Invent. math. 91, 525–542 (1988)

Inventiones mathematicae

Absolute stable rank and Witt cancellation for noncommutative rings

B.A. Magurn[1]*, W. Van der Kallen[2], and L.N. Vaserstein[3]**

[1] Department of Mathematics and Statistics Miami University, Oxford, OH 45056, USA
[2] Math. Instituut, University of Utrecht, Postbus 80.010, NL-3508 TA, Utrecht, The Netherlands
[3] Department of Mathematics, The Pennsylvania State University, University Park, PA 16802, USA

0. Introduction

Stable range conditions on a ring R were devised by H. Bass in order to determine values of n for which every matrix in $GL_n(R)$ can be row reduced (by addition operations with coefficients from R) to a matrix with the same last row and column as the identity matrix I_n. In order to obtain analogous results for orthogonal groups, M.R. Stein defined "absolute stable range" conditions on a commutative ring R. Because he was working with group schemes, Stein did not consider absolute stable range conditions for noncommutative rings. Here we do so, and take up a corresponding stability question for orthogonal groups, namely cancellation of quadratic forms. For this we use a very general definition of quadratic form, which specializes to all classical examples.

Sections 1, 2 and 3 contain definitions associated with, and computations of, absolute stable rank. Definitions associated with quadratic forms are introduced in Sections 4, 5, 6 and 7; and Section 8 is devoted to Witt cancellation.

1. Definitions and their connections

Suppose A is an associative ring with unit. If S is a subset of A, let $J(S)$ denote the intersection of A and all maximal left ideals of A which contains S. We say a sequence $a_0, \ldots, a_n$ in A *can be shortened* if there are coefficients $t_0, \ldots, t_{n-1}$ in A for which

$$a_n \in J(a_0 + t_0 a_n, \ldots, a_{n-1} + t_{n-1} a_n).$$

Consider the condition on the ring A:

Condition $L(n)$: Every sequence $a_0, \ldots, a_n$ in A can be shortened.

Lemma 1.1. $L(n)$ *implies* $L(n+1)$.

Proof. Shorten a sequence $a_0, \ldots, a_{n+1}$ using coefficients $t_0, \ldots, t_{n-1}, 0$. □

* Supported by Miami University FRC Summer Research Appointment
** Supported by the National Science Foundation and the Guggenheim Foundation

The *absolute stable rank* of A is the least n with $L(n)$ true. A sequence $a_0, \ldots, a_n$ in A is called *unimodular* if $J(a_0, \ldots, a_n) = A$. The *stable rank* of A is the least n with $L(n)$ true for unimodular sequences. (It is true that $L(n)$ for unimodular sequences implies $L(n+1)$ for unimodular sequences; but this is harder to prove than Lemma 1.1 – see Theorem 1 of [**12**].) We abbreviate the absolute stable rank and stable rank of A by $\operatorname{asr}(A)$ and $\operatorname{sr}(A)$, respectively.

Lemma 1.2. *For every ring* A, $\operatorname{sr}(A) \leqq \operatorname{asr}(A)$.

Proof. If $L(n)$ holds for all sequences, it holds for unimodular sequences. □

In many cases, $\operatorname{sr}(A) = \operatorname{asr}(A)$. To see that they do not always agree, consider the following examples. We learned about the first from R.M. Guralnick, and the second from H.W. Lenstra, Jr.

Example 1. In [**8**, 5.1] D.R. Estes and R.M. Guralnick construct Dedekind domains A with $\operatorname{sr}(A) = 1$, but with nontorsion class group G. There are elements a_1, a_2 which generate a maximal ideal M of infinite order in G. If $\operatorname{asr}(A) = 1$, there is some t in A with

$$J(a_1 + t a_2) = J(a_1, a_2) = M.$$

Since A is Dedekind, $A(a_1 + t a_2)$ contains a power of its radical, M; so it equals a power of M, in contradiction to the choice of M.

Example 2. Suppose R is the ring of integers in an algebraic number field with nontrivial class group. Let S denote the smallest multiplicative set containing the generators of the nonzero principal prime ideals of R. Take A to be $S^{-1}R$. Then $\operatorname{sr}(A) = 1$ and $\operatorname{asr}(A) > 1$.

To see this, suppose a, $b \in A$ and $Aa + Ab = A$. For some α, β in R and s in S, $a = \alpha/s$ and $b = \beta/s$. Then $R\alpha + R\beta$ meets S, hence equals a product of principal primes, Rs'. Then $\alpha = \alpha' s'$, $\beta = \beta' s'$ and $s' = \gamma\alpha + \delta\beta$ for some α', β', γ, δ in R. Thus $1 = \gamma\alpha' + \delta\beta'$. By the theorem of Dirichlet on the distribution of primes (see [7, p. 83]), $\alpha' + R\beta'$ meets S. So for some t in R, the element

$$(\alpha' + t\beta')\frac{s'}{s} = a + tb$$

is a unit of A, proving $\operatorname{sr}(A) = 1$.

On the other hand, A has a nonprincipal prime ideal M. If d is a nonzero element of M^2, then A/Ad is a principal ideal ring; so there is some c in M with $M = Ac + Ad$. Suppose $\operatorname{asr}(A) = 1$. Then for some t in A,

$$J(c + td) = J(c, d) = M.$$

So $A(c + td) = M^n$ for some integer $n > 1$. In the local ring A_M,

$$\begin{aligned} M_M &= A_M(c + td) + A_M d \\ &= M_M^{n-1} M_M + A_M d. \end{aligned}$$

So by Nakayama's Lemma, $M_M = A_M d \subseteq M_M^2$, which is impossible in the Dedekind ring A_M. (In Section 3, we show that $\operatorname{asr}(A) \leqq \dim(A) + 1$; so that, actually, $\operatorname{asr}(A) = 2$ in this example.)

The presence, in these two examples, of ideals which require at least two generators is no coincidence.

Theorem 1.3. *If A is a left principal ideal ring, then* $\operatorname{asr}(A)=\operatorname{sr}(A)$.

