varepsilon$ for $i = 1, \ldots, d$.

PROPOSITION 6. *Let R be a local ring, M a free left R-module of rank n, and $\pi \in GL(M)$ such that $B(\pi)$ is a subspace of M with $\dim B(\pi) = d$. Assume $\overline{\pi}$ is a homothety η_ε modulo $F(\overline{\pi})$ for some $\varepsilon \in Z(\overline{R} \setminus \{\overline{0}\})$. Then $\pi = \sigma_1 \cdots \sigma_d$, where $\sigma_i \in GL(M)$ are simple mappings such that $B(\sigma_i)$ are subspaces of M, type $\sigma_i = \tilde{\varepsilon}_i$ with $\varepsilon_i \in R^*$ and $\overline{\varepsilon}_i = \varepsilon$ for $i = 1, \ldots, d$.*

PROOF. Let $\{b_1, \ldots, b_d\}$ and $\{x_{d+1}, \ldots, x_n\}$ be bases for $B(\pi)$ and $F(\pi)$, respectively. Clearly there is a basis $\{x_1, \ldots, x_d, x_{d+1}, \ldots, x_n\}$ for M such that $x_i^\pi - x_i = b_i$ for $i = 1, \ldots, d$. There are $\varepsilon_j \in R$, $z_j \in F(\pi)$, and $v_j \in IM$ such that $\overline{\varepsilon}_j = \varepsilon$ and $x_j^\pi = \varepsilon_j x_j + z_j + v_j$ for $1 \leq j \leq d$. We define $\sigma_d \in \mathrm{Hom}(M)$ by $x_i^{\sigma_d} = x_i$ for $i \neq d$ and $x_d^{\sigma_d} = x_d^\pi$. Then $\sigma_d \in GL(M)$ since $\overline{\varepsilon}_d = \varepsilon \neq \overline{0}$, and $B(\sigma_d)$ is a subspace of M since $x_d^{\sigma_d} - x_d = x_d^\pi - x_d = b_d \neq \overline{0}$. Also

$$B(\pi\sigma_d^{-1}) = \left\{ \sum_{i=1}^{d-1} \beta_i(x_i^{\pi\sigma_d^{-1}} - x_i) \,|\, \beta_i \in R \right\} = \left\{ \sum_{i=1}^{d-1} \beta_i b_i^{\sigma_d^{-1}} \,|\, \beta_i \in R \right\}$$

is a subspace of M and $\dim B(\pi\sigma_d^{-1}) = d - 1$. Now we shall see that $\overline{\pi\sigma_d^{-1}}$ modulo $\overline{F(\pi\sigma_d^{-1})}$ is a homothety η_ε. Clearly $F(\pi\sigma_d^{-1}) = \langle x_1, \ldots, x_d \rangle \supset F(\pi)$. For $1 \leq j \leq d-1$ we get $x_j^{\pi\sigma_d^{-1}} = \varepsilon_j x_j + z_j + v_j^{\sigma_d^{-1}}$, where $z_j \in F(\pi) \subset F(\pi\sigma_d^{-1})$ and $v_j^{\sigma_d^{-1}} \in IM$. We use induction to finish the proof.

4. Transvections and reflections

Transvections and reflections are the most widely used simple mappings. We shall determine the minimal number of transvections or reflections needed to

express certain transformations. This also provides an application of Theorem 5.

A transvectiòn τ is a simple mapping in $GL(M)$ whose path is a subspace of M such that $B(\tau) \subset F(\tau)$, or equivalently type $\tau = 1$.

For the rest of this section we assume that the local ring is commutative, so a determinant is defined for a mapping in $GL(M)$. If $\sigma \in GL(M)$ is a simple mapping such that $B(\sigma)$ is a subsapce of M and type $\sigma = \tilde{\lambda}$ for some $\lambda \in R^*$, then $\det \sigma = \lambda = \text{type } \sigma$.

