PACIFIC JOURNAL OF MATHEMATICS
Vol. 64, No. 2, 1976

POWER-CANCELLATION OF GROUPS AND MODULES

K. R. GOODEARL

This paper is concerned with deriving conditions which ensure that even though a module A may not necessarily cancel from a direct sum $A \oplus B \cong A \oplus C$, it can at least be concluded that $B^n \cong C^n$ for some positive integer n. This conclusion is obtained from a type of stable range condition on the endomorphism ring of A, which holds, for example, when A is a finitely generated module over any subring of a finite-dimensional Q-algebra. As an application of these methods to groups, it is shown that if A is a torsion-free abelian group of finite rank, and B, C are arbitrary groups (not necessarily abelian) such that $A \times B \cong A \times C$, then there exists a positive integer n such that the direct product of n copies of B is isomorphic to the direct product of n copies of C.

This research was partially supported by a National Science Foundation grant. The author would like to thank R. B. Warfield, Jr. for a number of very helpful conversations related to this material.

All rings in this paper are associative with unit, and all modules are unital. Most modules are right modules, so that endomorphism rings act on the left. The letter R always denotes a ring.

1. Introduction.

Let us say that a module A satisfies the *power-cancellation property* if for all modules B and C, $A \oplus B \cong A \oplus C$ implies that $B^n \cong C^n$ for some positive integer n. (Here B^n denotes the direct sum of n copies of B.) The objective of this paper is to derive sufficient conditions for power-cancellation. We obtain power-cancellation from a stronger property called *power-substitution*: Given any decomposition $M = A_1 \oplus B_1 = A_2 \oplus B_2$ with each $A_i \cong A$, there must exist a positive integer n such that B_1^n and B_2^n have a common complement in M^n. Power-substitution depends only on the endomorphism ring of A, and is equivalent to a condition resembling the stable range conditions of algebraic K-theory. Because the derivation of power-cancellation from power-substitution is directly analogous to the derivation of cancellation theorems from the stable range conditions, we begin by recalling the appropriate stable range results.

DEFINITION. A ring R is said to have 1 *in the stable range* provided that whenever $ax + b = 1$ in R, there exists $y \in R$ such that $a + by$ is a unit in R. (It can be shown that this definition is left-right symmetric.)

For example, every artinian ring has 1 in the stable range [**12**, Lemma 11.8].

The following theorem shows that 1 in the stable range is equivalent to a substitution property. It was first proved by Fuchs for quasi-projective modules with projective covers [**2**, Theorem 3], then for arbitrary modules by Warfield [**14**].

THEOREM 1.1. [**14**, Theorem 1] *Let A be a right R-module, and set $E = \mathrm{End}_R(A)$. Then E has 1 in the stable range if and only if for any right R-module decomposition $M = A_1 \oplus B_1 = A_2 \oplus B_2$ with each $A_i \cong A$, there exists a submodule $C \leqq M$ such that $M = C \oplus B_1 = C \oplus B_2$.*

The substitution property expressed in Theorem 1.1 clearly implies that $B_1 \cong B_2$, which yields a proof of the following theorem.

THEOREM 1.2. [**1**, Theorem 2] *Let A be a right R-module such that $\mathrm{End}_R(A)$ has 1 in the stable range. If B and C are any right R-modules such that $A \oplus B \cong A \oplus C$, then $B \cong C$.*

There are analogous substitution and cancellation results connected with the higher stable range conditions. Since some of these results will be needed later in the paper, we recall them here.

DEFINITION. A row $(a_1, \cdots, a_r)$ of elements from a ring R is said to be a *right unimodular row* if $\Sigma\, a_i R = R$. Given a positive integer n, a ring R is said to have *n in the stable range* provided that for any right unimodular row $(a_1, \cdots, a_r)$ of $r \geqq n+1$ elements of R, there exist elements $b_1, \cdots, b_{r-1} \in R$ such that the row $(a_1 + a_r b_1, \cdots, a_{r-1} + a_r b_{r-1})$ is right unimodular. (As above, this property can be shown to be left-right symmetric. Also, the case $n = 1$ of this definition is easily seen to be equivalent to the previous definition of 1 in the stable range.)

THEOREM 1.3. [**14**, Theorem 6] *Let A be a right R-module, set $E = \mathrm{End}_R(A)$, and let n be a positive integer. Then E has n in the stable range if and only if for any right R-module decomposition*

$$M = A_1 \oplus \cdots \oplus A_n \oplus B_1 = A_{n+1} \oplus B_2$$

with all $A_i \cong A$, there exist submodules $C \leqq M$ and $L \leqq A_1 \oplus \cdots \oplus A_n$ such that $M = C \oplus L \oplus B_1 = C \oplus B_2$.

THEOREM 1.4. [**14**, Theorem 7] *Let A be a right R-module such that $\mathrm{End}_R(A)$ has n in the stable range, for some positive integer n. If B and C are any right R-modules such that $A \oplus B \cong A \oplus C$ and B has a direct summand isomorphic to A^n, then $B \cong C$.*

2. Power-substitution. We use $M_n(R)$ to denote the ring of all $n \times n$ matrices over a ring R, and we use I to denote the identity matrix in any $M_n(R)$. Given $r \in R$ and $P \in M_n(R)$, we write rP and Pr for the matrices obtained from P by multiplying each entry on the left (right) by r. In particular, $rI = Ir$ is the diagonal matrix with all diagonal entries equal to r.

THEOREM 2.1. *Let A be a right R-module, and set $E = \mathrm{End}_R(A)$. Then the following conditions are equivalent:*

(a) *Given any right R-module decomposition $M = A_1 \oplus B_1 = A_2 \oplus B_2$ with each $A_i \cong A$, there exist a positive integer n and a submodule $C \leqq M^n$ such that $M^n = C \oplus B_1^n = C \oplus B_2^n$.*

(b) *If $ax + b = 1$ in E, then there exist a positive integer n and a matrix $Q \in M_n(E)$ such that $aI + bQ$ is a unit in $M_n(E)$.*

Proof. Given any positive integer n, there is an additive functor from Mod-$R \to$ Mod-R which carries any module D to D^n. For any map $f: D \to E$, we use f^* to denote the image of f under this functor. Thinking of f^* as an $n \times n$ matrix with entries from $\mathrm{Hom}_R(D, E)$, f^* is a diagonal matrix with all diagonal entries equal to f.

(a) $\Rightarrow$ (b): Set $M = A^2$, and let $p_i: M \to A$, $q_i: A \to M$ (for $i = 1, 2$) denote the projections and injections of this direct sum. Set $A_1 = q_1(A)$ and $B_1 = q_2(A)$, so that $M = A_1 \oplus B_1$ with $A_1 \cong A$. Define maps $f = ap_1 + bp_2$ from $M \to A$ and $g = q_1 x + q_2$ from $A \to M$. Observing that $fg = ax + b = 1_A$, we see that $M = g(A) \oplus (\ker f)$. Set $A_2 = g(A)$ and $B_2 = \ker f$, so that $M = A_2 \oplus B_2$ with $A_2 \cong A$.

According to (a), there exist $n > 0$ and $C \leqq M^n$ such that $M^n = C \oplus B_1^n = C \oplus B_2^n$. Since C and A_1^n are both complements for B_1^n in M^n, we see that $C \cong A_1^n \cong A^n$. As a result, there exists a monomorphism $h: A^n \to M^n$ such that $h(A^n) = C$. Inasmuch as $p_1^*: M^n \to A^n$ is an epimorphism and

$$M^n = C \oplus B_1^n = h(A^n) \oplus (\ker p_1^*),$$

we infer that $p_1^* h: A^n \to A^n$ is an isomorphism. Similarly, f^* is an epimorphism and

$$M^n = C \oplus B_2^n = h(A^n) \oplus (\ker f^*),$$

whence $f^* h$ is an isomorphism. Observing that $f^* h = a^* p_1^* h + b^* p_2^* h$, we conclude that $a^* + b^* p_2^* h (p_1^* h)^{-1}$ is an automorphism of A^n.

Identifying $\mathrm{End}_R(A^n)$ with $M_n(E)$ in the obvious manner, we thus have $Q = p_2^* h (p_1^* h)^{-1}$ in $M_n(E)$ such that $aI + bQ = a^* + b^* Q$ is a unit in $M_n(E)$.

(b) $\Rightarrow$ (a): Using the decomposition $M = A_1 \oplus B_1 \cong A \oplus B_1$, we obtain projections $p_1\colon M \to A$, $p_2\colon M \to B_1$ and injections $q_1\colon A \to M$, $q_2\colon B_1 \to M$ such that $p_1q_1 = 1_A$, $q_1p_1 + q_2p_2 = 1_M$, and $\ker p_1 = B_1$. Using the decomposition $M = A_2 \oplus B_2 \cong A \oplus B_2$, we obtain a projection $f\colon M \to A$ and an injection $g\colon A \to M$ such that $fg = 1_A$ and $\ker f = B_2$.

Now $1_A = f(q_1p_1 + q_2p_2)g = (fq_1)(p_1g) + (fq_2p_2g)$. Setting $a = fq_1$, $x = p_1g$, and $b = fq_2p_2g$, we thus have $a, x, b \in E$ such that $ax + b = 1$. According to (b), there exist $n > 0$ and $Q \in M_n(E)$ such that $aI + bQ$ is a unit in $M_n(E)$. Using the identification of $M_n(E)$ with $\mathrm{End}_R(A^n)$, we thus obtain a map $h\colon A^n \to A^n$ such that $(f^*q_1^*) + (f^*q_2^*p_2^*g^*)h = a^* + b^*h$ is an automorphism of A^n.