Proof. Suppose $\operatorname{sr}(A)=n$ and $a_0, \ldots, a_n \in A$. For some d in A,

$$A a_0 + \ldots + A a_n = A d.$$

Specifically, for some α_i, β_i in A, each $a_i = \alpha_i d$, while

$$\beta_0 a_0 + \ldots + \beta_n a_n = d.$$

Then $\beta_0 \alpha_0 + \ldots + \beta_n \alpha_n - 1$ annihilates d. The left annihilator of d in A is a left ideal $A d'$ ($d' \in A$); so $\alpha_0, \ldots, \alpha_n, d'$ is unimodular. Since $\operatorname{sr}(A)=n$, there are elements α_i' in $\alpha_i + A d'$ for which $\alpha_0', \ldots, \alpha_n'$ is unimodular. Again, $\operatorname{sr}(A)=n$ implies there are elements c_i, t_i in A with

$$t_0(\alpha_0' + c_0 a_n') + \ldots + t_{n-1}(\alpha_{n-1}' + c_{n-1} \alpha_n') = 1.$$

Multiplying on the right by d, we discover that every left ideal of A which contains

$$\{a_0 + c_0 a_n, \ldots, a_{n-1} + c_{n-1} a_n\}$$

also includes d, and hence a_n. So $\operatorname{asr}(A) \leqq n = \operatorname{sr}(A)$. (The reverse inequality is Lemma 1.2.) □

2. Semilocal rings

We denote the Jacobson radical of a ring A by $\operatorname{rad}(A)$. This radical is especially pertinent to absolute stable rank because $\operatorname{rad}(A)$ is the intersection of all maximal left ideals of A. Following Bass (in [5]), we call a ring A *semilocal* if $A/\operatorname{rad}(A)$ is a left artinian ring. Then by Wedderburn's Theorems, $A/\operatorname{rad}(A)$ is a direct product of finitely many matrix rings over division rings.

Lemma 2.1. *If A is a ring and I is a (two-sided) ideal of A, then* $\operatorname{asr}(A/I) \leqq \operatorname{asr}(A)$; *equality holds if* $I \subseteq \operatorname{rad}(A)$.

Proof. If $\operatorname{asr}(A)=n$ any sequence $a_0, \ldots, a_n$ in A can be shortened with some coefficients $t_0, \ldots, t_{n-1}$ in A. Suppose $f\colon A \to A/I$ is the canonical homomorphism. If M is a maximal left ideal of A/I, then $f^{-1}(M)$ is a maximal left ideal of A, and $ff^{-1}(M)=M$. So $f(a_0), \ldots, f(a_n)$ is shortened by the coefficients $f(t_0), \ldots, f(t_{n-1})$, proving $\operatorname{asr}(A/I) \leqq n$.

If $\operatorname{asr}(A/I)=m$ and $a_0, \ldots, a_m \in A$, there are $t_0, \ldots, t_{m-1}$ in A for which $f(a_0), \ldots, f(a_m)$ is shortened by the coefficients $f(t_0), \ldots, f(t_{m-1})$ in A/I. But if $I \subseteq \operatorname{rad}(A)$, then for every maximal left ideal N of A, $f(N)$ is a maximal left ideal of A/I, and $N = f^{-1} f(N)$. In that case, $a_0, \ldots, a_m$ is shortened by $t_0, \ldots, t_{m-1}$ in A. □

Lemma 2.2. *If* $A=\prod_{i=1}^{r} A_i$ *is the direct product of finitely many rings* A_i, *then*

$$\operatorname{asr}(A)=\sup_{1\leqq i\leqq r} \operatorname{asr}(A_i)$$

Proof. Apply Lemma 2.1 to the projections $\pi_i: A \to A_i$ to see that

$$\operatorname{asr}(A)\geqq \sup_{1\leqq i\leqq r} \operatorname{asr}(A_i)$$

To prove the reverse inequality, shorten a sequence in A with coefficients whose i-coordinates shorten the corresponding sequence of i-coordinates in A_i for each i. This works because each maximal ideal of A is π_i^{-1} of a maximal left ideal of A_i for some i. □

Lemma 2.3. *If* $A=M_n(D)$ *is the ring of n-by-n matrices with entries in a division ring D, then* $\operatorname{asr}(A)=1$.

Proof. Suppose a_0 and a_1 belong to A. If the j-th row of a_1 is not in the (left) row space of a_0 then some row (say the i-th row) of a_0 is in the linear span of the others. Let e_{ij} denote the matrix with 1 in the ij-position and 0's elsewhere. Then $a_0+e_{ij}a_1$ differs from a_0 only in that the j-th row of a_1 has been added to the i-th row of a_0. The effect has been to adjoin the j-th row of a_1 to the row space of a_0. Continuing in this way, we arrive at $a_0+t_0a_1$ $(t_0\in A)$ whose row space includes all rows of a_1. So there exists b in A with $b(a_0+t_0a_1)=a_1$. Then $a_1\in J(a_0+t_0a_1)$. □

Together, these lemmas prove:

Theorem 2.4. *If A is a semilocal ring, then* $\operatorname{asr}(A)=1$. □

Remark 2.5. We can improve the statement of this result when $\operatorname{rad}(A)=0$. For any division ring D and positive integer n, there is a lattice isomorphism "row" from the lattice of left ideals of $M_n(D)$ to the lattice of left vector subspaces of D^n: If I is a left ideal, $\operatorname{row}(I)$ is the set of rows of its members. Since every subspace of D^n is an intersection of co-dimension one subspaces, it follows that every left ideal of $M_n(D)$ is an intersection of maximal left ideals. Therefore every left ideal I of a *semisimple artinian* ring S is an intersection of maximal left ideals: $J(I)=I$. So, in such a ring S, every list $a_0, \ldots, a_n$ of generators of a left ideal I can be shortened to a single generator:

$$a_0+\sum_{i=1}^{n} c_i a_i \qquad (c_i\in S).$$

We need the following lemma in Section 3:

Lemma 2.6. *If J is a left ideal of a finite dimensional semisimple algebra S over a field k,* $p(t)\in J[t]$, *and for some x in k,* $Sp(x)=J$, *then there are at most finitely many y in k with* $Sp(y)\neq J$.

Proof. Each simple component of S is a matrix ring $M_n(D)$ over a finite dimensional division k-algebra D. The projection π: $S \to M_n(D)$ is a k-algebra homomorphism. For each simple component of S, fix a left regular representation of D over k, and apply it entrywise to define a k-algebra embedding ρ: $M_n(D) \to M_{ns}(k)$. We may apply the composite $\rho\pi$ to each coefficient to define a ring homomorphism:

$$S[t] \to M_{ns}(k)[t] \cong M_{ns}(k[t]).$$

Let $p^{\rho\pi}(t)$ denote the image of $p(t)$ under this map.