PROPOSITION 7. *Let R be a commutative local ring, M a free R-module of rank n, $\pi \in GL(M)$ such that $B(\pi)$ is a subspace of M and $\det \pi = 1$. Then $\pi = \tau_1 \cdots \tau_t$, where τ_i are transvections. The smallest number t for which such a factorization of π exists is $t = \dim B(\pi)$ if $\overline{\pi}$ is not a homothety modulo $F(\overline{\pi})$. If $\overline{\pi}$ is a homothety η_ε modulo $F(\overline{\pi})$ for some $\varepsilon \in \overline{R} \setminus \{\overline{0}\}$, then $t \leq \dim B(\pi) + 1$. If $\varepsilon \neq \overline{1}$, then $t = \dim B(\pi) + 1$.*

PROOF. If $\dim B(\pi) = 1$, then π is a transvection, thus $t = 1$. If $\dim B(\pi) \geq 2$, we apply Theorem 5. If $\overline{\pi}$ is not a homothety modulo $F(\overline{\pi})$, then $\pi = \tau_1 \cdots \tau_{d-1} \rho$ where τ_i are transvections, ρ is simple, and $B(\rho)$ is a subspace of M. Since $\det \pi = 1$, we get $\det \rho = 1$. Thus τ_i and ρ are transvections for $i = 1, \ldots, d-1$. Now assume $\overline{\pi}$ is a homothety η_ε modulo $F(\overline{\pi})$ where $\varepsilon \in \overline{R} \setminus \{\overline{0}\}$. Then $\pi = \tau_1 \cdots \tau_d \rho$ where τ_i and ρ are transvections for $i = 1, \ldots, d$. This is immediate if $\varepsilon = \overline{1}$. If $\varepsilon \neq \overline{1}$, then we observe that all $\overline{\varepsilon}_i = \overline{1} \neq \varepsilon$. Finally if $\varepsilon \neq \overline{1}$ and $\pi = \tau_1 \cdots \tau_t$, then $\overline{\pi} = \overline{\tau}_1 \cdots \overline{\tau}_t$ where $\overline{\tau}_i$ are tranvections. Now [2, Corollary 8] shows that $t \geq \dim B(\pi) + 1$.

For Proposition 8 we need the additional assumption that $1 + 1 \notin I$. Then a reflection is defined as a simple mapping $\sigma \in GL(M)$ such that $B(\sigma)$ is a subspace of M and $\det \sigma = -1$. If σ is a reflection, then $M = B(\sigma) \oplus F(\sigma)$.

We shall show now that every transvection is a product of two reflections. Let τ be a transvection. There is a reflection σ such that $B(\sigma) = B(\tau)$. Let $\{x_1, \ldots, x_{n-1}\}$ and $\{x_n\}$ be bases for $F(\sigma)$ and $B(\sigma)$, respectively. If $x \in M$, then $x = \sum_{i=1}^n \alpha_i x_i$ where $\alpha_i \in R$. Then $x_i^\tau - x_i = \gamma_i x_n$ for some $\gamma_i \in R$ and $\gamma_j \notin I$ for some $j < n$ since $B(\tau)$ is a subspace. Now

$$x^{\sigma\tau} - x = \sum_{i=1}^n \alpha_i (x_i^{\sigma\tau} - x_i) = \sum_{i=1}^{n-1} \alpha_i (x_i^\tau - x_i) - 2\alpha_n x_n = \left(\sum_{i=1}^n \alpha_i \gamma_i - 2\alpha_n \right) x_n.$$

Since $\gamma_j \notin I$ for some $j < n$, there are $\alpha_i \in R$ such that $\sum_{i=1}^{n-1} \alpha_i \gamma_i - 2\alpha_n = 1$. Therefore $B(\sigma\tau) = Rx_n$ is a subspace. Clearly $\det \sigma\tau = -1$. Therefore $\sigma' = \sigma\tau$ is a reflection.

