L'Enseignement Mathématique (2) 57 (2011), 155–163

THE STABLE RANK OF ARITHMETIC ORDERS IN DIVISION ALGEBRAS – AN ELEMENTARY APPROACH

by Joachim SCHWERMER and Ognjen VUKADIN

ABSTRACT. A well-known theorem of Bass implies that 2 defines a stable range for an arithmetic order in a finite-dimensional semisimple algebra over an algebraic number field. The purpose of this note is to provide an independent and elementary proof of this fact for arithmetic orders contained in a finite-dimensional division algebra over an algebraic number field.

1. INTRODUCTION

In the study of general linear groups over rings and the description of all their normal subgroups the concept of a *stable range* is fundamental. Given a ring R with identity, an element $x \in GL_n(R)$ is an *elementary matrix* if x is of the form $x = 1 + aE_{ij}$ where $a \in R$, $i \neq j$ and E_{ij} is the matrix with (i,j)-coordinate 1 and zeroes elsewhere. Let $E_n(R)$ be the subgroup of $GL_n(R)$ generated by all elementary matrices. Define the *stable linear group* $GL(R)$ to be the union $\bigcup_{n\geq 1} GL_n(R)$, where $GL_m(R)$ is naturally identified with a subgroup of $GL_{m+1}(R)$. This identification sends elementary matrices to elementary matrices. Thus, we set $E(R) = \bigcup_{n\geq 1} E_n(R)$.

In the case of a field k, the group $E_n(k)$ coincides with the derived group of $GL_n(k)$ (except if $n = 2$ and $|k| = 2$). In the case of an arbitrary ring R, the relation between the group $GL_n(R)$ and the group $E_n(R)$ is much more intricate. However, for the stable groups, $E(R) = [GL(R), GL(R)]$. More generally, given a two-sided ideal $\mathfrak{q}$ in R, one has

$$E(R,\mathfrak{q}) = [E(R), GL(R,\mathfrak{q})]\,,$$

where $GL(R,\mathfrak{q})$ denotes the union $\bigcup_{n\geq 1} GL_n(R,\mathfrak{q})$ over the principal congruence subgroups of level $\mathfrak{q}$.

Due to the work of Bass [1] one can recover this stable structure theorem for the linear group $GL_n(R)$ subject to the assumption that n is larger than the so-called *stable rank of* R. We say that $n \in \mathbf{N}$, $n \geq 1$, defines a *stable range for* $GL(R)$, or, simply, *for the ring* R, if, for all $m \geq n$, given $x = (x_1, \dots x_{m+1})$ unimodular in R^{m+1}, there exist $\mu_1, \dots, \mu_m \in R$ such that $(x_1 + \mu_1 x_{m+1}, \dots, x_m + \mu_m x_{m+1})$ is unimodular in R^m. The smallest integer n such that for every $k \geq n$, k defines a stable range for R, is called the *stable rank of* R, to be denoted $sr(R)$.

There are many important families of rings for which the stable rank is known. Among these are semi-local rings for which $sr(R) = 1$ (see Section 2) or Dedekind domains which have stable rank less than or equal 2. More generally, as proved in [1, Thm 11.1], an S-algebra R which is finitely generated as a module over a commutative Noetherian ring S of finite Krull dimension d has stable rank less than or equal to $d+1$.

In view of the applications of this latter result and the methods of proof within the realm of linear groups over orders in a finite-dimensional semi-simple algebra over $\mathbf{Q}$ (see [1, Sect. 19]), it might be of interest to have an elementary proof, independent of the result just alluded to, of the following:

THEOREM. *Let D be a finite-dimensional division algebra over an algebraic number field K and let Λ be an $\mathcal{O}_K$-order in D. Then 2 defines a stable range for $GL(\Lambda)$, i.e., $sr(\Lambda) \leq 2$.*

For the lack of reference, retaining the previous notation, we conclude the note with the following result:

PROPOSITION. *Let $A = M_r(D)$ with D a finite-dimensional division algebra over K, and let Λ be a maximal $\mathcal{O}_K$-order in A. Let $\mathfrak{q}$ be a nonzero two-sided ideal in Λ. Then $\Lambda/\mathfrak{q}$ is a finite ring, in particular: $sr(\Lambda/\mathfrak{q}) = 1$.*