Set $k = q_1^* + q_2^*p_2^*g^*h\colon A^n \to M^n$ and $C = k(A^n)$. Since f^*k is an isomorphism, we infer that $M^n = k(A^n) \oplus (\ker f^*) = C \oplus B_2^n$. Similarly, $p_1^*k = p_1^*q_1^*$ is the identity map on A^n, whence $M^n = k(A^n) \oplus (\ker p_1^*) = C \oplus B_1^n$.

DEFINITION. We say that a right R-module A has the *power-substitution property* if A satisfies condition (a) of Theorem 2.1. We say that a ring E has the *right power-substitution property* if the right module E_E has the power-substitution property, or, equivalently, if E satisfies condition (b) of Theorem 2.1. Obviously there is a *left* power-substitution property as well, but we do not know whether it is equivalent to right power-substitution.

COROLLARY 2.2. *Let A be a right R-module such that $\mathrm{End}_R(A)$ has the right power-substitution property. If B and C are any right R-modules such that $A \oplus B \cong A \oplus C$, then $B^n \cong C^n$ for some positive integer n.*

Obviously any ring which has 1 in the stable range also satisfies right power-substitution, and there is a sense in which power-substitution and stable range 1 are nearly equivalent. Given a ring R and positive integers k, n such that $k \mid n$, there is a natural ring map $M_k(R) \to M_n(R)$. Considering the positive integers as a directed set ordered by divisibility, we thus obtain a directed system of matrix rings over R, and we can form the direct limit $S = \varinjlim M_n(R)$. It is clear from the definitions that S has 1 in the stable range if and only if every $M_n(R)$ satisfies right power-substitution. It it were proved that right power-substitution is preserved in matrix rings, this would show that R satisfies right power-substitution if and only if S has stable range 1. (In addition, because of the left-right symmetry of stable range 1, it would follow that power-substitution is left-right symmetric.)

In general, power-substitution is weaker than stable range 1. For example, $\mathbf{Z}$ has power-substitution (Corollary 3.4), but it is easily checked

that **Z** does not have 1 in the stable range. More generally, if F is any algebraic field extension of **Q**, then every subring of F satisfies power-substitution (Corollary 3.12). In particular, the ring of algebraic integers in any algebraic number field satisfies power-substitution. This might lead one to expect that power-substitution is a property of Dedekind domains, or perhaps at least of principal ideal domains. This is false, however, for the polynomial ring $F[x]$ over any field F of characteristic zero never satisfies power-substitution (Corollary 3.8). For noncommutative examples of power-substitution, we have any ring R whose additive group has finite rank (Theorem 4.12).

We also have examples to show that power-substitution does not in general imply any of the stable range conditions. If X is a compact Hausdorff space and $C(X)$ is the ring of all continuous real-valued functions on X, then we claim that $C(X)$ satisfies power-substitution. For if $ax + b = 1$ in $C(X)$, then the functions a, b are not both zero anywhere, whence $a^2 + b^2 > 0$ everywhere. As a result, $aI + b\begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$, which has determinant $a^2 + b^2$, is a unit in $M_2(C(X))$.

As shown in [**11**, pp. 264–269], there is a category equivalence Γ between the real vector bundles over X and the finitely generated projective $C(X)$-modules. For a given positive integer n, let τ^n denote the tangent bundle to the n-sphere S^n. Then $\Gamma(\tau^n) \oplus C(S^n)$ is free of rank $n+1$, but $\Gamma(\tau^n)$ is not free unless $n = 0, 1, 3, 7$ [**11**, Example 1, p. 269]. Thus for $n > 7$, $C(S^n) \oplus C(S^n)^n \cong C(S^n) \oplus \Gamma(\tau^n)$ and $C(S^n)^n \ncong \Gamma(\tau^n)$, hence we see from Theorem 1.4 that $C(S^n)$ does not have n in the stable range.

Now let Y be a disjoint union of the spheres $S^1, S^2, S^3, \cdots$, and let X be the Stone-Čech compactification of Y. Inasmuch as any bounded continuous map of Y into **R** extends to a continuous map of X into **R**, we see that the various restriction maps $C(X) \to C(S^n)$ are surjective, i.e., $C(S^n)$ is isomorphic to a factor ring of $C(X)$. Since $C(S^n)$ does not have n in the stable range for $n > 7$, we see that $C(X)$ does not have *any* n in the stable range, although $C(X)$ does satisfy power-substitution.

Theorem 2.1 and Corollary 2.2 can be used to show that certain abelian groups enjoy power-cancellation in the category of abelian groups. However, by taking a little care with the proof of Theorem 2.1, we can actually show that such abelian groups enjoy power-cancellation in the category of all groups. We must be careful with our notation in this situation. In order to avoid ambiguities, we use $\times^n G$ to denote the direct product of n copies of a group G. Given any subgroup H of G, we identify $\times^n H$ with its canonical image in $\times^n G$. Also, we identify the factors in a direct product of groups with the appropriate normal subgroups of the product group.

THEOREM 2.3. *Let A be an abelian group with the power-substitution property. Given any group M* (not necessarily abelian) *and decompositions $M = A_1 \times B_1 = A_2 \times B_2$ with each $A_i \cong A$, there exist a positive integer n and a normal subgroup $C \subseteq \times^n M$ such that $\times^n M = C \times (\times^n B_1) = C \times (\times^n B_2)$.*

Proof. As in Theorem 2.1, given a group homomorphism $f\colon G \to H$, we use f^* to denote the induced homomorphism $\times^n G \to \times^n H$.

Using the decomposition $M = A_1 \times B_1 \cong A \times B_1$, we obtain projections $p_1\colon M \to A$, $p_2\colon M \to B_1$ and injections $q_1\colon A \to M$, $q_2\colon B_1 \to M$ such that p_1q_1 is the identity map on A, $\ker p_1 = B_1$, and $[q_1p_1(x)][q_2p_2(x)] = x$ for all $x \in M$. Using the decomposition $M = A_2 \times B_2 \cong A \times B_2$, we obtain a projection $f\colon M \to A$ and an injection $g\colon A \to M$ such that fg is the identity map on A and $\ker f = B_2$. Since A is abelian, we see from these decompositions that $g(A)$ and $q_1(A)$ are contained in the center of M. For any $x \in A$, we thus have $q_2p_2g(x) = [q_1p_1g(x)]^{-1}g(x)$ in the center of M. Therefore q_2p_2g maps A into the center of M.

Clearly $[fq_1p_1g(x)][fq_2p_2g(x)] = fg(x) = x$ for all $x \in A$. Since fq_1, p_1g, and fq_2p_2g all belong to the ring $E = \mathrm{End}(A)$, this translates into additive notation as $(fq_1)(p_1g) + (fq_2p_2g) = 1$ in E. Inasmuch as A has the power-substitution property, E satisfies right power-substitution, hence we may proceed as in Theorem 2.1 to find $n > 0$ and an endomorphism h of $\times^n A$ such that $f^*q_1^* + f^*q_2^*p_2^*g^*h$ is an automorphism of $\times^n A$.

Inasmuch as q_1 and q_2p_2g map A into the center of M, we see that q_1^* and $q_2^*p_2^*g^*$ map $\times^n A$ into the center of $\times^n M$. As a result, the rule $k(x) = [q_1^*(x)][q_2^*p_2^*g^*h(x)]$ defines a homomorphism k of $\times^n A$ into the center of $\times^n M$, whence $C = k(\times^n A)$ is a normal subgroup of $\times^n M$. Since $p_1^*k = p_1^*q_1^*$ is the identity map on $\times^n A$, we thus obtain $\times^n M = C \times (\ker p_1^*) = C \times (\times^n B_1)$. We also know that $f^*k = f^*q_1 + f^*q_2^*p_2^*g^*h$ is an automorphism of $\times^n A$, from which we obtain $\times^n M = C \times (\ker f^*) = C \times (\times^n B_2)$.

COROLLARY 2.4. *Let A be an abelian group whose endomorphism ring has the right power-substitution property. If B and C are any groups* (not necessarily abelian) *such that $A \times B \cong A \times C$, then $\times^n B \cong \times^n C$ for some positive integer n.*

PROPOSITION 2.5. *Let K be a two-sided ideal of R.*

(a) *If R satisfies right power-substitution, then so does R/K.*

(b) *If $K \subseteq J(R)$ and R/K satisfies right power-substitution, then so does R.*

Proof. (a) is trivial.

(b) If $ax + b = 1$ in R, then $\overline{a}\overline{x} + \overline{b} = 1$ in R/K, hence there exist

$n > 0$ and $Q \in M_n(R)$ such that $\bar{a}I + \overline{bQ}$ is a unit in $M_n(R/K)$. Thus we have $aI + bQ \in M_n(R)$ which maps to a unit modulo $M_n(K) \subseteq J(M_n(R))$, whence $aI + bQ$ is a unit in $M_n(R)$.