For any x in k, $Sp(x) \subseteq J$. Suppose $Sp(y) \neq J$ for some y in k. It follows from Remark 2.5 that, for some projection π to a simple component $M_n(D)$, the D-dimension of the row space of $\pi(p(y))$ is less than the D-dimension m of row $(\pi(J))$. Thus the k-dimension of the row space of $\rho\pi(p(y)) = p^{\rho\pi}(y)$ is less than ms, so that every ms-by-ms submatrix of $p^{\rho\pi}(y)$ has determinant zero. These determinants are polynomials over k evaluated at y, and are not all identically zero since $Sp(x) = J$ for some x; so they vanish for at most finitely many y in k. Since there are only finitely many simple components of S, the lemma follows. □

3. Absolute stable rank and dimension

Suppose R is a commutative ring. In this section we relate the absolute stable rank of a module-finite R-algebra A to the dimension of R. For strongest results, we work with the dimension of mspec(R), the subspace of the prime spectrum of R consisting of the maximal ideals. (For its properties, we refer the reader to pp. 92–102 of [5].)

Theorem 3.1. *If the maximal spectrum of a commutative ring R is noetherian of finite dimension d, then any module-finite R-algebra A has absolute stable rank at most $d+1$.*

If the word "absolute" is deleted, this is a theorem proved by H. Bass in the early development of algebraic K-theory (see [4]). If "absolute" is put back in, but $A = R$, this theorem was proved by D. Estes and J. Ohm in 1967 (see Theorem 2.3 of [9] and M. Stein's elaboration in Theorem 1.4 of [10]).

Before embarking on the proof of this theorem, we marshall some well known facts about a commutative ring R and a module-finite R-algebra A. For simplicity we state and prove these facts for the case in which R is a central subring of A. The proofs carry over easily to the case in which the map $R \to A$ $(r \to r \cdot 1)$ has nonzero kernel.

Lemma 3.2. *If M is a maximal left ideal of A and S is a multiplicative subset of R which does not meet M, then $S^{-1}M$ is a maximal left ideal of $S^{-1}A$ whose contraction to A is M.*

Proof. Since M does not meet S, $S^{-1}M$ is a proper left ideal of $S^{-1}A$; thus $S^{-1}M \cap A$ is a proper left ideal of A containing, hence equal to M. A larger left ideal of $S^{-1}A$ would contract to a larger left ideal of A. □

Lemma 3.3. *For any ideal I of R, the canonical map $A \to A/IA$ induces a bijection between the maximal left ideals of A containing I and the maximal left ideals of A/IA.*

Proof. Elementary. □

Lemma 3.4. $\mathrm{Rad}(A)$ *contains* $\mathrm{rad}(R)$.

Proof. Suppose $r \in \mathrm{rad}(R)$. For each a in A, the finitely generated R-modules $A/A(1+ra)$ and $A/(1+ra)A$ vanish by Nakayama's Lemma; so $1+ra$ is invertible. □

Lemma 3.5. *If M is a maximal left ideal of A, then $M \cap R$ is a maximal ideal of R.*

Proof. Otherwise we may choose $r \notin M$ from a maximal ideal of R containing $M \cap R$. The multiplicative set $S = 1 + Rr$ does not meet M. By Lemmas 3.4 and 3.2,

$$S^{-1}Rr \subseteq \mathrm{rad}(S^{-1}R) \subseteq \mathrm{rad}(S^{-1}A) \subseteq S^{-1}M.$$

By Lemma 3.2, $r \in M$, a contradiction. □

Now we standardize some notation. Suppose p is a prime ideal of the commutative ring R. Then R_p denotes the location $(R-p)^{-1}R$, $k(p)$ denotes the residue field of R_p, A_p denotes $A \otimes_R R_p$, and $A(p)$ denotes $A \otimes_R k(p)$. Note that the localization $R \to R_p$ induces an embedding α: $R/p \to k(p)$ of the domain R/p into its field of fractions $k(p)$. There is a commutative diagram:

$$\begin{array}{ccccc} R/p & \xrightarrow{\ \beta\ } & A \otimes_R (R/p) & \xleftarrow{\ \delta\ } & A \\ {\scriptstyle\alpha}\downarrow & & {\scriptstyle\gamma}\downarrow & \swarrow & \\ k(p) & \longrightarrow & A \otimes_R k(p) & & \end{array}$$

where the maps are the standard ones. Note that δ is surjective with kernel pA; so we will identify $A \otimes_R (R/p)$ with A/pA. Also γ: $A/pA \to A(p)$ is a localization at $(R/p - \{0\})$; so its kernel is the set of elements with $R-p$ torsion. Although some of these maps need not be injective, we shall simplify notation by referring to elements of R/p, $k(p)$ or A as if they are *in* $A(p)$, via these maps.

To prove Theorem 3.1, we resort to an induction on d, and for this purpose it is natural to prove a more technical generalization. If Y is a subset of $\mathrm{mspec}(R)$ and A is a module-finite R-algebra, we say that a sequence $a_0, \ldots, a_n$ in A *can be Y-shortened* if there are coefficients $t_0, \ldots, t_{n-1}$ in A for which a_n belongs to every maximal left ideal of A that contains both

$$\{a_0 + t_0 a_n, \ldots, a_{n-1} + t_{n-1} a_n\}$$

and some member of Y. A certain flexibility is obtained from the following:

Lemma 3.6. *If, for some b in A and $i \neq d < n$, the sequence*:

$$a_0, \ldots, a_{d-1}, \quad a_d + b a_i, \quad a_{d+1}, \ldots, a_n$$

can be Y-shortened with coefficients $t_0, \ldots, t_{n-1}$, *then the sequence* $a_0, \ldots, a_n$ *can be Y-shortened with coefficients*:

$$t_0, \ldots, t_{d-1}, \quad t'_d, \quad t_{d+1}, \ldots, t_{n-1}.$$

Proof. If $i=n$, use $t'_d = b + t_d$. If $i \neq n$, use $t'_d = t_d - b t_i$. □

By Lemma 3.5, $\operatorname{asr}(A) \leqq d+1$ means that every sequence of more than $d+1$ elements of A can be mspec(R)-shortened. So Theorem 3.1 is a corollary to the following:

Theorem 3.7. *Suppose R is a commutative ring, A is a module-finite R-algebra, and* $X_1, \ldots, X_m$ *are finitely many noetherian subspaces of* mspec(R), *each of dimension at most d. Then every sequence* $a_0, \ldots, a_n$ *in A with* $n > d$ *can be* $X_1 \cup \ldots \cup X_m$*-shortened with coefficients* $t_0, \ldots, t_{n-1}$ *with* $t_i = 0$ *for all* $i > d$.

