PACIFIC JOURNAL OF MATHEMATICS
Vol. 124, No 1, 1986

POWER CANCELLATION OF MODULES

ROBERT M. GURALNICK

It is shown that for R an integrally closed domain then $M \oplus X \cong N \oplus X$ implies $M^{(t)} \cong N^{(t)}$ for some positive integer t for all finitely generated S-modules M, N, X whenever S is a module finite algebra if and only if one is in the stable range of the integral closure of R in the algebraic closure of its quotient field. In particular, this holds whenever R is a Dedekind domain with all residue fields torsion. This extends work of Goodearl, who showed this holds for module finite (and more generally, finite rank) algebras over the integers.

0. Introduction. If R is a ring, let $\operatorname{Mod} R$ ($\operatorname{Mod}_f R$) denote the category of unital right (finitely generated) R-modules. Let us say $X \in \operatorname{Mod}_f R$ satisfies *power cancellation* if for all $M, N \in \operatorname{Mod}_f R$, $M \oplus X \cong N \oplus X$ implies $M^{(t)} \cong N^{(t)}$ for some positive integer t. (Here $M^{(t)}$ denotes the direct sum of t copies of M.) Power cancellation can hold for various reasons. For example, if D is a Dedekind domain, any finitely generated module satisfies cancellation (that is, $t = 1$). If R is a $\mathbb{Z}$-order in a separable $\mathbb{Q}$-algebra, it follows from **[12]** that power cancellation holds for R-lattices. The author **[10, 11]** extended this to module finite algebras over Dedekind domains satisfying the Jordan-Zassenhaus Theorem (without the lattice assumption). See also **[14, 15, 16, 21]** for relevant examples as to when power cancellation does and does not hold.

The goal of this article to find necessary and sufficient conditions on an integrally closed commutative integral domain D such that for any X in $\operatorname{Mod}_f S$ with S a module finite D-algebra, X satisfies power cancellation. It turns out that the relevant property to study is *power substitution*: $X \in \operatorname{Mod} R$ satisfiesl power substitution if whenever $M \in \operatorname{Mod} R$ (not necessarily finitely generated) has a decomposition $M = A \oplus X_1 = B \oplus X_2$ with $X_1 \cong X$, then there exists a positive integer t such that $A^{(t)}$ and $B^{(t)}$ have a common complement in $M^{(t)}$. Goodearl **[8]** showed that this stronger property depends only on $E = \operatorname{End}_R X$ and is equivalent to a stable range condition on E. He used this idea to extend **[12]** and prove that any $X \in \operatorname{Mod}_f S$ satisfies power substitution for S a finite rank $\mathbb{Z}$-algebra (see §4).

Recall that one is in the stable range of a ring R if whenever $ax + b = 1$ in R, there exists $y \in R$ such that $a + by$ is a unit in R. (This definition is left-right symmetric).

If D is an integral domain, let $\overline{D}$ denote the integral closure of D in the algebraic closure of its quotient field. The main result is:

THEOREM A (*Power Cancellation*). *Let D be an integrally closed domain. The following are equivalent*:

(1) *One is in the stable range of $\overline{D}$.*

(2) *If S is a module finite D-algebra, then every $X \in \operatorname{Mod}_f S$ satisfies power cancellation.*

(3) *If S is a module finite D-algebra, then every $X \in \operatorname{Mod}_f S$ satisfies power substitution.*

It is worth noting that (2) need only be checked for S a commutative order in a semisimple algebra and for X an ideal of S.

Following Goodearl [**8**], we say a D-module M has finite rank if there is a bound on the number of generators required for all finitely generated submodules. Note this is equivalent to the usual definition for torsionfree modules (where rank n means $K \otimes_D M$ is n-dimensional over the quotient field K of D).

If D is a Dedekind domain such that the unit group of D/bD is torsion for all $b \neq 0$, then it follows (see Theorem 3.5) that D satisfies Theorem A(1). This allows us to extend [**8**, Theorem 4.12] and answer [**8**, question 6E] in the affirmative.