PROPOSITION 2.6. *Let e be an idempotent in R. If R satisfies right power-substitution, then so does eRe.*

Proof. Suppose that $a, x, b \in eRe$ with $ax + b = e$. Then $(a + 1 - e)(x + 1 - e) + b = 1$ in R, so there exist $n > 0$ and $Q \in M_n(R)$ such that $(a + 1 - e)I + bQ$ is a unit in $M_n(R)$. Set $T = [(a + 1 - e)I + bQ]^{-1}$, and note that $eT[(a + 1 - e)I + bQ] = eI$. Multiplying this equation on the right by e, we obtain $eT[aI + bQe] = eI$; multiplying it on the right by $1 - e$, we obtain $eT[(1 - e)I + bQ(1 - e)] = 0$. Combining these two results, we find that

$$eT[aI + bQ] = eT[aI + bQe] + eT[bQ(1 - e)] = eI - eT(1 - e).$$

As a result, we obtain

$$[eT + (1 - e)I][(a + 1 - e)I + bQ] = eT[aI + bQ] + eT(1 - e) + (1 - e)I = I,$$

and consequently $eT + (1 - e)I = [(a + 1 - e)I + bQ]^{-1} = T$.

We now observe that $Te = eTe$, whence

$$eI = [(a + 1 - e)I + bQ]Te = [(a + 1 - e)I + bQ]eTe = [aI + beQe]eTe.$$

On the other hand, we have seen above that $eT[aI + bQe] = eI$, whence $eTe[aI + beQe] = eI$. Therefore we have $eQe \in M_n(eRe)$ such that $aI + beQe$ is a unit in $M_n(eRe)$.

The obvious complement to Proposition 2.6 would be to prove that if R satisfies right power-substitution, then so does any $M_n(R)$. We do not know whether this is true. However, we do have partial results in this direction, which are needed later in the paper. They require the following lemma, which was suggested by R. B. Warfield, Jr.

LEMMA 2.7. *Let k be a positive integer, and let A be a right R-module such that $\mathrm{End}_R(A)$ has k in the stable range. Given any right R-module decomposition*

$$M = A_{11} \oplus \cdots \oplus A_{1n} \oplus B_1 = A_{21} \oplus \cdots \oplus A_{2n} \oplus B_2$$

with $n \geqq k$ and all $A_{ij} \cong A$, there exist submodules $C, D, H \leqq M$ such that

$$M = C \oplus D \oplus H \oplus B_1 = C \oplus D \oplus A_{21} \oplus \cdots A_{2,k-1} \oplus B_2$$

and $D \cong A$, $D \oplus H \cong A^k$.

Proof. We first claim that there exist $C, J \leqq M$ such that

$$M = C \oplus J \oplus B_1 = C \oplus A_{21} \oplus \cdots \oplus A_{2k} \oplus B_2$$

and $J \cong A^k$. If $n = k$, take $C = 0$ and $J = A_{11} \oplus \cdots \oplus A_{1k}$. Now let $n > k$, and assume that the claim holds for $n - 1$.

Using the case $n - 1$ on the decomposition

$$M = A_{11} \oplus \cdots \oplus A_{1,n-1} \oplus (A_{1n} \oplus B_1) = A_{21} \oplus \cdots \oplus A_{2,n-1} \oplus (A_{2n} \oplus B_2),$$

we obtain $D, K \leqq M$ such that

$$M = D \oplus K \oplus A_{1n} \oplus B_1 = D \oplus A_{21} \oplus \cdots \oplus A_{2k} \oplus A_{2n} \oplus B_2$$

and $K \cong A^k$. Write $K = A'_{11} \oplus \cdots \oplus A'_{1k}$ with each $A'_{1j} \cong A$. We now have a decomposition

$$\begin{aligned} M &= A'_{11} \oplus \cdots \oplus A'_{1k} \oplus (A_{1n} \oplus B_1 \oplus D) \\ &= A_{2n} \oplus (A_{21} \oplus \cdots \oplus A_{2k} \oplus B_2 \oplus D) \end{aligned}$$

with $A'_{11} \cong \cdots \cong A'_{1k} \cong A_{2n} \cong A$.

Since $\mathrm{End}_R(A)$ has k in the stable range, Theorem 1.3 shows that there exist $E, L \leqq M$ such that

$$M = E \oplus L \oplus A_{1n} \oplus B_1 \oplus D = E \oplus A_{21} \oplus \cdots \oplus A_{2k} \oplus B_2 \oplus D.$$

Now E and A_{2n} are complements for $A_{21} \oplus \cdots \oplus A_{2k} \oplus B_2 \oplus D$ in M, whence $E \cong A_{2n} \cong A$. Also, $E \oplus L$ and K are complements for $A_{1n} \oplus B_1 \oplus D$ in M, hence

$$L \oplus A_{1n} \cong A \oplus L \cong E \oplus L \cong K \cong A^k.$$

Setting $C = D \oplus E$ and $J = L \oplus A_{1n}$, we thus have

$$M = C \oplus J \oplus B_1 = C \oplus A_{21} \oplus \cdots \oplus A_{2k} \oplus B_2$$

with $J \cong A^k$. Thus the claim is proved.

By virtue of this claim, we obtain a decomposition

$$M = A''_{11} \oplus \cdots \oplus A''_{1k} \oplus (B_1 \oplus C) = A_{2k} \oplus (A_{21} \oplus \cdots \oplus A_{2,k-1} \oplus B_2 \oplus C)$$

with $A''_{11} \cong \cdots \cong A''_{1k} \cong A_{2k} \cong A$. Using Theorem 1.3 again, there exist $D, H \leqq M$ such that

$$M = D \oplus H \oplus B_1 \oplus C = D \oplus A_{21} \oplus \cdots \oplus A_{2,k-1} \oplus B_2 \oplus C.$$

As above, we conclude that $D \cong A$ and $D \oplus H \cong A^k$.

PROPOSITION 2.8. *Let k be a positive integer, and let R be a ring which has k in the stable range. If $M_k(R)$ satisfies right power-substitution, then so does $M_n(R)$, for all n.*

Proof. In view of Proposition 2.6, we need only consider the case $n > k$. Setting $A = R_R$, we are given that the module A^k has the power-substitution property, and we must prove it for A^n.

Thus consider any right R-module decomposition $M = A_1 \oplus B_1 = A_2 \oplus B_2$ in which each $A_i \cong A^n$. Write each $A_i = A_{i1} \oplus \cdots \oplus A_{in}$, where all $A_{ij} \cong A$. According to Lemma 2.7, there exist $C, D, H \leqq M$ such that

$$\begin{aligned} M &= C \oplus D \oplus H \oplus B_1 = C \oplus D \oplus A_{21} \oplus \cdots \oplus A_{2,k-1} \oplus B_2 \\ &= (D \oplus H) \oplus (B_1 \oplus C) = (A_{21} \oplus \cdots \oplus A_{2,k-1} \oplus D) \oplus (B_2 \oplus C) \end{aligned}$$

and $D \cong A$, $D \oplus H \cong A^k$. Since A^k has the power-substitution property, there must exist $s > 0$ and $E \leqq M^s$ such that

$$\begin{aligned} M^s &= E \oplus (B_1 \oplus C)^s = E \oplus (B_2 \oplus C)^s \\ &= (E \oplus C^s) \oplus B_1^s = (E \oplus C^s) \oplus B_2^s. \end{aligned}$$

Therefore A^n has power-substitution.

PROPOSITION 2.9. *Let R be a commutative ring which has 2 in the stable range. If R satisfies power-substitution, then so does $M_n(R)$, for all n.*

Proof. With $A = R_R$, we must prove that the module A^n has power-substitution, for all $n \geqq 2$.

Thus consider any R-module decomposition $M = A_1 \oplus B_1 = A_2 \oplus B_2$ in which each $A_i \cong A^n$. Write each $A_i = A_{i1} \oplus \cdots \oplus A_{in}$, where all $A_{ij} \cong A$. According to Lemma 2.7, there exist $C, D, H \leqq M$ such that

$$\begin{aligned} M &= C \oplus D \oplus H \oplus B_1 = C \oplus D \oplus A_{21} \oplus B_2 \\ &= H \oplus (B_1 \oplus C \oplus D) = A_{21} \oplus (B_2 \oplus C \oplus D) \end{aligned}$$

and $D \cong A$, $D \oplus H \cong A^2$. Now H is an R-module such that $R \oplus H \cong R \oplus R$, whence $H \cong R = A$ [**6**, Theorem, p. 76]. As a result, there must exist $k > 0$ and $E \leqq M^k$ such that

$$\begin{aligned} M^k &= E \oplus (B_1 \oplus C \oplus D)^k = E \oplus (B_2 \oplus C \oplus D)^k \\ &= (E \oplus C^k \oplus D^k) \oplus B_1^k = (E \oplus C^k \oplus D^k) \oplus B_2^k. \end{aligned}$$

Therefore A^n has power-substitution.

3. Commutative examples.

LEMMA 3.1. *Let R be a commutative ring. Given elements $a, b, a_1, \cdots, a_n \in R$, there exists a matrix $Q \in M_n(R)$ such that*

$$\det(aI + bQ) = a^n + a_1 a^{n-1} b + a_2 a^{n-2} b^2 + \cdots + a_n b^n.$$

Proof. Set

$$Q = \begin{bmatrix} a_1 & -a_2 & a_3 & \cdots & (-1)^{n+1} a_n \\ 1 & 0 & 0 & \cdots & 0 \\ 0 & 1 & 0 & \cdots & 0 \\ & & \vdots & & \\ 0 & 0 & \cdots & 1 & 0 \end{bmatrix}$$

so that

$$aI + bQ = \begin{bmatrix} a + a_1 b & -a_2 b & a_3 b & \cdots & (-1)^{n+1} a_n b \\ b & a & 0 & \cdots & 0 \\ 0 & b & a & \cdots & 0 \\ & & \vdots & & \\ 0 & 0 & \cdots & b & a \end{bmatrix}$$

The lemma clearly holds for $n = 1, 2$.