2. SEMI-LOCAL RINGS

Let R be a ring with identity element. The *radical* $\mathrm{rad}(M)$ of an R-module M is defined to be the intersection of all the maximal submodules of M. If we view R as a module over itself, the radical $\mathrm{rad}(R)$ of R is defined. It is a two-sided ideal in R, equals the intersection of the annihilators in R of all simple R-modules. By definition, a non-zero ring R is called *local* if it has a unique maximal left ideal, or, equivalently, if $R/\mathrm{rad}(R)$ is a division ring. A ring R is said to be *semi-local* if $R/\operatorname{rad}(R)$ is a left artinian ring, or, equivalently, if $R/\operatorname{rad}(R)$ is a semi-simple ring. A semi-local ring has only a finite number of maximal left ideals. The converse holds if $R/\operatorname{rad}(R)$ is commutative.

In general, the projection $R \longrightarrow R/\operatorname{rad}(R)$ is a ring homomorphism. If an element $r \in R$ is invertible, viewed as an element in $R/\operatorname{rad}(R)$, then it is invertible in R.

The following result [1, 6.4] due to Bass plays a decisive role. For the sake of completeness, we include the simple proof given by Swan [7, 11.8].

LEMMA. *Let R be a semi-local ring, let $a \in R$ and let I be a left ideal of R such $Ra + I = R$. Then there exists an element $x \in I$ such that $a + x$ is a unit of R.*

Proof. By the previous remark we may assume that $\operatorname{rad}(R) = 0$ and that R is a semi-simple ring. Then there exists a left ideal $J \subset I$ such that $R = Ra \oplus J$. The map $\alpha\colon R \to Ra$, defined by the assignment $y \mapsto ya$, gives rise to a short exact sequence

$$0 \to \ker\alpha \to R \to Ra \to 0$$

of left R-modules. Since R is semi-simple the exact sequence splits, that is, there exists a splitting $\beta\colon R \to \ker\alpha$. Thus, there exists an R-submodule $S \subset R$ such that $\ker\alpha \oplus S = R$. By $Ra \oplus J = R$, this induces an isomorphism $\gamma\colon \ker\alpha \xrightarrow{\sim} J$. The composition of isomorphisms

$$R \to Ra \oplus \ker\alpha \to Ra \oplus J = R$$

sends 1 to $a + x$, where $x := \gamma(\beta(1)) \in J$. Hence $a + x$ is a right unit, and, by semi-simplicity, a unit of R.

3. STABLE RANGE FOR $GL(R)$

3.1 THE STABLE RANK OF A RING

Let R be a ring with identity element. Let $x = (x_1, \dots, x_m)$ be an element of the right R-module R^m. By definition, x is *unimodular* in R^m if $Rx_1 + \cdots + Rx_m = R$.

We say that $n \in \mathbf{N}$, $n \geq 1$, *defines a stable range for* $GL(R)$, or, simply, *for the ring* R, if, for all $m \geq n$, given $x = (x_1, \dots x_{m+1})$ unimodular in R^{m+1}, there exist $\mu_1, \dots, \mu_m \in R$ such that $(x_1 + \mu_1 x_{m+1}, \dots, x_m + \mu_m x_{m+1})$ is

Achevé de composer le 28 juin 2011 à 15 :18

unimodular in R^m. This definition uses the structure of a right R-module on R^m. As shown in [9, Thm 2] or [10, Thm 1.6], using the natural left module structure leads to an equivalent condition. It follows from the definition that if n defines a stable range for R, then so does any $m \geq n$. The smallest integer n such that for every $k \geq n$, k defines a stable range for R, is called the *stable rank of* R, to be denoted $sr(R)$.

If R is a semi-local ring then $sr(R) = 1$. This follows from the lemma in Section 2.

If $R = \mathcal{O}_k$ is the *ring of integers* in an algebraic number field k, or, more generally, if R is a Dedekind ring, then 2 defines a stable range for $GL(\mathcal{O}_k)$, whereas 1 does not define a stable range for R. Thus $sr(\mathcal{O}_k) = 2$. A simple direct proof of these facts is given in [3, Prop. K 13] or [2].