Proof. Since each X_i is the union of finitely many irreducible components, we can rewrite $X_1 \cup \ldots \cup X_m$ as $Y_1 \cup \ldots \cup Y_r$ where each Y_i is an *irreducible* noetherian subspace of mspec(R) of dimension at most d. Then the intersection of the elements of Y_i is a prime ideal p_i of R.

Step 1. (Putting a_d in general position.)

We begin with an arbitrary sequence $a_0, \ldots, a_n$ in A with $n > d$. Taking advantage of Lemma 3.6, we now describe how to modify a_d by a finite sequence of addition operations until it generates the same left ideal as $a_0, \ldots, a_n$ in each ring $A(p_i)/\operatorname{rad} A(p_i)$.

Suppose p is a prime ideal of R. Since $A(p)$ is a finite dimensional $k(p)$-algebra, $A(p)/\operatorname{rad} A(p)$ is a semisimple artinian ring. Let J denote the left ideal of $A(p)/\operatorname{rad} A(p)$ generated by $a_0, \ldots, a_n$. We say an element of J is in *general position* if it generates J as a principal left ideal. By Remark 2.5, there are coefficients $c_0, \ldots, c_n$ in $A(p)$, with $c_d = 0$, for which $g(1)$ is in general position, where

$$g(x) = a_d + \sum_{i=1}^{n} x c_i a_i.$$

By Lemma 2.6, $g(x)$ is in general position for all but finitely many x in $k(p)$. So for each nonzero z in R/p, there is a nonzero x in R/p for which $g(zx)$ is in general position. (If R/p is finite, it is a field, and $g(c \cdot (1/c)) = g(1)$ is in general position.)

Since $A(p)$ is obtained from A/pA by inverting the nonzero elements of R/p, we can choose a nonzero z in R/p for which each zc_i comes from A/pA, and hence from A. For each i, choose a lifting $\tilde{c}_i$ in A of zc_i, choosing $\tilde{c}_d = 0$. Define

$$h(x) = a_d + \sum_{i=1}^{n} x \tilde{c}_i a_i.$$

Then for each x in $R-p$, $h(x)$ belongs to A; and there is some y in $R-p$ for which $h(xy)$ maps to $g(cxy)$ in general position.

Renumber the primes p_i, if necessary, so that $p_i \nsubseteq p_j$ if $i<j$. (First number the primes maximal among the p_i's then delete them and number those which become maximal among the remaining p_i's, etc.) Assume a_d is already in general position at p_i for every $i<j$. For each $i<j$, choose x_i in $p_i - p_j$. Then the product $x_1 \dots x_{j-1}$ belongs to $R-p_j$. Choose y in $R-p_j$ for which

$$a'_d = h(x_1 \dots x_{j-1} y)$$

has general position in $A(p_j)/\mathrm{rad}\, A(p_j)$. Notice that a_d and a'_d are equal in each $A(p_i)$ for $i<j$; so a'_d is in general position at p_i for every $i \leqq j$. Continue in this way, to reach a'_d in general position at every p_i, where $a'_d - a_d$ is a left A-linear combination of $a_1, \dots, a_{d-1}, a_{d+1}, \dots, a_n$.

Step 2. We now show that there is a subset Y of $Y_1 \cup \dots \cup Y_r$ with each $Y_i - Y$ having dimension at most $d-1$, for which $a_0, \dots, a_{d-1}, a'_d, a_{d+1}, \dots, a_n$ is Y-shortened by *any* coefficients $t_o, \dots, t_{n-1}$ in A with $t_d = 0$.

Suppose a'_d is in general position at a prime ideal p of R. Then in $A(p)/\mathrm{rad}\, A(p)$, a'_d generates a left ideal containing a_n; so for some element a of $A(p)$, $a_n - a a'_d$ belongs to $\mathrm{rad}\, A(p)$. Since $A(p)$ is artinian, its radical is nilpotent; so for some positive integer N,

$$[A(p)(a_n - a a'_d)]^N = 0.$$

For some element u of $R-p$, ua lifts to an element b of A/pA. Then

$$[(A/pA)(u a_n - b a'_d)]^N$$

is a finitely generated left R/p-module in the kernel of the localization $A/pA \to A(p)$. So for some v in $R-p$,

$$[(A/pA)(v u a_n - v b a'_d)]^N = 0.$$

For each p_i (= intersection of the primes in Y_i), let r_i denote the product vu associated with $p = p_i$ above. Let Y denote the set of primes $\mathfrak{m}$ in $X_1 \cup \dots \cup X_m = Y_1 \cup \dots \cup Y_r$ which satisfy $r_i \notin \mathfrak{m} \in Y_i$ for some i.

We claim that a_n belongs to every maximal left ideal M of A which contains both $\{a'_d\}$ and a prime $\mathfrak{m}$ from Y. To see this, suppose $r_i \notin \mathfrak{m} \in Y_i$ and let S be the multiplicative set generated by r_i. Notice that M contains p_i but does not meet S (since $M \cap R = \mathfrak{m}$ is prime). By Lemmas 3.2 and 3.3, M is the contraction to A of a maximal left ideal N of $S^{-1}A/p_iA$. Since the element $a_n - r_i^{-1} v b a'_d$ generates a nilpotent left ideal of $S^{-1}A/p_iA$, it belongs to the Jacobson radical of this ring, and hence to N. Since $a'_d \in M$, which is contracted from N, $a_n \in M$ as well, proving the claim.

For each i, $r_i \notin p_i$; so there are primes from Y_i which do not contain it. So the primes from Y_i which do not contain r_i form a proper closed subset of the irreducible component Y_i, containing $Y_i - Y$. Thus $Y_i - Y$ is either empty or noetherian of dimension at most $d-1$. And

$$(Y_1 \cup \dots \cup Y_r) - Y = (Y_1 - Y) \cup \dots \cup (Y_r - Y).$$

Step 3. (The induction.) If every $Y_i - Y$ is empty (as happens when $d=0$), the sequence

$$a_0, \ldots, a_{d-1}, a'_d, a_{d+1}, \ldots, a_n$$

is $X_1 \cup \ldots \cup X_m$ ($=Y$)-shortened with coefficients that are all zero. So by Lemma 3.6, $a_0, \ldots, a_n$ can be $X_1 \cup \ldots \cup X_m$ – shortened with coefficients $0, \ldots, 0, t_d, 0, \ldots, 0$ as required.