Now let $n > 2$, and expand $\det(aI + bQ)$ by the right-hand column, which yields

$$a_n b \begin{vmatrix} b & a & 0 & \cdots & 0 \\ 0 & b & a & \cdots & 0 \\ & & \vdots & & \\ 0 & 0 & \cdots & b & a \\ 0 & 0 & \cdots & 0 & b \end{vmatrix} + a \begin{vmatrix} a + a_1 b & -a_2 b & a_3 b & \cdots & (-1)^n a_{n-1} b \\ b & a & 0 & \cdots & 0 \\ 0 & b & a & \cdots & 0 \\ & & \vdots & & \\ 0 & 0 & \cdots & b & a \end{vmatrix}$$

The first determinant is clearly b^n, while the second (by induction), is $a^{n-1} + a_1 a^{n-2} b + \cdots + a_{n-1} b^{n-1}$, which yields the desired result.

PROPOSITION 3.2. *A commutative ring R satisfies the power-substitution property if and only if whenever $ax + b = 1$ for some $a, x, b \in R$, there exist a positive integer n and an element $y \in R$ such that $a^n + by$ is a unit in R.*

Proof. First assume that R satisfies power-substitution. Given $ax + b = 1$ in R, there exist $n > 0$ and $Q \in M_n(R)$ such that $aI + bQ$ is a unit in $M_n(R)$. Then $\det(aI + bQ)$ is a unit in R, and we observe that $\det(aI + bQ) = a^n + by$ for some $y \in R$.

Conversely, let $ax + b = 1$ in R and assume that $a^n + by$ is a unit in R, for some $n > 0$ and some $y \in R$. Now

$$a^n + by = a^n + by(ax + b)^{n-1} = a^n + a_1 a^{n-1} b + a_2 a^{n-2} b^2 + \cdots + a_n b^n$$

for suitable $a_1, \cdots, a_n \in R$. According to Lemma 3.1, there exists $Q \in M_n(R)$ for which $\det(aI + bQ) = a^n + by$, whence $aI + bQ$ is a unit in $M_n(R)$.

COROLLARY 3.3. *Let R be a commutative ring such that for all nonzero $b \in R$, the group of units of R/bR is torsion.* (In particular, this holds if R/bR is finite for all nonzero $b \in R$.) *Then R satisfies power-substitution.*

Proof. Let $ax + b = 1$ in R. If $b = 0$, then $a^1 + b0$ is a unit, hence we may now assume that $b \neq 0$. Then a maps to an element $\bar{a}$ in the group of units of R/bR. Since this group is torsion, we must have $\bar{a}^n = 1$ for some $n > 0$, hence $a^n + by = 1$ for some $y \in R$.

COROLLARY 3.4. *All subrings of $\mathbf{Q}$ satisfy power-substitution.*

COROLLARY 3.5. *If F is a field which is an algebraic extension of a finite field, then the polynomial ring $F[x]$ satisfies power-substitution.*

Proof. Since F is algebraic over a finite field, it must be a directed union of finite subfields F_i, whence $F[x]$ is a directed union of the subrings $F_i[x]$. Each such $F_i[x]$ satisfies power-substitution by Corollary 3.3, from which we conclude that $F[x]$ satisfies power-substitution.

LEMMA 3.6. *Let R be a commutative ring, let $a, b, c, d \in R$, and set $f = x^2 + cx + d$ in $R[x]$. If there exists $g \in R[x]$ such that $a + bx + fg$ is a unit in $R[x]$, then b is nilpotent.*

Proof. Consider any prime ideal P of R, and map everything into $(R/P)[x]$, where $\bar{a} + \bar{b}x + \bar{f}g$ is a unit. If $\bar{g} \neq 0$, then $\deg(\bar{f}\bar{g}) \geqq 2$ and so $\deg(\bar{a} + \bar{b}x + \bar{f}\bar{g}) \geqq 2$, which is impossible. Thus $\bar{g} = 0$, so that $\bar{a} + \bar{b}x$ is a unit in $(R/P)[x]$. As a result, $\bar{b} = 0$, i.e., $b \in P$.

Therefore b lies in all prime ideals of R and thus is nilpotent.

THEOREM 3.7. *Let R be a commutative ring. Then the polynomial ring $R[x]$ satisfies power-substitution if and only if*

(a) *R has positive characteristic.*

(b) *The group of units of R is torsion.*

(c) *R has Krull dimension zero.*

Proof. First assume that $R[x]$ satisfies power-substitution. Since $(1+x)(1-x)+x^2 = 1$, there exist $n > 0$ and $t \in R[x]$ such that $(1+x)^n + x^2 t$ is a unit in $R[x]$. Observing that $(1+x)^n + x^2 t = 1 + nx + x^2 g$ for some $g \in R[x]$, we see from Lemma 3.6 that n is nilpotent in R, i.e., $n^k R = 0$ for some $k > 0$. Thus R has positive characteristic.

Next consider any unit $a \in R$, and observe that

$$(ax + 1 - x)(a^{-1}x + 1 - x) + (x^2 - x)(a + a^{-1} - 2) = 1.$$

Then there exist $n > 0$ and $t \in R[x]$ such that $(ax + 1 - x)^n + (x^2 - x)t$ is a unit in $R[x]$. Observing that x and $1 - x$ are orthogonal idempotents modulo $x^2 - x$, we see that

$$(ax + 1 - x)^n + (x^2 - x)t = a^n x + 1 - x + (x^2 - x)g$$

for some $g \in R[x]$. According to Lemma 3.6, the element $c = a^n - 1$ must be nilpotent, hence $c^k = 0$ for some $k > 0$. Inasmuch as $pR = 0$ for some positive integer p, we compute that $(1+c)^{p^k} = 1 + c^{p^k} = 1$, i.e., $a^{np^k} = 1$. Thus the group of units of R is torsion.

If R is not zero-dimensional, then it has a prime ideal P which is not maximal. Set $S = R/P$, and note from Proposition 2.5 that $S[x]$ has power-substitution. Now S is a domain but not a field, hence there exists a nonzero element $a \in S$ which is not a unit. Obviously $ax + (1 - ax) = 1$, whence there exist $n > 0$ and $t \in S[x]$ such that $a^n + (1 - ax)t$ is a unit in $S[x]$. Since S is a domain, this can only happen for $t = 0$. But then a^n is a unit in S and so a is a unit, which is false. Therefore R must be zero-dimensional.

Conversely, assume that (a), (b), (c) hold. Since R is zero-dimensional, $J(R)$ is nil and $R/J(R)$ is von Neumann regular. Inasmuch as the natural map from the group of units of R to the group of units of $R/J(R)$ is surjective, we see that the group of units of $R/J(R)$ is

torsion. Thus $R/J(R)$ satisfies conditions (a), (b), (c). Since $J(R)$ is nil, so is $J(R)[x]$, whence $J(R)[x] \subseteq J(R[x])$. According to Proposition 2.5, it thus suffices to prove that $(R/J(R))[x]$ has power-substitution. Therefore we may assume, without loss of generality, that R is von Neumann regular.

We claim that for any $M \in \mathrm{Spec}(R)$, $(R/M)[x]$ satisfies power-substitution. Since R/M is a field of positive characteristic, its prime field is finite, hence by Corollary 3.5 it suffices to show that R/M is algebraic over its prime field. Thus consider any nonzero $\bar{a} \in R/M$. Then $aR = eR$ for some idempotent $e \in R - M$, and we note that $1 - e \in M$. Observing that $a + 1 - e$ is a unit in R, we see from (b) that $(a + 1 - e)^n = 1$ for some $n > 0$. Since $1 - e \in M$, it follows that $\bar{a}^n = 1$ in R/M, whence $\bar{a}$ is algebraic over the prime field of R/M. Thus the claim is proved.

Now let $at + b = 1$ in $R[x]$. For any $M \in \mathrm{Spec}(R)$, we have $\bar{a}\bar{t} + \bar{b} = 1$ in $(R/M)[x]$, hence there exist $n > 0$ and $\bar{u}, \bar{v} \in (R/M)[x]$ such that $(\bar{a}^n + \bar{b}\bar{u})\bar{v} = 1$, i.e., $(a^n + bu)v - 1 \in M[x]$.

Let X be the family of all clopen sets $W \subseteq \mathrm{Spec}(R)$ for which there exist $n > 0$ and $u, v \in R[x]$ such that $(a^n + bu)v - 1 \in M[x]$ for all $M \in W$. We have just seen above that given any $M \in \mathrm{Spec}(R)$, there exist $n > 0$ and $u, v \in R[x]$ such that $(a^n + bu)v - 1 \in M[x]$. Since there are only a finite number of coefficients from M needed to express $(a^n + bu)v - 1$, there must exist an idempotent $e \in M$ such that $(a^n + bu)v - 1 \in eR[x]$. As a result,

$$W = \{M' \in \mathrm{Spec}(R) \mid e \in M'\} = \{M' \in \mathrm{Spec}(R) \mid 1 - e \notin M'\}$$

is a member of X which contains M. Thus X covers $\mathrm{Spec}(R)$.