THEOREM B. *Let D be a Dedekind domain such that one is in the stable range of $\overline{D}$. If S is a finite rank D-algebra and $X \in \operatorname{Mod}_f S$, then X satisfies power substitution.*

Let D be a commutative ring and S a module finite D-algebra. If $M, N \in \operatorname{Mod}_f S$, we say M and N are in the same genus (and write $M \vee N$) if $M_P = M \otimes_D D_P \cong N_P$ for all maximal ideals P of R as S_P-modules. Note that by local cancellation ([**3**] or [**9**]), if $M \oplus X \cong N \oplus X$ for some $X \in \operatorname{Mod}_f S$, then $M \vee N$. We can ask when $M \vee N$ implies $M^{(t)} \cong N^{(t)}$ for some $t > 0$. The answer is similar to that in Theorem A except the stable range condition must be strengthened. A commutative ring D satisfies the *primitive criterion* if every primitive polynomial $f(x) \in D[x]$ represents a unit in D ($f = \sum a_i x^i$ is primitive if $D = \sum a_i D$). See [**4**, **17**, **20**]. Let $\operatorname{Pic} D$ denote the group of projective rank one modules (under tensor product).

THEOREM C (*Torsion Genus*). *Let D be an integrally closed domain. The following are equivalent*:

(1) $\bar{D}$ *satisfies the primitive criterion.*

(2) *One is in the stable range of* $\bar{D}$ *and* $\operatorname{Pic}\bar{D} = \{\bar{D}\}$.

(3) *If S is a module finite D-algebra and M, N are finitely presented S-modules, then $M \vee N$ implies $M^{(t)} \cong N^{(t)}$ for some $t > 0$.*

In fact, it suffices to check condition (3) for S a commutative order in a semisimple algebra and $M \vee S$. Note that any Dedekind domain satisfying the Jordan-Zassenhaus Theorem also satisfies condition (1) [**11**, Theorem 2.4]. Also one can replace the isomorphism condition in (3) by M is locally isomorphic to a summand of N. The conclusion would then be that $M^{(t)}|N^{(t)}$ for some t.

The article is organized as follows. In §2, we give an example to show power cancellation implies a stable range condition. The proofs of the main theorems and some consequences are given. Finally we consider when cancellation holds and some connections with the Jordan-Zassenhaus Theorem.

All rings have 1 and, unless stated otherwise, all modules are unital right modules.

I would like to thank D. Estes and L. Levy for several helpful discussions and the referee for his careful detailed comments.

2. An example. Let $S[x]$ denote the ring of polynomials over S, where x commutes with S. Any square matrix A over S defines an $S[x]$-module $M(A)$ by taking $M(A)$ to be the set of column vectors over S and defining $vx = Av$ for any $v \in M(A)$. Moreover, $M(A) \cong M(B)$ if and only if A and B are similar. Now fix $\alpha \in S$, and set

$$A = \begin{pmatrix} 0 & -1 \\ 0 & \alpha \end{pmatrix} \quad \text{and} \quad B = \begin{pmatrix} 0 & -\beta \\ 0 & \alpha \end{pmatrix}$$

for some $\beta \in S$. Denote $M(B) = M(\beta)$. For the rest of this section, we will assume that $ab = 1$ in S implies $ba = 1$ (in particular, this holds if S is a module finite algebra over a commutative ring). A straightforward computation now yields:

LEMMA 2.1. (a) *$M(\beta) \cong M(1) \Leftrightarrow \beta + x\alpha$ is a unit for some x in S.*
(b) *If $y\beta + \alpha = 1$, then $\left(\begin{smallmatrix} A & 0 \\ 0 & 0 \end{smallmatrix}\right)$ and $\left(\begin{smallmatrix} B & 0 \\ 0 & 0 \end{smallmatrix}\right)$ are similar.*

The desired similarity in (b) is given by

$$P = \begin{pmatrix} -\beta & 0 & 1 \\ 0 & -1 & 0 \\ \alpha & 1 & y \end{pmatrix}.$$

Note

$$P^{-1} = \begin{pmatrix} -y & 1 & 1 \\ 0 & -1 & 0 \\ 1-\beta y & \beta & \beta \end{pmatrix}.$$

If S is a module finite R-algebra, then α satisfies some monic polynomial $f(x) \in R[x]$. Thus $M(\beta)$ is in fact a $T = S[x](xf(x))$-module, and T is a module finite R-algebra. In particular, if $R = S$, then $M(\beta)$ is an $R[x]/(x^2 - \alpha x)$-module.