If $d>1$, we assume the theorem holds when d is decreased by 1. Then

$$a_0, \ldots, a_{d-1}, a_{d+1}, \ldots, a_n$$

can be $(Y_1 - Y) \cup \ldots \cup (Y_r - Y)$-shortened by some coefficients $t_0, \ldots, t_{d-1}, 0, \ldots, 0$. By Step 2 above,

$$a_0, \ldots, a_{d-1}, a'_d, a_{d+1}, \ldots, a_n$$

is $X_1 \cup \ldots \cup X_m$-shortened by the coefficients

$$t_0, \ldots, t_{d-1}, t_d(=0), 0, \ldots, 0.$$

So by Lemma 3.6, $a_0, \ldots, a_n$ can be shortened by coefficients

$$t_0, \ldots, t_{d-1}, t'_d, 0, \ldots, 0$$

as required. □

4. Quadratic forms

To include the various quadratic forms arising in L-theory, we combine the definitions of A. Bak [**1**, **2**, **3**] with those of J. Tits [**11**] and C.T.C. Wall [**14**, **15**] for maximum generality. Let A denote an associative ring with unit. Let α denote an antiautomorphism of the ring A; for notational convenience we shall write a^* to mean $\alpha(a)$ for a in A. Assume there is a unit ε of A, with $\varepsilon^* = \varepsilon^{-1}$, so that $a^{**} = \varepsilon a \varepsilon^{-1}$ for every a in A. (Of course, if ε is central, then α is simply an involution on A.)

Each right A-module V becomes a left A-module via α. In particular, the dual $V^* = \mathrm{Hom}_A(V, A)$ has a right A-module structure defined, for each f in V^* and a in A, by

$$(fa)(v) = a^* f(v)$$

for all v in V.

An *α-sesquilinear form* (subsequently just called a *form* or *scalar product*) on a right A-module V is a biadditive map $Q\colon V \times V \to A$ satisfying

$$Q(ua, vb) = a^* Q(u, v) b$$

for all u, v in V and a, b in A. The set $\mathrm{Sesq}_\alpha(V)$ of forms on V is an additive abelian group. The formula:

$$[f(u)](v) = Q(u, v)$$

defines a group isomorphism $f \leftrightarrow Q$ between $\mathrm{Hom}_A(V, V^*)$ and $\mathrm{Sesq}_\alpha(V)$. A form Q is called *non-singular* if the corresponding homomorphism $f\colon V \to V^*$ is an isomorphism.

A form Q on V is called *ε-hermitian* if

$$Q(u, v) = Q(v, u)^* \varepsilon$$

for all u, v in V, and is called even *ε-hermitian* if

$$Q(u, v) = F(u, v) + F(v, u)^* \varepsilon$$

for some F in $\mathrm{Sesq}_\alpha(V)$ and all u, v in V.

To clarify these definitions, Wall defined a transposition operator

$$T_\varepsilon\colon \mathrm{Sesq}_\alpha(V) \to \mathrm{Sesq}_\alpha(V)$$

by $T_\varepsilon Q(u, v) = Q(v, u)^* \varepsilon$. This T_ε is a group homomorphism, $T_\varepsilon^2 = 1$, and $T_{-\varepsilon} = -T_\varepsilon$. The ε-hermitian forms make up the kernel of $1 - T_\varepsilon$, and the even ε-hermitian forms constitute the image of $1 + T_\varepsilon$. According to Wall's definition, a *quadratic form* on V is any element of the cokernel of $1 - T_\varepsilon$ (see [**15**, p. 120].)

For greater generality, following A. Bak (in [**2**, **3**]), we fix an additive subgroup Λ of A with the two properties:

i) $a^* \Lambda a \subseteq \Lambda$ for all a in A,

ii) $A_\varepsilon \subseteq \Lambda \subseteq A^\varepsilon$,

where

$$A_\varepsilon = \{a - a^* \varepsilon\colon\ a \in A\}$$
$$A^\varepsilon = \{a \in A\colon\ a = -a^* \varepsilon\}$$

For any right A-module V, we define $X(V, \alpha, \varepsilon, \Lambda)$ to be the additive group of all $(-\varepsilon)$-hermitian forms F on V for which $F(v, v) \in \Lambda$ for each v in V.

A *quadratic* (or more precisely an *(α, ε, Λ)-quadratic*) *form* on V is any element of the quotient group:

$$\mathrm{Sesq}_\alpha(V)/X(V, \alpha, \varepsilon, \Lambda).$$

If V is a finitely generated projective right A-module, then $X(V, \alpha, \varepsilon, A_\varepsilon)$ coincides with the image of $1 - T_\varepsilon$, as shown by the proof of Theorem 1.3 in [**3**]. So our quadratic forms include those of Wall. (The various L-groups are constructed from finitely generated projective modules with nonsingular forms.)

For any quadratic form

$$q = Q + X(V, \alpha, \varepsilon, \Lambda)$$

on V, we define an associated *length*

$$|\ |_q\colon V \to A/\Lambda \quad \text{by} \quad |v|_q = Q(v, v) + \Lambda$$

and an associated *scalar product* or *linearization*

$$(\,,)_q\colon V \times V \to A \quad \text{by} \quad (u, v)_q = Q(u, v) + Q(v, u)^* \varepsilon.$$

Neither of these depends on a choice of coset representative Q. In fact, a form is taken to its linearization by $1+T_\varepsilon=1-T_{-\varepsilon}$ which has kernel the $(-\varepsilon)$-hermitian forms, and image the even ε-hermitian forms on V. Clearly q is uniquely determined by its length map and linearization. If the even ε-hermitian form $(,)_q$ is non-singular, we call q *non-singular*.

The lengths and scalar products of elements u, v of V are related by the following useful identities:

$$|u+v|_q=|u|_q+|v|_q+(u,v)_q$$
$$(v,v)_q=x+x^*\varepsilon$$
$$|va|_q=a^*xa+\Lambda$$

for any x in $|v|_q$ and a in A.