Inasmuch as $\mathrm{Spec}(R)$ is compact, it follows that we can cover it with pairwise disjoint clopen sets $W_1, \cdots, W_k$ from X. There exist orthogonal idempotents $e_1, \cdots, e_k \in R$ such that $e_1 + \cdots + e_k = 1$ and each $W_i = \{M \in \mathrm{Spec}(R) \mid e_i \notin M\}$.

For each $i = 1, \cdots, k$, there exist $n(i) > 0$ and $u_i, v_i \in R[x]$ such that $(a^{n(i)} + bu_i)v_i - 1 \in M[x]$ for all $M \in W_i$. Set $n = n(1)n(2)\cdots n(k)$ and $s(i) = n/n(i)$ for each i. Since

$$(a^{n(i)} + bu_i)^{s(i)} v_i^{s(i)} - 1 \in M[x]$$

for all $M \in W_i$, we see that there exist $w_i, z_i \in R[x]$ such that $(a^n + bw_i)z_i - 1 \in M[x]$ for all $M \in W_i$.

Setting $w = e_1 w_1 + \cdots + e_k w_k$ and $z = e_1 z_1 + \cdots + e_k z_k$, we observe that

$$e_i[(a^n + bw)z - 1] = e_i[(a^n + bw_i)z_i - 1] \in M[x]$$

for all $M \in W_i$, whence $(a^n + bw)z - 1 \in M[x]$ for all M in any

W_i. Since the W_i cover Spec(R), and since $J(R) = 0$, we conclude that $(a^n + bw)z - 1 = 0$, i.e., $a^n + bw$ is a unit in $R[x]$.

Therefore $R[x]$ satisfies power-substitution.

COROLLARY 3.8. *Let F be a field. Then the polynomial ring $F[x]$ satisfies power-substitution if and only if F is an algebraic extension of a finite field.*

DEFINITION. If R is a ring whose additive group is torsion-free of finite rank, then we refer to R as a *torsion-free finite rank* **Z**-*algebra.* In this section, we prove that any commutative, torsion-free, finite rank **Z**-algebra satisfies power-substitution. Although the commutativity hypothesis will be removed in the following section, we present the commutative case here because its proof is far simpler than the noncommutative case. We require the following lemma, which is also needed in the noncommutative case.

For use in the following proofs, we recall a few standard items from noncommutative ring theory. A ring R is *prime* if the product of any two nonzero two-sided ideals of R is nonzero; R is *semiprime* if it has no nonzero nilpotent two-sided ideals. A module A is *finite-dimensional* (in the sense of Goldie) provided A contains no infinite direct sums of nonzero submodules. A *right Goldie ring* is a ring R such that the right module R_R is finite-dimensional and such that R satisfies the ACC on right annihilator ideals. We refer the reader to [**3**, Chapter 3] for the basic theory of finite-dimensional modules and Goldie rings.

LEMMA 3.9. *Let R be a semiprime, torsion-free, finite rank* **Z**-*algebra. Then R is right and left noetherian. For any right ideal K of R, the following conditions are equivalent:*

(a) *K is an essential right ideal of R.*
(b) *K contains a non-zero-divisor of R.*
(c) *$kR \subseteq K$ for some positive integer k.*
(d) *R/K is finite.*

Proof. Since R is torsion-free of finite rank, it contains no infinite direct sums of nonzero subgroups. Consequently, R_R must be finite-dimensional. Since R is torsion-free, we see that the right annihilator of any subset of R is a pure subgroup of R. Using finite rank once again, we see that R has ACC on pure subgroups, whence R also has ACC on right annihilators. Thus R is a semiprime right Goldie ring.

Given any right ideal K of R, we now obtain (a) $\Leftrightarrow$ (b) as a standard property of semiprime Goldie rings [**3**, Theorem 3.34]. The implications (d) $\Rightarrow$ (c) $\Rightarrow$ (b) are clear. Given (b), we see that R is isomorphic to a

subgroup of K. Inasmuch as R is a torsion-free abelian group of finite rank, [5, Theorem 2.4] implies that R/K is finite. Therefore (a)–(d) are equivalent.

Given any essential right ideal K of R, we now know that $kR \subseteq K$ for some positive integer k, and that R/kR is finite. As a result, K must be finitely generated as a right ideal of R. Inasmuch as every right ideal of R is a direct summand of an essential right ideal [3, Proposition 1.3], it follows that R is right noetherian. By symmetry, R is left noetherian as well.

THEOREM 3.10. *If R is a commutative, torsion-free, finite rank $\mathbf{Z}$-algebra, then R satisfies power-substitution.*

Proof. Since R is torsion-free, it embeds in the algebra $R \otimes \mathbf{Q}$. Now $R \otimes \mathbf{Q}$ is a commutative finite-dimensional $\mathbf{Q}$-algebra, hence $J(R \otimes \mathbf{Q})$ is nilpotent and $(R \otimes \mathbf{Q})/J(R \otimes \mathbf{Q})$ has no nilpotent elements. As a result, we see that R has a nilpotent ideal N such that R/N is a torsion-free $\mathbf{Z}$-algebra with no nilpotent elements. According to Proposition 2.5, it suffices to show that R/N satisfies power-substitution. Thus we may assume, without loss of generality, that R is a semiprime, commutative, torsion-free, finite rank $\mathbf{Z}$-algebra.

Suppose that $ax + b = 1$ in R. Choose an ideal K of R such that $bR \oplus K$ is essential in R [3, Proposition 1.3], and note that $bK = 0$. Note also that $\overline{ax} = 1$ in $R/(bR \oplus K)$. According to Lemma 3.9, the ring $R/(bR \oplus K)$ is finite, whence its group of units is torsion. Thus $\bar{a}^n = 1$ for some $n > 0$, and consequently $a^n + by + c = 1$ for some $y \in R$, $c \in K$.

Since $ax + b = 1$, $a^n x^n + bz = (ax + b)^n = 1$ for a suitable $z \in R$, from which we obtain $(a^n + by)x^n + b(z - yx^n) = 1$. Multiplying this equation by the equation $(a^n + by) + c = 1$, and noting that $bc = 0$, we conclude that $(a^n + by)w = 1$ for some $w \in R$, so that $a^n + by$ is a unit.

Therefore R satisfies power-substitution.

COROLLARY 3.11. *If R is any commutative, torsion-free, algebraic $\mathbf{Z}$-algebra, then R satisfies power-substitution.*

Proof. Since R is a directed union of finitely generated subrings, it suffices to show that every finitely generated subring of R satisfies power-substitution. Thus we may assume, without loss of generality, that R is finitely generated, say $R = \mathbf{Z}[r_1, \cdots, r_n]$.

Since the r_i are algebraic over $\mathbf{Z}$, there exists a positive integer k such that $kr_1, \cdots, kr_n$ are integral over $\mathbf{Z}$. As a result, $S = \mathbf{Z}[kr_1, \cdots, kr_n]$ is a finitely generated integral $\mathbf{Z}$-algebra, and thus is finitely generated as a $\mathbf{Z}$-module. Note that R/S is a torsion group. Since R is torsion-free, it

follows that R is a torsion-free finite rank $\mathbf{Z}$-algebra. By Theorem 3.10, R satisfies power-substitution.

COROLLARY 3.12. *If F is any algebraic field extension of $\mathbf{Q}$, then every subring of F satisfies power-substitution.*

COROLLARY 3.13. *If R is any commutative ring which is integral over $\mathbf{Z}$, then R satisfies power-substitution.*

Proof. As in Corollary 3.11, we need only consider the case when R is finitely generated (as a ring). Since R is integral over $\mathbf{Z}$, we thus have that R is a finitely generated $\mathbf{Z}$-module. In addition, Proposition 2.5 says that we need only show that $R/J(R)$ has power-substitution. Thus we may also assume that $J(R) = 0$, so that R is semiprime.

We claim that every finite ideal I of R is a direct summand of R. If I is a minimal ideal, this follows from the semiprimeness of R [7, Corollary, p. 63]. If $I \neq 0$, then I must contain a minimal ideal K, and $R = K \oplus K'$ for some K'. Now $I = K \oplus (I \cap K')$, and by induction, $I \cap K'$ is a direct summand of R. As a result, $I \cap K'$ is a direct summand of K', hence we obtain $K' = (I \cap K') \oplus K''$ for some K'', and consequently $R = I \oplus K''$.

Now let T denote the torsion subgroup of R, which is a finite ideal of R and thus is a direct summand of R. Since R is commutative, this gives us a ring decomposition $R = S \times T$, where S is a finitely generated free $\mathbf{Z}$-module. By Theorem 3.10, S satisfies power-substitution. Since T is artinian, it has 1 in the stable range [12, Lemma 11.8] and consequently satisfies power-substitution. Therefore R satisfies power-substitution.

4. Finite rank Z-algebras. Of the numerous definitions of "finite rank abelian group" in the literature, the following is best suited for our purposes, since it is clearly preserved by subgroups and homomorphic images.

DEFINITION. An abelian group A is said to have *finite rank* [6, p. 49] provided there exists a positive integer n such that every finitely generated subgroup of A can be generated by n elements. Note that if A has finite rank, then $A/T(A)$ has finite rank and each of the primary components of $T(A)$ has *DCC* on subgroups.