PROPOSITION 8. *Let R be a commutative local ring, $1+1 \in R^*$, M a free R-module of rank n, $\pi \in GL(M)$ such that $B(\pi)$ is a subspace of M, $\dim B(\pi) = d \geq 2$, and $\det \pi = \pm 1$. Then $\pi = \sigma_1 \cdots \sigma_t$ where σ_i are reflections for $i = 1, \ldots, t$. Let $l(\pi)$ denote the smallest number t for which such a factorization exists.*

(a) *Assume $\bar{\pi}$ is not a homothety modulo $F(\bar{\pi})$. Then*

$$l(\pi) = d \quad if \ \det \pi = (-1)^d,$$
$$l(\pi) = d + 1 \quad if \ \det \pi = (-1)^{d+1}.$$

(b) *Assume $\bar{\pi}$ is a homothety η_ε modulo $F(\bar{\pi})$, $\varepsilon \in Z(\overline{R} \setminus \{\overline{0}\})$. Then*

$$l(\pi) = d + 1 \quad if \ \det \pi = (-1)^{d+1} \quad and \ \varepsilon \neq -1,$$
$$l(\pi) = d + 2 \quad if \ \det \pi = (-1)^d \quad and \ \varepsilon \neq -1,$$
$$l(\pi) = d \quad or \ d + 2 \quad if \ \det \pi = (-1)^d \quad and \ \varepsilon = -1,$$
$$l(\pi) = d + 1 \quad or \ d + 3 \quad if \ \det \pi = (-1)^{d+1} \quad and \ \varepsilon = -1.$$

PROOF. We apply Theorem 5. If $\bar{\pi}$ is not a homothety modulo $F(\bar{\pi})$, then $\pi = \sigma_1 \cdots \sigma_{d-1} \rho$ where σ_i are reflections and $\det \pi = (-1)^{d-1} \det \rho$. Thus ρ is a reflection or a transvection. In the latter case ρ is a product of two reflections.

If $\bar{\pi}$ is a homothety η_ε modulo $F(\bar{\pi})$, and $\varepsilon \neq -1$, then $\pi = \sigma_1 \cdots \sigma_d \rho$ and $\det \pi = (-1)^d \det \rho$. Again ρ is either a reflection or a product of two reflections. If $\pi = \sigma_1 \cdots \sigma_t$ where σ_i are reflections, then $\bar{\pi} = \bar{\sigma}_1 \cdots \bar{\sigma}_t$ and $\bar{\sigma}_i$ are reflections. Now [2, Corollary 9] confirms that $l(\pi)$ cannot be smaller than stated.

If $\bar{\pi}$ is a homothety η_ε modulo $F(\bar{\pi})$ and $\varepsilon = -1$, then by Lemma 4 there is a transvection τ such that $B(\pi\tau)$ is a subspace of M, $\dim B(\pi\tau) = \dim B(\pi) = d$, and $\overline{\pi\tau}$ is not a homothety modulo $F(\overline{\pi\tau})$. Clearly $\det \pi\tau = \det \pi$. Now we can apply the first part of this proof to $\pi\tau$.

References

[1] P. M. Cohn, *Free rings and their relations* (Academic Press, London, New York, 1971).

[2] E. W. Ellers, 'Decomposition of equiaffinities into reflections', *Geom. Dedicata* **6** (1977), 297–304.

[3] E. W. Ellers, 'Decomposition of orthogonal, symplectic, and unitary isometries into simple isometries', *Abh. Math. Sem. Univ. Hamburg* **46** (1977), 97–127.

[4] E. W. Ellers, 'Products of axial affinities and products of central collineations', *The geometric vein, Coxeter-Festschrift* (pp. 465–470) Springer-Verlag, New York, Heidelberg, Berlin, 1982.

[5] E. W. Ellers and R. Frank, 'Products of quasi-reflections and transvections over local rings', *J. Geom.* **31** (1988), 69–78.

[6] E. W. Ellers and H. Ishibashi, 'Factorization of transformations over a local ring', *Linear Algebra Appl.* **85** (1987), 17–27.

[7] E. W. Ellers and Huberta Lausch, 'Generators for classical groups of modules over local rings' (preprint).

[8] W. Klingenberg, 'Projektive Geometrie und lineare Algebra über verallgemeinerten Bewertungsringen', *Algebraical and topological foundations of geometry*, Proc. Colloq. Utrecht, 1959, pp. 99–107 (Pergamon, Oxford, 1962).

Department of Mathematics
University of Toronto
Toronto, Ontario
Canada M5S 1A1

Mathematisches Institut
Universität Würzburg
Am Hubland
D-8700 Würzburg
West Germany