When $\Lambda=A^\varepsilon$, the quadratic form q is uniquely determined by its linearization $(,)_q$, which can be *any* even ε-hermitian form on V. When Λ does not contain any nonzero ideals of A, then q is uniquely determined by its length map $|\ |_q$. (To see the latter, note that the additive subgroup of A generated by the values of $(,)_q$ is an ideal of A, contained in Λ if the length map is zero.)

Now $\Lambda=0$ if and only if $\varepsilon=1$, α is the identity, and A is commutative. This is the case in which $|\ |_q: V\to A$ is a classical quadratic form on V.

Another classical case is $\Lambda=A$. Then $\varepsilon=-1$, α is the identity, and A is commutative. In this case there is a bijection between the quadratic forms q on V and their linearizations, which are the alternating forms on V.

Remark. The definition of quadratic form used by A. Bak in [**1**, **2** and **3**], H. Bass in [**6**] and L.N. Vaserstein in [**13**] is just a special case of the definition presented here – namely the case where ε is central in A, so that α is an involution. The data $(A, \alpha, \varepsilon, \Lambda)$ is called a *form ring* by Bak in [3] and a *unitary ring* by Bass in [6]. In [**14**] and [**15**], C.T.C. Wall removes the hypothesis that ε is central, does not use Λ, and calls the data (A, α, ε) an *antistructure*.

5. Quadratic spaces and morphisms

If q is a quadratic form on the right A-module V, the pair (V, q) is called a *quadratic space*. If (V', q') is another quadratic space over the same A, α, ε and Λ, then an A-linear map $f: V\to V'$ is called a *morphism* $(V, q)\to(V', q')$ of quadratic spaces if

$$|f(v)|_{q'}=|v|_q \quad \text{and} \quad (f(v),f(w))_{q'}=(v,w)_q$$

for all v, w in V. With these morphisms, the $(A, \alpha, \varepsilon, \Lambda)$-quadratic forms become a category. A morphism f in this category is an isomorphism (i.e. invertible) if and only if it is bijective.

If $Q\in q$ and $Q'\in q'$ the form $Q\oplus Q'$ determines a quadratic form $q\oplus q'$ on $V\oplus V'$ which is independent of the choice of Q and Q'. Thus we can define the *orthogonal sum*:

$$(V,q)\perp(V',q)=(V\oplus V',q\oplus q')$$

as a binary operation on $(A, \alpha, \varepsilon, \Lambda)$-quadratic forms.

If a morphism $(V', q') \to (V, q)$ is an inclusion of modules $V' \subseteq V$, we call (V', q') a quadratic *subspace* of (V, q). In this case, if q' is non-singular, then (V', q') is an orthogonal summand of (V, q):

$$(V, q) \cong (V', q') \perp (V'', q'')$$

where V'' is the orthogonal complement of V' under $(,)_q$, and q'' is the coset of forms on V'' restricting those of q to V''.

6. Hyperbolic forms and Witt index

For any right A-module V, the *hyperbolic space* $H(V)$ is the quadratic space $(V \oplus V^*, q)$, where q is represented by the form Q defined by

$$Q((u, u'), (v, v')) = u'(v)$$

for all u, v in V and u', v' in V^*. Recall that V^* is a right A-module via α. If we make V^{**} into a right A-module via the anti-isomorphism α^{-1}, then the map $\beta: V \to V^{**}$, defined by

$$\beta(v)(v') = \alpha^{-1}(v'(v))$$

for all v' in V^*, is A-linear. It is routine to show that the hyperbolic form q (above) is non-singular if and only if β is an isomorphism. The latter condition does not involve A, and (according to Wall [**14**, p. 247]) it is independent of α, and is true when V is a finitely generated projective A-module.

Any quadratic space (V, q) can be embedded into the hyperbolic space $H(V)$ as follows: Pick Q in q, and send V to $V \oplus V^*$ by

$$v \to (v, Q(v, -)).$$

Of course, each choice of Q gives rise to a different embedding. If q is nonsingular, each such embedding can be extended to an isomorphism:

$$(V, q) \perp (V, -q) \cong H(V)$$

of quadratic spaces.

On the other hand, a quadratic space is measured by means of hyperbolic subspaces. The *Witt index*, $\operatorname{ind}(q)$, of (V, q) is the lagest $r \geq 0$ for which (V, q) contains a quadratic subspace isomorphic to $H(A^r)$. Since $H(A^r)$ is non-singular, it is then an orthogonal summand of (V, q).

If $v_1, \ldots, v_r$ is a basis of A^r, and $v'_1, \ldots, v'_r$ is the dual basis of $(A^r)^*$, and if q is the quadratic form in $H(A^r)$, the for each i, j with $i \neq j$,

$$|v_i|_q = |v'_i|_q = 0, \qquad (v'_i, v_i)_q = 1$$

and

$$(v_i, v_j)_q = (v'_i, v'_j)_q = (v'_i, v_j)_q = 0.$$

For an internal description of the Witt index in an arbitrary quadratic space (V, q), we therefore define a *hyperbolic pair* in (V, q) to be any (ordered) pair e, f in V satisfying the conditions:

$$|e|_q = |f|_q = 0 \quad \text{and} \quad (e, f)_q = 1.$$

A vector v in V is called *q-unimodular* if there is a vector w in V for which $(v, w)_q = 1$. In a hyperbolic pair e, f both e and f are q-unimodular, and every q-unimodular vector e with $|e|_q = 0$ can be included in a hyperbolic pair.

The A-linear span of a hyperbolic pair e, f is a subspace of (V, q) isomorphic to the hyperbolic plane $H(A)$ by $f \to 1 \in A$, $e \to$ identity map$\in A^*$. More generally, the span of mutually orthogonal hyperbolic pairs $e_1, f_1, \ldots, e_r, f_r$ is isomorphic to

$$H(A^r) \cong H(A) \perp \ldots \perp H(A) \qquad (r \text{ copies}).$$

So $\operatorname{ind}(q) \geqq r$ if and only if V contains r mutually orthogonal hyperbolic pairs.

7. The orthogonal group and transvections

Take A, α, ε, Λ, V and q to have the same meaning as above. The group of automorphisms of the quadratic space (V, q) is called the *orthogonal group*, $\mathcal{O}(q)$. They are the A-linear automorphisms of V which preserve lengths $|\ |_q$ and scalar products $(,)_q$.