We refer to a ring R whose additive group has finite rank as a *finite rank $\mathbf{Z}$-algebra.* The purpose of this section is to prove that every finite rank $\mathbf{Z}$-algebra satisfies power-substitution. Most of the difficulties occur in the torsion-free case, and the proof for this case involves a number of steps, covering matrix rings over noncommutative domains, orders over Dedekind domains, prime rings, and semiprime rings.

LEMMA 4.1. *Let R be a semiprime, torsion-free, finite rank* $\mathbf{Z}$*-algebra. Let $a, x, b \in R$ such that $ax + b = 1$. If b is either zero or a non-zero-divisor, then there exist a positive integer n and a matrix $Q \in M_n(R)$ such that $aI + bQ$ is a unit in $M_n(R)$.*

Proof. If $b = 0$, then $ax = 1$. In view of Lemma 3.9, R is a semiprime right noetherian ring, whence R is a subring of a semisimple artinian ring. (This follows from Goldie's Theorem: [**3**, Theorem 3.35].) In this case $ax = 1$ implies $xa = 1$, so that $a^1 + b0$ is a unit in R.

Now assume that b is a non-zero-divisor.

According to Lemma 3.9, there is a positive integer k such that $kR \subseteq bR$, and R/kR is finite. Now R/kR is an artinian ring and so has 1 in the stable range [**12**, Lemma 11.8]. Inasmuch as $\overline{ax} + \bar{b} = 1$ in R/kR, we thus obtain $y \in R$ such that $\bar{a} + \overline{by}$ is a unit in R/kR. Since the group of units of R/kR is finite, it follows that $(\bar{a} + \overline{by})^n = 1$ for some $n > 0$. Since $kR \subseteq bR$, we thus obtain $(a + by)^n + bz = 1$ for some $z \in R$.

Set $c = a + by$ and $d = bz$, so that $c^n + d = 1$. Let S denote the subring of R generated by c and d, which is commutaitve. Now

$$1 = c^n + d(c^n + d)^{n-1} = c^n + c_1 c^{n-1} d + c_2 c^{n-2} d^2 + \cdots + c_n d^n$$

for suitable $c_1, \cdots, c_n \in S$. As in Proposition 3.2, it follows that there exists $P \in M_n(S)$ such that $cI + dP$ is a unit in $M_n(S)$. As a result, we now have a matrix $Q = yI + zP$ in $M_n(R)$ such that $aI + bQ = cI + dP$ is a unit in $M_n(R)$.

LEMMA 4.2. *Let R be a torsion-free finite rank* $\mathbf{Z}$*-algebra, and assume that R is a domain* (not necessarily commutative). *Given any right R-module decomposition $M = A_1 \oplus B_1 = A_2 \oplus B_2$ such that $R \oplus A_1 \cong R^2$ and $A_2 \cong R$, there exist a positive integer n and a submodule $C \leqq M^n$ such that $M^n = C \oplus B_1^n = C \oplus B_2^n$.*

Proof. Since every element of R is either zero or a non-zero-divisor, we see from Lemma 4.1 that R satisfies right power-substitution. Applying Corollary 2.2 to the relation $R \oplus A_1 \cong R^2$, we thus find that $A_1^s \cong R^s$ for some $s > 0$.

We now proceed in a manner close to the proof of Theorem 2.1. In order to keep the notation in line with that proof, we write E for $\mathrm{End}_R(R_R)$.

Using the decomposition $M = A_1 \oplus B_1$, we obtain projections $p_1 \colon M \to A_1$, $p_2 \colon M \to B_1$ and injections $q_1 \colon A_1 \to M$, $q_2 \colon B_1 \to M$. Using the decomposition $M = A_2 \oplus B_2 \cong R \oplus B_2$, we obtain a projection $f \colon M \to R$ and an injection $g \colon R \to M$.

Now $1_R = f(q_1p_1 + q_2p_2)g = (fq_1)(p_1g) + (fq_2p_2g)$. Setting $a = fq_1 \in \mathrm{Hom}_R(A_1, R)$, $x = p_1g \in \mathrm{Hom}_R(R, A_1)$, and $b = fq_2p_2g \in E$, we have $ax + b = 1$ in E. Applying the sth power functor, we obtain $a^* \in \mathrm{Hom}_R(A_1^s, R^s)$, $x^* \in \mathrm{Hom}_R(R^s, A_1^s)$, and $b^* \in \mathrm{End}_R(R^s) = M_s(E)$ such that $a^*x^* + b^* = 1$ in $M_s(E)$. Inasmuch as $E \cong R$ is a domain, b is either zero or a non-zero-divisor in E, from which we see that b^* is either zero or a non-zero-divisor in $M_s(E)$.

Choose an isomorphism $\phi\colon R^s \to A_1^s$. This gives us elements $a^*\phi$, $\phi^{-1}x^*$, b^* in $M_s(E)$ such that $(a^*\phi)(\phi^{-1}x^*) + b^* = 1$. Now $M_s(E)$ is a prime, torsion-free, finite rank $\mathbf{Z}$-algebra, hence Lemma 4.1 says that there exist $n > 0$ and $Q \in M_n(M_s(E)) = M_{ns}(E)$ such that $a^*\phi I + b^*Q$ is a unit in $M_{ns}(E)$. Thus we now have a map $h = Q(\phi^{-1}I)$ in $\mathrm{Hom}_R(A_1^{ns}, R^{ns})$ such that $a^* + b^*h$ is an isomorphism of A_1^{ns} onto R^{ns}. Taking $C = \ker(q_1^* + q_2^*p_2^*g^*h)$, we conclude as in Theorem 2.1 that $M^{ns} = C \oplus B_1^{ns} = C \oplus B_2^{ns}$.

PROPOSITION 4.3. *Let R be a torsion-free finite rank $\mathbf{Z}$-algebra. If R is Morita-equivalent to a domain S* (not necessarily commutative), *then R satisfies right power-substitution.*

Proof. Since S is isomorphic to the endomorphism ring of a finitely generated projective R-module, we see that S is torsion-free and finite rank over $\mathbf{Z}$.

On the other hand, there exist a positive integer n and an idempotent $e \in M_n(S)$ such that $R \cong eM_n(S)e$. By Proposition 2.6, it suffices to show that $M_n(S)$ has right power-substitution, or equivalently, that the module $(S_S)^n$ has the power-substitution property. For $n = 1$, this follows from Lemma 4.1, hence we need only consider the case $n \geqq 2$.

Now let $M = A_1 \oplus B_1 = A_2 \oplus B_2$ be any right S-module decomposition such that each $A_i \cong S^n$. Write each $A_i = A_{i1} \oplus \cdots \oplus A_{in}$ with all $A_{ij} \cong S$. According to [**14**, Theorem 9] (with the help of Lemma 3.9), S has 2 in the stable range. As a result, Lemma 2.7 shows that there exist $C, D, H \leqq M$ such that

$$\begin{aligned} M &= C \oplus D \oplus H \oplus B_1 = C \oplus D \oplus A_{21} \oplus B_2 \\ &= H \oplus (C \oplus D \oplus B_1) = A_{21} \oplus (C \oplus D \oplus B_2) \end{aligned}$$

and $D \cong S$, $D \oplus H \cong S^2$. Thus $S \oplus H \cong S^2$ and $A_{21} \cong S$, whence Lemma 4.2 says that there exist $k > 0$ and $F \leqq M^k$ such that

$$\begin{aligned} M^k &= F \oplus (C \oplus D \oplus B_1)^k = F \oplus (C \oplus D \oplus B_2)^k \\ &= (F \oplus C^k \oplus D^k) \oplus B_1^k = (F \oplus C^k \oplus D^k) \oplus B_2^k. \end{aligned}$$

Therefore S^n has the power-substitution property, as required.

LEMMA 4.4. *Let T be a ring satisfying right power-substitution, let K be a two-sided ideal of T, and let R be a subring of T which contains K. If R/K has 1 in the stable range* (in particular, if R/K is right artinian), *then R satisfies right power-substitution.*

Proof. Let $ax + b = 1$ in R. Since R/K has 1 in the stable range, there exists $z \in R$ such that $\bar{a} + \bar{b}\bar{z}$ is a unit in R/K. Now $(a + bz)x + b(1 - zx) = 1$, and it suffices to find $n > 0$ and $Q \in M_n(R)$ such that $(a + bz)I + b(1 - zx)Q$ is a unit. Thus we may assume, without loss of generality, that $\bar{a}$ is a unit in R/K.

Now $aw + k = 1$ for some $w \in R$, $k \in K$, and we note that $bk \in K$. Observing that $k = axk + bk$, we obtain $a(w + xk) + bk = 1$. Since it suffices to make $aI + bkQ$ a unit in some $M_n(R)$, we may now assume also that $b \in K$.

Since $ax + b = 1$, ax must commute with b, and consequently $1 = (ax + b)^2 = ax' + b^2$ for some $x' \in R$. Inasmuch as T satisfies right power-substitution, there exist $n > 0$ and $P \in M_n(T)$ such that $aI + b^2P$ is a unit in $M_n(T)$. Note that $Q = bP$ lies in $M_n(R)$, because $bT \subseteq K \subseteq R$. We now have $A = aI + bQ$ in $M_n(R)$ which has an inverse B in $M_n(T)$. As a result, $\bar{B}$ is an inverse for $\bar{A}$ in $M_n(T/K)$. Since $\bar{a}$ is a unit in R/K, $\bar{A} = \bar{a}I$ also has an inverse in $M_n(R/K)$, from which we conclude that $\bar{B} \in M_n(R/K)$. Therefore $B \in M_n(R)$, whence $aI + bQ$ is a unit in $M_n(R)$, as desired.