3.2 Arithmetic orders

Let k be an algebraic number field and let $\mathcal{O}_k$ denote its ring of integers. Let A be a finite-dimensional semi-simple algebra over k. We call a subring Λ of A an *arithmetic order in* A (or an $\mathcal{O}_k$*-order in* A) if $1 \in \Lambda$, Λ is a finitely generated $\mathcal{O}_k$-module and $k \cdot \Lambda = A$.

Examples. Given a positive integer $m > 2$, let k_m be the *cyclotomic field* of m^{th} roots of unity over $\mathbf{Q}$. One has $k_m = \mathbf{Q}(\zeta_m)$ with a primitive root of unity $\zeta_m \in \overline{\mathbf{Q}}$. A field with an abelian Galois group over $\mathbf{Q}$ has a unique maximal *totally real* subfield. In the case of the cyclotomic field k_m this is the field $l_m = \mathbf{Q}(\zeta_m + \zeta_m^{-1})$. The ring of integers of the field l_m is $\mathcal{O}_{l_m} = \mathbf{Z}(\zeta_m + \zeta_m^{-1})$.

Now we assume that m is even. Let I be the two-sided ideal in the free algebra $Q := \mathbf{Q}(X, Y)$ over X and Y generated by Φ_m, $X^2 + 1$, and $XYX^{-1} - Y^{-1}$, where Φ_m denotes the m^{th} *cyclotomic polynomial*. Then Q/I is a $\mathbf{Q}$-algebra generated by $x_m = X + I$ and $y_m := Y + I$. The center of this algebra is a field, isomorphic to the maximal subfield l_m in k_m. In fact, $A_{\zeta_m} := \mathbf{Q}(X, Y)/I$, viewed as an l_m-algebra is a central simple algebra with $1, y_m, x_m, y_m x_m$ as a basis over l_m. Thus, A_{ζ_m} is what is usually called a *quaternion algebra* over l_m. The algebra A_{ζ_m} ramifies at each archimedean place $v \in V_\infty$ of the field l_m, that is, $A_{\zeta_m} \otimes (l_m)_v$ is isomorphic to the algebra of Hamilton quaternions.

We denote by Λ_m the $\mathcal{O}_{l_m}$-order in A_{ζ_m} generated by $1, y_m, x_m, y_m x_m$. In the case of a prime power $\frac{m}{2} = p^k$ with a prime $p \equiv 3 \mod 4$ the order Λ_m is a maximal order whereas in the case $\frac{m}{2} = p^k$ with a prime $p \equiv 1$

mod 4 there are two maximal orders which properly contain Λ_m. If $\frac{m}{2}$ is not a prime power then Λ_m is a maximal order. (This follows by determining the discriminant of the order, or see, for example, [4, Satz 3.2.4].)

THEOREM. *Let D be a finite-dimensional division algebra over an algebraic number field k and let Λ be an arithmetic order in D. Then 2 defines a stable range for $GL(\Lambda)$, i.e., $sr(\Lambda) \leq 2$.*

COROLLARY. *For the matrix algebra $M_n(\Lambda)$ over an arithmetic order Λ of the above type one has $sr(M_n(\Lambda)) \leq 2$ for all $n \geq 1$.*

Proof. We need to show that given $x_1, x_2, x_3 \in \Lambda$ such that $\Lambda \cdot x_1 + \Lambda \cdot x_2 + \Lambda \cdot x_3 = \Lambda$ there exist μ_1, $\mu_2 \in \Lambda$ such that $\Lambda \cdot (x_1 + \mu_1 \cdot x_3) + \Lambda \cdot (x_2 + \mu_2 \cdot x_3) = \Lambda$. Without loss of generality we may suppose that $x_1 \neq 0$. Let $I := \Lambda \cdot x_1$ be the left ideal in Λ generated by x_1. Since $k \cdot \Lambda = D$, we have [1])