Suppose e and u are elements of V with $|e|_q = 0$ and $(e, u)_q = 0$. Choose x in $|u|_q$. The map $\tau(e, u, x)$: $V \to V$ defined by

$$\tau(e, u, x)(v) = v + u(e, v)_q - e\varepsilon^*(u, v)_q - e\varepsilon^* x(e, v)_q$$

belongs to $\mathcal{O}(q)$. If e is q-unimodular, then $\tau(e, u, x)$ is called an *orthogonal transvection.*

8. Application of absolute stable rank

Theorem 8.1. *Suppose (V, q) is a quadratic space over A. Assume that either $\operatorname{ind}(q) \geqq \operatorname{asr}(A) + 2$, or that α is the identity map (so A is commutative) and $\operatorname{ind}(q) \geqq \operatorname{asr}(A) + 1$. Then $\mathcal{O}(q)$ acts transitively on the set of all q-unimodular vectors v in V with a given length $|v|_q$.*

Proof. Suppose $e_1, f_1, \ldots, e_n, f_n$ are n mutually orthogonal hyperbolic pairs in (V, q), where $n \geqq \operatorname{asr}(A) + 1$, and, if α is not trivial, $n \geqq \operatorname{asr}(A) + 2$. Suppose

$$v = \sum_{i=1}^{n} e_i a_i + \sum_{i=1}^{n} f_i b_i + u$$

$(a_i, b_i \in A,\ u \in V)$ is a q-unimodular vector with length $|v|_q = x + \Lambda$ $(x \in A)$, where u is orthogonal to all e_i, f_i. Note that the coefficients a_i, b_i (and hence the vector u) are uniquely determined by v, since

$$a_i^* = (v, f_i)_q \quad \text{and} \quad b_i = (e_i, v)_q.$$

We will perform a sequence of orthogonal transvections $\tau(e_i, ?, ?)$ and $\tau(f_i, ?, ?)$ on v to transform v to the standard vector $e_1 + f_1 x$ of the same length.

Step 1. Since v is q-unimodular, there is a vector w orthogonal to all e_i, f_i for which

$$\sum_{i=1}^{n} (Aa_i + Ab_i) + A(w, u)_q = A.$$

Since $\operatorname{sr}(A) \leqq n$, we can make

$$\sum_{i=1}^{n} (Aa_i + Ab_i) = A$$

if we replace v by

$$\prod_{i=1}^{n} \tau(e_i, wc_i, c_i^* yc_i)(v)$$

with appropriate c_i in A, where $y \in |w|_q$.

Step 2. Assume $\sum_{i=1}^{n} (Aa_i + Ab_i) = A$. Since $\operatorname{sr}(A) \leqq n-1$, we can make,

$$Ab_n + \sum_{i=1}^{n-1} (Aa_i + Ab_i) = A$$

if we replace v by

$$\tau\left(f_n, \sum_{i=1}^{n-1} e_i c_i, 0\right)(v)$$

with appropriate c_i in A.

Step 3. Assume $Ab_n + \sum_{i=1}^{n-1} (Aa_i + Ab_i) = A$. Replacing v by

$$\tau\left(e_n, \sum_{i=1}^{n-1} (e_i c_i + f_i d_i), 0\right)(v)$$

for appropriate c_i, d_i in A, we can make $a_n = 1 + zb_n$ for some z in A,

So far we have only used $\operatorname{sr}(A) \leqq n-1$, which follows from $\operatorname{sr}(A) \leqq \operatorname{asr}(A)$. At this point we bring to bear the absolute stable range condition, in an altered but equivalent form:

Lemma 8.2. *For any ring R and positive integer n,* $\operatorname{asr}(R) \leqq n$ *if and only if for each list* $r_0, r_1, \ldots, r_n$ *of elements from R, there exist* $t_0, t_1, \ldots, t_{n-1}$ *in R so that*

$$R(1+hr_n)+\sum_{i=0}^{n-1} R(r_i+t_i r_n)=R$$

for every h in R.

Proof. If $\operatorname{asr}(R) \leqq n$, use the same coefficients $t_0, \ldots, t_{n-1}$ which shorten $r_0, \ldots, r_n$.
For the converse, if r_n is not in a maximal left ideal M containing the $r_i+t_i r_n$ $(0 \leqq i \leqq n-1)$, then $-1=m+hr_n$ for some m in M and h in A. So $1+hr_n$ belongs to M, a contradiction.

Step 4. Assume that $a_n=1+zb_n$ for some z in A, and suppose α is the identity map ($a^*=a$ for all $a \in A$). Since $\operatorname{asr}(A) \leqq n-1$, we can apply Lemma 8.2 to the list $a_1, \ldots, a_{n-1}, b_n^2$; so there are c_1 in A with

$$A(1+hb_n^2)+\sum_{i=1}^{n-1} A(a_i+c_i b_n^2)=A$$

for all h in A.
Since α is trivial, A is a commutative ring. Let B denote the ideal

$$\sum_{i=1}^{n-1} A(a_i+c_i b_n^2).$$

Then $b_n^2 \in \operatorname{rad}(A/B)$; so also $b_n \in \operatorname{rad}(A/B)$, and

$$A(1+hb_n)+\sum_{i=1}^{n-1} A(a_i+c_i b_n^2)=A$$

for all h in A. So, if we replace v by

$$\tau\left(e_n, \sum_{i=1}^{n-1} e_i c_i b_n, 0\right)(v),$$

we then have $Aa_1+\ldots+Aa_n=A$.
Now consider the general case with $\operatorname{asr}(A) \leqq n-2$. Again assume that $a_n=1+zb_n$ for some z in A. Apply Lemma 8.2 to the list $b_1, a_2, \ldots, a_{n-1}$ to find c_i in A with

$$A(1+hb_1)+\sum_{i=2}^{n-1} A(a_i+c_i b_1)=A$$

for all h in A. Replacing v by

$$\tau\left(e_1, \sum_{i=2}^{n-1} e_i c_i, 0\right)(v),$$

we then have

$$A(1+hb_1)+\sum_{i=2}^{n-1} Aa_i=A.$$

Since $a_n=1+zb_n$, it follows that $Aa_n+Ab_n=A$. So we can choose c_n, d_n in A and replace v by

$$\tau(e_1, e_n c_n+f_n d_n, x)(v)$$

(where $x\in|e_n c_n+f_n d_n|_q$), to make

$$Aa_1+\ldots+Aa_{n-1}=A.$$

So again,

$$Aa_1+\ldots+Aa_n=A.$$

Step 5. Assume that $Aa_1+\ldots+Aa_n=A$. By replacing v with

$$\tau(f_j, e_i c_i \varepsilon^*, 0)(v) \qquad (i\neq j, c_i\in A)$$

we change a_i to $a_i+c_i a_j$ without affecting the other coefficients among $a_1, \ldots, a_n$. Since $\mathrm{sr}(A)\leqq n-1$, we can perform a sequence of such orthogonal transvections until $a_1=1$.