DEFINITION. A *separable algebra* over a field F is a finite-dimensional semisimple algebra R such that the center of each simple component of R is a separable field extension of F. (In particular, every finite-dimensional semisimple algebra over a field of characteristic zero is separable.) Equivalently, a finite-dimensional algebra R over a field F is separable if and only if R is projective as a module over the algebra $R \otimes_F R^{op}$ [**9**, Theorem 7.20].

DEFINITION. Let S be a Dedekind domain with quotient field F, and let Q be a (finite-dimensional) separable F-algebra. An *S-order in Q* is any S-subalgebra R of Q such that $FR = Q$ and R is finitely generated as an S-module. A *maximal S-order* is one which is maximal with respect to inclusion among the S-orders in Q. Every S-order is contained in a maximal S-order [**9**, Corollary 10.4].

PROPOSITION 4.5. *Let S be a Dedekind domain which is a torsion-free finite rank $\mathbf{Z}$-algebra, let Q be a finite-dimensional simple algebra over the quotient field of S, and let R be an S-order in Q. Then R satisfies right power-substitution.*

Proof. Note that the quotient field F of S has characteristic zero, so that Q is a separable algebra over F. Also, F is finite-dimensional over $\mathbf{Q}$, hence so is Q. As a result, we see that every S-order in Q is a prime, torsion-free, finite rank $\mathbf{Z}$-algebra.

We know that R must be contained in a maximal S-order T in Q. The maximality of T implies that T is Morita-equivalent to a domain, as follows from [**10**, Chapter IV, Theorem 5.5]. By Proposition 4.3, T has right power-substitution.

Choose generators $t_1, \cdots, t_n$ for T as an S-module. There exist elements $r_1, \cdots, r_n \in R$ and $s \in S$ such that each $t_i = r_i/s$, from which we see that $sT \subseteq R$. Note that sT is a two-sided ideal of T, and also an essential right ideal of R. According to Lemma 3.9, R/sT is finite, hence artinian. By Lemma 4.4, we conclude that R satisfies right power-substitution.

DEFINITION. Let R be a subring of a ring Q. Then R is called a *right order in* Q provided every non-zero-divisor of R is invertible in Q and every element of Q can be expressed in the form ab^{-1} for suitable $a, b \in R$, b a non-zero-divisor. Any S-order as defined above is also a right order in this sense.

LEMMA 4.6. *Let Q be a finite-dimensional simple $\mathbf{Q}$-algebra, and let R be a right order in Q. Then there exists a noetherian domain S, contained in the centers of R and Q, such that R is a finitely generated S-module.*

Proof. Note that R is a prime, torsion-free, finite rank $\mathbf{Z}$-algebra. Given any $x \in Q$, we have $x = ab^{-1}$ for some $a \in R$ and some non-zero-divisor $b \in R$. According to Lemma 3.9, $kR \subseteq bR$ for some positive integer k, whence $kx \in R$. As a result, we find that $\mathbf{Q}R = Q$. According to [**8**, Theorem, p. 242], there exist a field F contained in the center of Q, a basis $q_1, \cdots, q_k$ for Q over F, and a nonzero integer m such that

$$mR \subseteq (R \cap F)q_1 + \cdots + (R \cap F)q_k.$$

Set $S = R \cap F$, which is a domain contained in the centers of R and Q. Since S is a torsion-free finite rank $\mathbf{Z}$-algebra, Lemma 3.9 shows that S is noetherian. As a result, we see that mR is a finitely generated S-module, hence so is R.

LEMMA 4.7. *Let F be a finite-dimensional field extension of $\mathbf{Q}$, let S be a domain with quotient field F, and let T be the integral closure of S in F. Then T is a Dedekind domain, and T is a finitely generated S-module.*

Proof. If V is the integral closure of $\mathbf{Z}$ in F, then V is a Dedekind domain with quotient field F, hence any ring between V and F is also a Dedekind domain. In particular, $V \subseteq T \subseteq F$, whence T is a Dedekind domain.

Now V is finitely generated as a $\mathbf{Z}$-module, and so SV is finitely generated as an S-module. Inasmuch as SV contains V, it is a Dedekind domain with quotient field F, and so is integrally closed in F. In addition, $S \subseteq SV \subseteq T$, hence we find that $SV = T$. Therefore T is finitely generated as an S-module.

PROPOSITION 4.8. *If R is a prime, torsion-free, finite rank $\mathbf{Z}$-algebra, then R satisfies right power-substitution.*

Proof. Since R is right noetherian by Lemma 3.9, it must be a right order in a simple artinian ring Q [**3**, Corollary 3.36]. Every nonzero integer is a non-zero-divisor in R and so is invertible in Q, whence Q is a $\mathbf{Q}$-algebra. As in Lemma 4.6, we obtain $\mathbf{Q}R = Q$, from which we see that Q is a finite-dimensional $\mathbf{Q}$-algebra. Now Lemma 4.6 shows that there exists a noetherian domain S, contained in the centers of R and Q, such that R is a finitely generated S-module.

Let F denote the quotient field of S, which we may view as a subfield of the center of Q, and let T denote the integral closure of S in F. According to Lemma 4.7, T is a Dedekind domain and also a finitely generated S-module.

Note that Q is a finite-dimensional simple F-algebra, and that TR is a T-subalgebra of Q. Since R is a finitely generated S-module, TR is a finitely generated T-module. Also, $\mathbf{Q}R = Q$ implies that $FTR = Q$, whence TR is a T-order in Q. Thus, according to Proposition 4.5, TR satisfies right power-substitution.

Inasmuch as T is a finitely generated S-module, there must be a nonzero element $s \in S$ such that $sT \subseteq S$. As a result, sTR is a two-sided ideal of TR which is contained in R. Observing that sTR is an essential right ideal of R, we see from Lemma 3.9 that R/sTR is finite. Therefore R satisfies right power-substitution, by Lemma 4.4.

PROPOSITION 4.9. *If R is a semiprime, torsion-free, finite rank $\mathbf{Z}$-algebra, then R satisfies right power-substitution.*

Proof. Since R is right noetherian by Lemma 3.9, it must be a right order in a semisimple artinian ring Q [**3**, Theorem 3.35]. Write $Q = Q_1 \times \cdots \times Q_n$, with each Q_i simple. If R_i denotes the image of the projection $R \to Q \to Q_i$, then R_i is a right order in Q_i and so is a prime ring. Let $T = R_1 \times \cdots \times R_n$, so that $R \subseteq T \subseteq Q$.

As in Proposition 4.8, Q is a finite-dimensional $\mathbf{Q}$-algebra. Then T is a torsion-free finite rank $\mathbf{Z}$-algebra, and consequently Proposition 4.8 shows that T satisfies right power-substitution.

Setting $K_i = R \cap Q_i$, we check that K_i is a two-sided ideal of R_i, whence $K = K_1 \times \cdots \times K_n$ is a two-sided ideal of T. In addition, K is an essential right ideal of R, hence R/K is finite by Lemma 3.9. Thus Lemma 4.4 shows that R satisfies right power-substitution.

PROPOSITION 4.10. *If R is a torsion-free finite rank $\mathbf{Z}$-algebra, then R satisfies right power-substitution.*

Proof. Since R is torsion-free, we may identify it with its canonical image in $R \otimes \mathbf{Q}$. Now $R \otimes \mathbf{Q}$ is a finite-dimensional $\mathbf{Q}$-algebra, hence $J(R \otimes \mathbf{Q})$ is nilpotent and $(R \otimes \mathbf{Q})/J(R \otimes \mathbf{Q})$ is semisimple artinian. Consequently, we see that $N = R \cap J(R \otimes \mathbf{Q})$ is a nilpotent two-sided ideal of R, and R/N is a right order in $(R \otimes \mathbf{Q})/J(R \otimes \mathbf{Q})$. Thus R/N is a semiprime, torsion-free, finite rank $\mathbf{Z}$-algebra, whence Proposition 4.9 shows that R/N satisfies right power-substitution. According to Proposition 2.5, R must satisfy right power-substitution.

LEMMA 4.11. *Let S be a ring such that $M_n(S)$ satisfies right power-substitution for all n, let K be a two-sided ideal of S, and let R be a subring of S which contains K. If R/K satisfies right power-substitution, then so does R.*

Proof. Given $ax + b = 1$ in R, there exist $n > 0$ and $Q \in M_n(R)$ such that $\bar{a}I_n + \overline{bQ}$ is a unit in $M_n(R)/M_n(K)$. Set $S' = M_n(S)$, $K' = M_n(K)$, $R' = M_n(R)$, $a' = aI_n + bQ$, $x' = xI_n$, and $b' = b(I_n - Qx')$. Then $a'x' + b' = 1$ in R' and $\overline{a'}$ is a unit in R'/K'.

Proceeding as in Lemma 4.4, there exist $k > 0$ and $P \in M_k(R')$ such that $a'I_k + b'P$ is a unit in $M_k(R')$. As a result, we have $QI_k + (I_n - Qx')P$ in $M_{kn}(R)$ such that $aI_{kn} + b[QI_k + (I_n - Qx')P]$ is a unit in $M_{kn}(R)$.