$$x_1^{-1} = \sum_{i=1}^{n} k_i \cdot \lambda_i$$

for some $k_1, \ldots, k_n \in k$ and $\lambda_1, \ldots, \lambda_n \in \Lambda$. Now, since k is the quotient field of $\mathcal{O}_k$, we have $k_i = \frac{r_i}{s_i}$ with r_i, $s_i \in \mathcal{O}_k$, $s_i \neq 0$ for $i = 1, \ldots, n$; so for $s = \prod_{i=1}^{n} s_i$ we have: $sx_1^{-1} \in \Lambda$, with $s \in \mathcal{O}_k$, $s \neq 0$. Then

$$s = sx_1^{-1} \cdot x_1 \in I,$$

so $\mathfrak{b} := I \cap \mathcal{O}_k$ is a nonzero ideal in $\mathcal{O}_k$. Consider

$$J = \Lambda \cdot \mathfrak{b} = \{ \sum_{\text{finite}} \lambda_i \cdot b_i \mid \lambda_i \in \Lambda,\ b_i \in \mathfrak{b} \}.$$

J is obviously a left ideal in Λ, and since the b_i's are elements of the center of Λ we have that J is a two-sided ideal and Λ/J is a ring. Since Λ is a finitely generated module over $\mathcal{O}_k$, we have that Λ/J is a finitely generated module over $\mathcal{O}_k/\mathfrak{b}$. Since $\mathcal{O}_k/\mathfrak{b}$ is always finite, we have that Λ/J is a finite ring, in particular, it is a semi-local ring. The equality $\Lambda \cdot x_1 + \Lambda \cdot x_2 + \Lambda \cdot x_3 = \Lambda$ leads to [2])

$$\Lambda/J \cdot (x_2 + J) + \Lambda/J \cdot \langle (x_1 + J), (x_3 + J) \rangle = \Lambda/J.$$

[1]) Note that x_1^{-1} is the inverse of x_1 in D, this element needs not to be in Λ.

[2]) For a ring R and $x_1, \ldots, x_k \in R$ we denote by $R \cdot \langle x_1, \ldots, x_k \rangle$ the left ideal of R generated by $x_1, \ldots, x_k$.

Achevé de composer le 28 juin 2011 à 15 :18

Now we can apply the Lemma in Section 2 for semi-local rings to conclude that the set

$$(x_2 + J) + \Lambda/J \cdot \langle (x_1 + J), (x_3 + J) \rangle$$

contains a unit, so there exist $\rho, \tau \in \Lambda$ such that

$$\Lambda/J \cdot ((x_2 + \rho \cdot x_1 + \tau \cdot x_3) + J) = \Lambda/J .$$

This implies that

$$J + \Lambda \cdot (x_2 + \rho \cdot x_1 + \tau \cdot x_3) = \Lambda .$$

Now, we have $\Lambda x_1 \supseteq J$ and $x_2 + \rho \cdot x_1 + \tau \cdot x_3 \in \Lambda x_1 + \Lambda(x_2 + \tau \cdot x_3)$, which implies that

$$\Lambda x_1 + \Lambda(x_2 + \tau \cdot x_3) = \Lambda .$$

By setting $\mu_1 := 0$, $\mu_2 := \tau$ we get the desired reduction.

The corollary follows from the result of Vaserstein [9, Thm 3] which states that for any ring R with identity element $sr(M_n(R)) = 1 + [\frac{sr(R)-1}{n}]$, where $[x]$ denotes the smallest integer greater than or equal to x.

REMARKS. (1) Note that the idea for the proof is based on the fact that, for $x_1 \neq 0$, the left ideal $\Lambda \cdot x_1$ has a nonzero intersection with $\mathcal{O}_k$. This allows us to factor the ring modulo J and then at the end capture J with x_1. However, this is not valid if we omit the condition "D is a division algebra". One can easily verify this for $M_n(\mathbf{Z})$ as a $\mathbf{Z}$-order in the matrix algebra $M_n(\mathbf{Q})$.

(2) Since a ring is semi-local if and only if $R/\operatorname{rad} R$ is left artinian we can slightly modify the proof of the theorem using the fact that an algebra which is finitely generated as a module over an artinian ring is artinian as a ring, in order to generalize the result for orders in finite-dimensional division algebras over quotient fields of arbitrary Dedekind rings R.