Step 6. Assume $a_1=1$. Replacing v by

$$\tau(f_1, -u\varepsilon^*, ?)\,\tau\left(f_1, -\sum_{i=2}^{n} f_i b_i \varepsilon^*, 0\right)\tau\left(f_1, -\sum_{i=2}^{n} e_i a_i \varepsilon^*, 0\right)(v)$$

results in $v=e_1+f_1 b_1$. Then

$$x+A=|v|_q=|e_1+f_1 b_1|_q=b_1+A.$$

And

$$\tau(f_1, 0, \varepsilon(b_1-x)\varepsilon^*)(e_1+f_1 b_1)=e_1+f_1 x,$$

completing the proof of Theorem 8.1. □

Corollary 8.3. (*Cancellation*) *Suppose* (V, q) *is a quadratic space with* $\mathrm{ind}(q)\geqq \mathrm{asr}(A)$. *If the anti-isomorphism* α *is not the identity map, assume further that* $\mathrm{ind}(q)\geqq \mathrm{asr}(A)+1$. *Suppose* (V', q') *and* (V'', q'') *are quadratic spaces,* V'' *is a finitely generated projective A-module,* q'' *is non-singular, and*

$$(V', q')\perp(V'', q'')\cong(V, q)\perp(V'', q'').$$

Then $(V', q')\cong(V, q)$.

Proof. Since (V'', q'') is isomorphic to an orthogonal summand of

$$H(A^n) \cong H(A) \perp \ldots \perp H(A) \quad (n \text{ copies})$$

for some positive integer n, it suffices to prove the cancellation in the case $(V'', q'') = H(A)$.

Choose mutually orthogonal hyperbolic pairs $e_2, f_2, \ldots, e_r, f_r$ $(r = \operatorname{ind}(q)+1)$ in (V, q) and let e_1, f_1 denote the standard hyperbolic pair in $H(A)$. Identify these pairs with their images in $(V, q) \perp H(A)$. By Theorem 8.1, applied to q-unimodular elements of length zero, we can compose the given isomorphism

$$(V', q') \perp H(A) \cong (V, q) \perp H(A)$$

with a sequence of orthogonal transvections on $(V, q) \perp H(A)$, so that the composite takes f_1 to itself, and hence takes e_1 to some

$$w = \sum_{i=1}^{n} e_i a_i + \sum_{i=1}^{n} f_i b_i + u$$

(a_i, b_i in A, u orthogonal to all e_i, f_i) for which w, f_1 is a hyperbolic pair. In particular, $a_1 = 1$. Just as in Step 6 of the proof of Theorem 8.1, a sequence of orthogonal transvections $\tau(f_1, ?, ?)$ will take w to e_1. Since $\tau(f_1, ?, ?)$ fixes f_1, the entire composite of the above isomorphisms takes the orthogonal summand $H(A)$ to itself. Since $H(A)$ is non-singular, this composite restricts to the desired isomorphism $(V', q') \cong (V, q)$. □

Note. The proof of Theorem 8.1 also works under the hypotheses: A is commutative, $\operatorname{ind}(q) \geqq \operatorname{asr}(A)+1$, and for all a in A, $\alpha(a) \in Aa$ (or equivalently α leaves ideals invariant). So the conclusion of Corollary 8.3 also works under the hypotheses: A is commutative, $\operatorname{ind}(q) \geqq \operatorname{asr}(A)$, and α leaves ideals invariant.

References

1. Bak, A.: On modules with quadratic forms. In: Algebraic K-Theory and its Geometric Applications (Lect. Notes Math. vol. 108, pp. 55–66) Berlin Heidelberg New York: Springer 1969
2. Bak, A.: Definitions and problems in surgery and related groups. Gen. Topol. Appl. **7**, 215–231 (1977)
3. Bak, A.: K-Theory of Forms. Ann. Math. Studies **98**, 1981
4. Bass, H.: K-Theory and stable algebra. Publ. Math. I.H.E.S. **22**, 5–60 (1964)
5. Bass, H.: Algebraic K-Theory. New York: W.A. Benjamin, Inc., 1968
6. Bass, H.: Unitary algebraic K-Theory. In: Algebraic K-Theory III. (Lect. Notes Math. vol. 343, pp. 57–265) Berlin Heidelberg New York: Springer 1973
7. Bass, H., Milnor, J., Serre, J.-P.: Solution of the congruence subgroup problem for SL_n $(n \geqq 3)$ and Sp_{2n} $(n \geqq 2)$. Publ. Math. I.H.E.S. **33**, 58–137 (1967)
8. Estes, D.R., Guralnick, R.M.: Module equivalences: Local to global. When primitive polynomials represent units. J. Algebra **77**, 138–157 (1982)
9. Estes, D.R., Ohm, J.: Stable range in commutative rings. J. Algebra **7**, 343–362 (1967)
10. Stein, M.R.: Stability theorems for K_1, K_2 and related functors modeled on Chevalley groups. Jpn. J. Math. **4**, 77–108 (1978)

11. Tits, J.: Formes quadratiques, groupes orthogonaux et algebres de Clifford. Invent. Math. **5**, 19–41 (1968)
12. Vaserstein, L.N.: Stable rank of rings and dimensions of topological spaces. Funct. Anal. Appl. **5**, 102–110 (1971); Funk. Anal. Pril. **5**, 17–27 (1971)
13. Vaserstein, L.N.: Stabilization for classical groups over rings. Math. USSR Sb. **22**, 271–303 (1975); Mat. Sb. **93**, 268–295 (1974)
14. Wall, C.T.C.: On the axiomatic foundation of the theory of hermitian forms. Proc. Camb. Philos. Soc. **67**, 243–250 (1970)
15. Wall, C.T.C.: On the classification of Hermitian forms II. Semisimple rings. Invent. Math. **18**, 119–141 (1972)

Oblatum 1-IX-1987