THEOREM 4.12. *If R is any finite rank $\mathbf{Z}$-algebra, then R satisfies the right and left power-substitution properties.*

Proof. By symmetry, we need only check right power-substitution. By Proposition 2.5, it suffices to prove that $R/J(R)$ has right power-substitution. Thus we may assume, without loss of generality, that $J(R) = 0$, so that R is semiprime.

Let T denote the torsion subgroup of R, which is a two-sided ideal of R. For each prime integer p, let T_p denote the p-primary component of T, which also is a two-sided ideal of R. Since R has finite rank over $\mathbf{Z}$, T_p must have DCC on subgroups and hence also on right R-submodules.

Because R is semiprime, all minimal right ideals of R are direct sumands of R_R, from which we infer (as in Corollary 3.13) that $T_p = e_pR$ for some idempotent e_p. Using semiprimeness again, it follows that e_p is central. Note that the idempotents e_p are pairwise orthogonal, and that $T = \bigoplus e_pR$.

For any positive integer n, $M_n(\prod e_pR) \cong \prod M_n(e_pR)$ is a direct product of artinian rings. Since artinian rings have 1 in the stable range [**12**, Lemma 11.8], so does $M_n(\prod e_pR)$, whence $M_n(\prod e_pR)$ satisfies right power-substitution. In addition, $M_n(R/T)$ is a torsion-free finite rank **Z**-algebra, hence Proposition 4.10 shows that $M_n(R/T)$ satisfies right power-substitution. Setting $S = (R/T) \times (\prod e_pR)$, we thus see that $M_n(S)$ satisfies right power-substitution for all n.

Observing that $T \cap [\cap (1 - e_p)R] = 0$, we obtain an injective ring map $\phi\colon R \to S$. Note that $\phi(T) = \{0\} \times (\bigoplus e_pR)$, which is a two-sided ideal of S. Inasmuch as $\phi(R)/\phi(T) \cong R/T$ satisfies right power-substitution, so does $\phi(R) \cong R$, by Lemma 4.11.

COROLLARY 4.13. *If R is any direct limit of finite rank* **Z***-algebras, then R satisfies the right and left power-substitution properties.*

5. Applications.

THEOREM 5.1. *Let A be a torsion-free abelian group of finite rank, and let B, C be arbitrary groups* (not necessarily abelian). *If $A \times B \cong A \times C$, then $\times^n B \cong \times^n C$ for some positive integer n.*

Proof. Since the endomorphism ring of A is a torsion-free finite rank **Z**-algebra, we may apply Theorem 4.12 and Corollary 2.4.

The case $A = \mathbf{Z}$ of Theorem 5.1 was proved by Hirshon in [**4**, Theorem 1]. A restricted version of this case was also proved by Warfield in [**13**, Theorem 2.1]. In addition, the case of Theorem 5.1 where A, B, C are all torsion-free abelian of finite rank has been proved by Warfield (unpublished), using entirely different methods.

LEMMA 5.2. *Let $\mathcal{F}$ denote the class of all direct limits of finite rank* **Z***-algebras.*

(a) *$\mathcal{F}$ is closed under subrings and factor rings.*

(b) *If $R \in \mathcal{F}$ and A is a finitely generated right R-module, then* $\mathrm{End}_R(A) \in \mathcal{F}$.

(c) *If $R \in \mathcal{F}$ and $R \to S$ is a ring map such that S is finitely generated as a right R-module, then $S \in \mathcal{F}$.*

(d) *If R is a commutative ring which is either integral over* **Z** *or torsion-free and algebraic over* **Z**, *then $R \in \mathcal{F}$.*

Proof. Note that a ring R belongs to $\mathcal{F}$ if and only if every finitely generated subring of R is a finite rank $\mathbf{Z}$-algebra.

(a) is clear.

(b) Choose a finitely generated free right R-module F such that A is isomorphic to a factor module of F. Then $\mathrm{End}_R(F)$ contains a subring S such that $\mathrm{End}_R(A)$ is isomorphic to a factor ring of S. Since $\mathrm{End}_R(F)$ is isomorphic to a direct limit of full matrix rings over finitely generated subrings of R, we see that $\mathrm{End}_R(F) \in \mathcal{F}$, where $S \in \mathcal{F}$, and consequently $\mathrm{End}_R(A) \in \mathcal{F}$.

(c) According to (b), $\mathrm{End}_R(S_R) \in \mathcal{F}$, whence $S \in \mathcal{F}$.

(d) If R is integral over $\mathbf{Z}$, then every finitely generated subring of R is also finitely generated as a $\mathbf{Z}$-module. If R is torsion-free and algebraic over $\mathbf{Z}$, then (as in Corollary 3.11), every finitely generated subring of R is a torsion-free finite rank $\mathbf{Z}$-algebra.

THEOREM 5.3. *Let S be a commutative ring which is either integral over $\mathbf{Z}$ or torsion-free and algebraic over $\mathbf{Z}$, let T be an S-algebra which is finitely generated as an S-module, and let R be any subring of T. Let A be a finitely generated right R-module, and let B, C be any right R-modules. If $A \oplus B \cong A \oplus C$, then $B^n \cong C^n$ for some positive integer n.*

Proof. According to Lemma 5.2, $\mathrm{End}_R(A)$ is a direct limit of finite rank $\mathbf{Z}$-algebras. Now apply Corollaries 4.13 and 2.2.

For example, Theorem 5.3 applies when R is a subring of the group algebra $F[G]$ of a finite group G over a field F which is algebraic over $\mathbf{Q}$.

DEFINITION. A right R-module A is *nonsingular* provided $xI \neq 0$ for all nonzero $x \in A$ and all essential right ideals I of R. A *right nonsingular ring* is a ring R for which the right module R_R is nonsingular. We refer the reader to [**3**, Chapter 1] for an exposition of these concepts.

THEOREM 5.4. *Let R be a right nonsingular ring whose maximal right quotient ring Q is a direct limit of finite rank $\mathbf{Z}$-algebras. Let A be a finite-dimensional nonsingular right R-module, and let B, C be any right R-modules. If $A \oplus B \cong A \oplus C$, then $B^n \cong C^n$ for some positive integer n.*

Proof. Since A is nonsingular and finite-dimensional, its injective hull $E(A)$ is a finitely generated right Q-module [**3**, Theorem 3.16]. Also, it follows from the nonsingularity of A that $\mathrm{End}_R(A)$ is naturally isomorphic to a subring of $\mathrm{End}_Q(E(A))$. Consequently, we see from Lemma 5.2 that $\mathrm{End}_R(A)$ is a direct limit of finite rank $\mathbf{Z}$-algebras. Now apply Corollaries 4.13 and 2.2.

6. Problems. A. Is the power-substitution property (for rings) left-right symmetric?

B. Is it Morita-invariant?

C. Does Theorem 5.1 hold for finite rank abelian groups which are not necessarily torsion-free? In particular, does the endomorphism ring of such a group satisfy power-substitution? (The answer to both questions is yes in case the torsion subgroup of the group is a direct summand.)

D. Does a noncommutative algebraic **Q**-algebra satisfy power-substitution?

E. Presumably Theorem 4.12 can be generalized to finite rank algebras over some domains other than **Z**. Perhaps it would work for a Dedekind domain S such for all nonzero $b \in S$, the group of units of S/bS is torsion.

References

1. E. G. Evans, Jr., *Krull-Schmidt and cancellation over local rings*, Pacific J. Math., **46** (1973), 115–121.

2. L. Fuchs, *On a substitution property for modules*, Monatshefte für Math., **75** (1971), 198–204.

3. K. R. Goodearl, *Ring Theory: Nonsingular Rings and Modules*, New York (1976) Marcel Dekker (Pure and Applied Math. Series, Vol. 33).

4. R. Hirshon, *The cancellation of an infinite cyclic group in direct products*, Arch. der Math.,**26** (1975), 134–138.

5. B. Jónsson, *On direct decomposition of torsion-free abelian groups*, Math. Scand., **7** (1959), 361–371.

6. I. Kaplansky, *Infinite Abelian Groups* (revised edition), Ann Arbor (1969), Univ. of Michigan Press.

7. J. Lambek, *Lectures on Rings and Modules*, Waltham, Mass. (1966) Blaisdell.

8. R. S. Pierce, *Subrings of simple algebras*, Michigan Math. J., **7** (1960), 241–243.

9. I. Reiner, *Maximal Orders*, New York (1975), Academic Press.

10. K. W. Roggenkamp and V. Huber-Dyson, *Lattices over Orders I*, Springer Lecture Notes No. 115, Berlin (1970), Springer-Verlag.

11. R. G. Swan, *Vector bundles and projective modules*, Trans. Amer. Math. Soc., **105** (1962), 264–277.

12. ———, *Algebraic K-Theory*, Springer Lecture Notes No. 76, Berlin (1968), Springer-Verlag.

13. R. B. Warfield, Jr., *Genus and cancellation for groups with finite commutator subgroup*, J. Pure Applied Algebra, **6** (1975), 125–132.

14. ———, *Notes on cancellation, stable range, and related topics*, Univ. of Washington, (August 1975).

Received November 14, 1975 and in revised form January 26, 1976.

UNIVERSITY OF UTAH