LEMMA 2.2. *Suppose $\beta, \gamma \in S$ and $z\gamma + \alpha = y\beta + \alpha = 1$ in S.*

(a) *$M(\beta) \oplus S \cong M(1) \oplus S$ as $S[x]$-modules (here we identify S with $S[x]/(x)$).*

(b) *If S is commutative, and $T = S[x]/(x^2 - \alpha x)$, then $M(\beta)$ is a projective rank one T-module and $M(\beta) \otimes_T M(\gamma) \cong M(\beta\gamma)$.*

Proof. (a) is just a restatement of Lemma 2.1(b). The first statement of (b) is determined locally in which case it follows from Lemma 2.1(a) and the observation that $M(1) \cong T$.

Now let e_1, e_2 and f_1, f_2 denote the standard bases for $M(\beta)$ and $M(\gamma)$, respectively. Set $g_1 = (e_1 + ye_2) \otimes f_1$ and $g_2 = e_2 \otimes f_2$. Then it can be verified locally that g_1, g_2 is an R-basis for $M(\beta) \otimes_T M(\gamma)$ and with respect to this basis x acts via the matrix $\left(\begin{smallmatrix} 0 & -\beta\gamma \\ 0 & \alpha \end{smallmatrix}\right)$. Thus (b) holds.

PROPOSITION 2.3. *Assume S is a module finite extension of a commutative ring R and $y\beta + \alpha = 1$ in S. Let $f(x)$ be a monic polynomial in $R[x]$ of minimal degree with $f(\alpha) = 0$. Set $T = S[x]/(xf(x))$.*

(a) *If S (considered as a T-module) satisfies cancellation, then $\beta + z\alpha$ is a unit in S for some z in S.*

Now assume $R = S$ (and so $f(x) = x - \alpha$).

(b) *If R (considered a T-module) satisfies power cancellation, then $\beta^t + z\alpha$ is a unit for some $t > 0$ and some z.*

(c) *If $M(\beta)^{(t)} \cong T^{(t)}$, then $\beta^t + z\alpha$ is a unit for some z.*

Proof. (a) follows Lemmas 2.1(a) and 2.2(a). If S satisfies power cancellation, then $M(\beta)^{(t)} \cong T^{(t)}$ for some $t > 0$. Now by taking exterior powers, it follows that $M(\beta^t) \cong T \cong M(1)$. Hence by Lemma 2.1, $\beta^t + z\alpha$ is a unit. Thus (b) and (c) hold.

3. Power substitution. We shall need the basic result about power substitution.

LEMMA 3.1. (*Goodearl* [8, *Theorem* 2.1].) *Let* $X \in \operatorname{Mod} S$. *The following are equivalent*:

(1) X *satisfies power substitution*.

(2) *If* $a, b \in E = \operatorname{End}_S X$ *with* $ax + b = 1$, *then there exists a positive integer* t *and a matrix* $Q \in M_t(E)$ *such that* $aI + bQ$ *is a unit in* $M_t(E)$.

Van der Kallen [20] introduced a stronger version of the stable range one condition. A commutative ring R is called U-irreducible if the set of polynomials in $R[x]$ which represents units in R is closed under multiplication.

PROPOSITION 3.2. *Let* S *be a module finite* R-*algebra*.

(1) *If* R *is* U-*irreducible, then one is in the stable range of* S.

(2) *If* R *is an integrally closed domain and* $\overline{R}$ *is* U-*irreducible, then every* $X \in \operatorname{Mod}_f S$ *satisfies power substitution*.

Proof. (1) Since S is the homomorphic image of a module finite R-subalgebra T of $M_n(R)$ and the stable range condition is preserved by homomorphic images, we can assume $S = T$. Let $a, b, c \in S$ with $ac + b = 1$. Let $f(x) = \det(ac + ax(1 - c) + b)$ and $g(x) = \det(c + x(1 - c)) \in R[x]$. Since $f(0) = 1 = g(1)$ and R is U-irreducible, there exists $r \in R$ with $f(r)g(r)$ a unit. Hence $d = c + r(1 - c)$ is a unit in T, and so $a + bd^{-1}$ is a unit in T (since d^{-1} is a polynomial in d). Thus (1) holds.