(3) The idea of the proof can be applied in a simplified version to give a short simple proof of the fact that 2 defines a stable range for any Dedekind ring.

4. MAXIMAL ORDERS IN $M_n(D)$

PROPOSITION. *In the above setting, let $A = M_r(D)$ and let Λ be a maximal arithmetic order in A. Let $\mathfrak{q}$ be a nonzero two-sided ideal in Λ. Then $\Lambda/\mathfrak{q}$ is a finite ring, in particular $sr(\Lambda/\mathfrak{q}) = 1$.*

Proof. By the classification of maximal orders in $M_n(D)$ [6, Thm 27.6], there are a maximal arithmetic order Δ in D and a right ideal[3]) J so that Λ has the form

$$\Lambda = \begin{pmatrix} \Delta & . & . & \Delta & J^{-1} \\ . & & & . & . \\ . & & & . & . \\ \Delta & . & . & \Delta & J^{-1} \\ J & . & . & J & \Delta' \end{pmatrix},$$

with $J^{-1} := \{x \in D \mid JxJ \subseteq J\}$, and $\Delta' := \{x \in D \mid xJ \subseteq J\}$. Let $\mathfrak{q}$ be a nonzero two-sided ideal in Λ. Then $\mathfrak{q}$ contains a matrix X with some nonzero entry $d = x_{ij}$ for some $i, j \in \{1, \ldots, r\}$. We want to show that $\mathcal{O}_k \cap \mathfrak{q}$ is a non-zero ideal in $\mathcal{O}_k$.

We first consider the case when $i, j \in \{1, \ldots, r-1\}$. Let E_{kl} denote the matrix with 1 in the (k, l)-coordinate, and zeroes elsewhere. The arithmetic order Δ contains the identity element, thus $E_{kl} \in \Lambda$ for $k, l \in \{1, \ldots, r-1\}$. Now, $E_{ii}XE_{ji} = dE_{ii} \in \mathfrak{q}$, and $E_{ki}dE_{ii}E_{ik} = dE_{kk} \in \mathfrak{q}$ for every $k \in \{1, \ldots, r-1\}$, thus:

$$\begin{pmatrix} d & 0 & . & 0 & 0 \\ 0 & d & . & . & . \\ . & . & . & 0 & . \\ 0 & . & 0 & d & 0 \\ 0 & . & . & 0 & 0 \end{pmatrix} \in \mathfrak{q}.$$

As in the proof of the theorem in 3.2, we can find $s \neq 0$, $s \in \mathcal{O}_k$, such that $s \cdot d^{-1} \in \Delta$. Then the product

$$\begin{pmatrix} sd^{-1} & 0 & . & 0 & 0 \\ 0 & sd^{-1} & . & . & . \\ . & . & . & 0 & . \\ 0 & . & 0 & sd^{-1} & 0 \\ 0 & . & . & 0 & 0 \end{pmatrix} \begin{pmatrix} d & 0 & . & 0 & 0 \\ 0 & d & . & . & . \\ . & . & . & 0 & . \\ 0 & . & 0 & d & 0 \\ 0 & . & . & 0 & 0 \end{pmatrix} = \begin{pmatrix} s & 0 & . & 0 & 0 \\ 0 & s & . & . & . \\ . & . & . & 0 & . \\ 0 & . & 0 & s & 0 \\ 0 & . & . & 0 & 0 \end{pmatrix},$$

to be denoted S, is an element of $\mathfrak{q}$.

Again, as in the proof of the theorem in 3.2, we have $J \cap \mathcal{O}_k \neq 0$. We choose any $t \neq 0$, $t \in J \cap \mathcal{O}_k$. Then

$$tE_{r(r-1)}S = tsE_{r(r-1)} \in \mathfrak{q}.$$

[3]) For the definition of a *right ideal* of an order, see [6]. In the case of an order in a skewfield, the definition of a right ideal of an order coincides with the usual ring theoretic definition.