(2) Let $E = \operatorname{End}_S X$. Then E is a homomorphic image of an R-subalgebra T of $M_n(R)$. Thus it suffices to show Lemma 3.1(2) holds for T. The proof of (1) shows that if $a, b \in T$ with $ac + b = 1$, then there exists $\theta \in \overline{R}$ and $d \in T[\theta]$ such that $a + bd$ is a unit in $T[\theta]$. However $T[\theta]$ embeds in $M_t(T)$ where t is the degree of $m(x)$, the minimal polynomial of θ over R (since R is integrally closed, $m(x)$ is monic) via the map ϕ which sends $\alpha \in T$ to αI and θ to the companion matrix of $m(x)$. Hence $aI + bQ$ is a unit for $Q = \phi(d) \in M_t(T)$, as desired.

We can now prove Theorem A which is included in:

THEOREM 3.3. *Let* D *be an integrally closed domain. The following are equivalent*:

(1) *One is the stable range of* $\overline{D}$.

(1′) $\overline{D}$ *is* U-*irreducible*.

(2) *If* S *is a module finite* D-*algebra, then every* $X \in \operatorname{Mod}_f S$ *satisfies power cancellation*.

(2′) *If S is a commutative D-order in a semisimple algebra, then every ideal of S satisfies power cancellation.*

(3) *If S is a module finite D-algebra, then every $X \in \operatorname{Mod}_{\mathrm{f}} S$ satisfies power substitution.*

Proof. Clearly (3) $\Rightarrow$ (2) $\Rightarrow$ (2′). Now assume (2′) and $ax + b = 1$ with a, b, and x in $\bar{D}$. Set $S = D[a, b, x]$. It follows from Proposition 2.3 that $a^t \equiv u \bmod bS$ for some positive integer t and some unit u in S. Hence by [**4**, Theorem 3.2], $a + by$ is a unit for some y in $\bar{S} = \bar{D}$. Thus (1) holds. Now (1) $\to$ (1′) by [**4**, Theorem 4.4]. Finally, (1′) $\Rightarrow$ (3) by Proposition 3.2.

It is perhaps worth noting that the proof of Proposition 3.2 actually gives a bit more than Theorem A.

PROPOSITION 3.4. *Let D be an integrally closed domain with one in the stable range of $\bar{D}$. If S is a module finite D-algebra and $M, N \in \operatorname{Mod} S$ and $X \in \operatorname{Mod}_{\mathrm{f}} S$ with $M \oplus X \cong N \oplus X$, there exists $\theta \in \bar{D}$ such that $M \otimes_D D[\theta] \cong N \otimes_D D[\theta]$ as $S \otimes_D D[\theta]$ modules. Moreover, $M^{(t)} \cong N^{(t)}$, where t is the degree of the minimal polynomial for θ over D.*

Proof. The proof of Proposition 3.2 showed that if T is an D-subalgebra of $M_n(D)$, then $\delta\varepsilon + \beta = 1$ in T implies $\delta + \beta\lambda$ is a unit in $T[\theta]$ for some $\theta \in \bar{D}$ and $\lambda \in T[\theta]$. Note $T[\theta] = T \otimes_D D[\theta]$. So this also holds for any homomorphic image of T. In particular, we shall apply this to $E = \operatorname{End}_S(X)$.

Suppose $\sigma = \left(\begin{smallmatrix} \alpha & \beta \\ \gamma & \delta \end{smallmatrix}\right)$ is an isomorphism from $M \oplus X$ to $N \oplus X$. Then $\delta\delta' + \gamma\beta' = 1$ in E where $\sigma^{-1} = \left(\begin{smallmatrix} \alpha' & \beta' \\ \gamma' & \delta' \end{smallmatrix}\right)$. By the preceding paragraph, $u = \delta + \gamma\beta'\lambda$ is a unit in $E[\theta] = E \otimes_D D[\theta]$. Also since D is integrally closed, $D[\theta]$ has $1, \theta, \ldots, \theta^{t-1}$ as a D-basis, where t is the degree of the minimal polynomial of θ over D. It follows easily that $E[\theta] = \operatorname{End}_{S[\theta]}(X[\theta])$. Now consider $\sigma = \sigma \otimes 1$ as an isomorphism from $M[\theta] \oplus X[\theta]$ to $N[\theta] \oplus X[\theta]$. Define $\nu \in \operatorname{Aut}_{S[\theta]}(M[\theta] \oplus X[\theta])$ by

$$\nu = \begin{pmatrix} 1 & \beta'\lambda \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & 0 \\ 0 & u^{-1} \end{pmatrix} \begin{pmatrix} 1 & 0 \\ -\gamma & 1 \end{pmatrix}.$$

Then

$$\sigma\nu = \begin{pmatrix} \alpha^* & \beta^* \\ 0 & 1 \end{pmatrix}$$

is an isomorphism, and so α^* is the desired isomorphism from $M[\theta]$ to $N[\theta]$.

Some examples of domains D satisfying Theorem A are given in [**4**, Section 5]. For example, if the residue fields of a Dedekind domain D are finite, D will satisfy Theorem A. This can be extended.

THEOREM 3.5. *Let D be a Dedekind domain such that the group of units in D/dD is torsion for all $d \neq 0$. Then one is in the stable range of $\overline{D}$.*

Proof. Let $a, b \in \overline{D}$ with $ax + b = 1$. Let E be the integral closure of $D[a, x]$ in its quotient field. Then E is also a Dedekind domain [**22**, Theorem 30]. Let $(b) = P_1^{e_1} \cdots P_r^{e_r}$, where the P_i are primes of E. Since E/P_i is an algebraic extension of $D/P_i \cap D$, by the hypothesis, E/P_i is an algebraic extension of a finite field. Thus there exists a positive integer t such that $a^t \equiv 1 \bmod P_1 \cdots P_r$. Moreover, as E/P_i has nonzero characteristic there exists a positive integer $m \in P_1 \cdots P_r$. Then $a^{tm^e} \equiv 1 \bmod bE$, where $e \geq e_i$. By [**4**, Theorem 3.2] (applied to $\overline{D} = \overline{E}$), one is in the stable range of $\overline{D}$.

4. Finite rank algebras. In this section, we extend Theorem A for D a Dedekind domain to finite rank D-algebras. A D-module M has finite rank if there is a positive integer t such that every finitely generated submodule can be generated by t elements. This extends [**8**, Theorem 4.12] and answers [**8**, Question 6E] affirmatively. Our proof follows that in [**8**] for $D = \mathbb{Z}$ except in the case of a prime torsionfree algebra; in this case, even for $\mathbb{Z}$, the proof given here is shorter. The main idea of the proof is to reduce to the case of a module finite algebra over a larger Dedekind domain. We need two preliminary results.

LEMMA 4.1. *Let D be a Dedekind domain with quotient field K. If E is a subring of K containing D, then E is also Dedekind. Moreover, if $\overline{D}$ is U-irreducible, so is $\overline{E}$.*

Proof. The first assertion is well known. (It follows easily from [**22**, Theorem 28]). Suppose $ax + b = 1$ for a, $0 \neq b \in \overline{E}$. Let C be the integral closure of D in $K[a, x]$. Then C is also a Dedekind domain. Then $C \subset V = C[a, x] \subset K[a, x]$. We claim $V = C + bV$; this can be checked locally. So let P be a prime ideal of C. If $V_P = C_P$, it is certainly true. If $V_P \neq C_P$, then V_P is a field and so $V_P = bV_P$. Hence $a \equiv c \bmod bV$ and $x \equiv y \bmod bV$ for some $c, y \in C$. Now $cy + z = 1$ for some $z \in bV \cap C$. Since $\overline{D} = \overline{C}$ is U-irreducible, $c \equiv u \bmod z\overline{C}$ for some unit u in $\overline{C}$. Thus $a \equiv c \equiv u \bmod b\overline{E}$. Hence one is in the stable range of $\overline{E}$, and so $\overline{E}$ is U-irreducible by [**4**, Theorem 4.4].