Since J is a right ideal of Δ we have $1 \in J^{-1}$, hence $E_{(r-1)r} \in \Lambda$ and

$$tsE_{r(r-1)}E_{(r-1)r} \in \mathfrak{q}\,.$$

Consequently, the product ts, written in the form

$$0 \neq \begin{pmatrix} ts & 0 & . & 0 & 0 \\ 0 & ts & . & . & . \\ . & . & . & 0 & . \\ 0 & . & 0 & ts & 0 \\ 0 & . & . & 0 & ts \end{pmatrix} = \begin{pmatrix} t & 0 & . & 0 & 0 \\ 0 & t & . & . & . \\ . & . & . & 0 & . \\ 0 & . & 0 & t & 0 \\ 0 & . & . & 0 & 0 \end{pmatrix} S + tsE_{r(r-1)}E_{(r-1)r}\,,$$

is an element in $\mathfrak{q} \cap \mathcal{O}_k$.

The cases where $i \in \{1,\dots,r-1\}$, $j = r$, reduce to the previous one by observing that $XtE_{ri} \in \mathfrak{q}$. Analogously, the cases where $i = r$, $j \in \{1,\dots,r-1\}$ also reduce to the first case by using the fact that $sE_{jr}X \in \mathfrak{q}$, and the case $i = j = r$ reduces to the latter case by observing that $XtE_{r1} \in \mathfrak{q}$.

We obtain that $\beta := \mathfrak{q} \cap \mathcal{O}_k$ is a nonzero ideal in $\mathcal{O}_k$. Thus, as in the proof of the theorem we have that $\Lambda/\mathfrak{q}$ is a finitely generated $\mathcal{O}_k/\beta$-module, hence finite, in particular, $\Lambda/\mathfrak{q}$ is a semi-local ring and $sr(\Lambda/\mathfrak{q}) = 1$.

REFERENCES

[1] BASS, H. K-theory and stable algebra. *Publ. Math. Inst. Hautes Études Sci. 22* (1964), 5–60.

[2] ESTES, D. and J. OHM. Stable range in commutative rings. *J. Algebra 7* (1967), 343–362.

[3] JANTZEN, J.C. and J. SCHWERMER. *Algebra.* Springer-Lehrbuch. Springer, Heidelberg, 2006.

[4] KIRSCHMER, M. Konstruktive Idealtheorie in Quaternionenalgebren. Diplomarbeit, Universität Ulm, 2005.

[5] LAM, T.Y. Bass's work in ring theory and projective modules. In: *Algebra, K-theory, Groups, and Education. On the Occasion of Hyman Bass's 65th Birthday.* Edited by T.Y. Lam and A.R. Magid, 83–124. Contemporary Mathematics *243*. Amer. Math. Soc., Providence, RI, 1999.

[6] REINER, I. *Maximal Orders.* London Mathematical Society Monographs *5*. Academic Press, London-New York, 1975.

[7] SWAN, R.G. *Algebraic K-Theory.* Lecture Notes in Mathematics *76*. Springer-Verlag, Berlin-Heidelberg-New York, 1968.

[8] —— *K-Theory of Finite Groups and Orders.* Lecture Notes in Mathematics *149*. Springer-Verlag, Berlin-Heidelberg-New York, 1970.

[9] VASERSTEIN, L. N. Stable rank of rings and dimensionality of topological spaces. *Funct. Anal. Appl.* *5* (1971), 102–110.

[10] WARFIELD, R. B., JR. Cancellation of modules and groups and stable range of endomorphism rings. *Pacific J. Math.* *91* (1980), 457–485.

(Reçu le 23 août 2010)

Joachim Schwermer

Faculty of Mathematics
University of Vienna
Nordbergstrasse 15
A-1090 Vienna
Austria

and

Erwin Schrödinger International Institute for Mathematical Physics
Boltzmanngasse 9
A-1090 Vienna
Austria
e-mail: Joachim.Schwermer@univie.ac.at

Ognjen Vukadin

Faculty of Mathematics
University of Vienna
Nordbergstrasse 15
A-1090 Vienna
Austria
e-mail: ognjenvukadin@yahoo.com

Achevé de composer le 28 juin 2011 à 15:18