LEMMA 4.2. *Let D be a Dedekind domain with quotient field K. Suppose S is a finitely generated prime D-subalgebra of a finite-dimensional K-algebra A. Then*

(1) *$Z = Z(S)$ is a finitely generated D-algebra.*

(2) *S is a module finite Z-algebra.*

(3) *There exists a finitely generated D-subalgebra C of Z such that Z is module finite over C, and the quotient field L of C is a finite-dimensional separable extension of K.*

Proof. We can assume $A = S \otimes_D K$. Since S is prime, A is simple. Let Z' be the integral closure of Z in its quotient field $F = Z(A)$. Now Z' contains D' the integral closure of D in the finite-dimensional extension F of K. Hence D' and Z' are both Dedekind. By [**6**, Theorem 1], SZ' is a finitely generated Z'-module. Hence $SZ' = \sum Z'a_i$ for some $a_1, \dots, a_t \in S$. Now $SZ'' = \sum Z''a_t$ for Z'' a finitely generated Z-subalgebra of Z''. Thus SZ'' is a finitely generated Z''-module and hence is a finitely generated Z-module. Since S is a finitely generated Z-subalgebra of SZ'', S is also a finitely generated Z-module (cf [**4**, Lemma 2.1]).

Now (1) follows by the Artin-Tate Lemma (cf. [**11**]). Let $C = \{x \in Z | z$ is separable over $K\}$. Then $Z^q \subset C$ for some power q of the characteristic K. Since Z is finitely generated over D, Z is module finite over C. Moreover, C is a finitely generated D-algebra by another application of the Artin-Tate Lemma.

We can prove Theorem B in the prime torsionfree case.

THEOREM 4.3. *Let D be a Dedekind domain such that one is in the stable range of $\overline{D}$. If S is a prime torsionfree finite rank D-algebra, then S (considered as an S-module) satisfies power substitution.*

Proof. By the hypotheses, S embeds in $A = S \otimes_D K$, a finite-dimensional simple K-algebra (K is the quotient field of D). Let C be as in Lemma 4.2. Let $V = CE$, where E is the integral closure of D in L, the quotient field of C. Since L is separable over K, V is a finitely generated C-module. Moreover, as $E \subset V \subset L$, V is a Dedekind domain and by Lemma 4.1, $\overline{V}$ is U-irreducible. Thus SV satisfies power substitution by Theorem A. Since V is finitely generated as a C-module, $bV \subset C$ for some $0 \neq b \in C$. Thus $bSV \subset S \subset SV$. Since SV/bSV is artinian, it now follows by [**8**, Lemma 4.4] that S satisfies power substitution.

We can now prove Theorem B. Let notation be as in the theorem. Set $E = \operatorname{End}_S X$. Since E is also a finite rank D-algebra (see the proof of [**8**, Lemma 5.2]), it suffices to take $S = E = X$. (Recall from 3.1 that power substitution depends only on the endomorphism ring.) As in the proof of [**8**, Theorem 4.12], one reduces to the semiprime torsionfree case. Then $S \otimes_D K = A$ is a semisimple K-algebra. So $A = \oplus Ae_i$, where the e_i are primitive central idempotents. Let $T = \oplus Se_i$ and $J = \oplus (S \cap Ae_i)$. Then $T \supset S \supset J$ and T/J is artinian. Since each Se_i is a prime torsionfree finite rank D-algebra, T satisfies power substitution by the previous result. Hence by [**8**, Lemma 4.4], S does also.

5. The genus. In order to prove Theorem C, we need to characterize the primitive criterion (for $\overline{D}$). If $f(x) \in D[x]$, define the content of f, $C(f)$, as the ideal generated by the coefficients of f (note this differs from the usual definition when D is a UFD). Recall f is primitive in $D[x]$ if $C(f) = D$.

LEMMA 5.1. *Let D be an integrally closed integral domain. If $f(x) \in D[x]$ is primitive, then there exists $0 \neq s \in D$ such that $sf = g_1 \cdots g_r$, where each $g_i \in D[x]$ is irreducible over the quotient field and $(s) = C(g_1) \cdots C(g_r)$. In particular, $C(g_i)$ is an invertible ideal of D.*

Proof. Certainly there exists $0 \neq s$ in D with $sf = g_1 \cdots g_r$ where each $g_i \in D[X]$ is irreducible over the quotient field. We need only prove that $(s) = C(g_1) \cdots C(g_r)$. Since $C(f) = D$, $s \in C(g_1) \cdots C(g_r)$. Conversely, let $d \in C(g_1) \cdots C(g_r)$. Since D is integrally closed, it is the intersection of valuation rings D_v (cf. [**22**], vol. II, p. 15); thus it suffices to show $s|d$ in D_v for each valuation v. This is obvious as now each $C(g_i)$ is a principal ideal.

LEMMA 5.2. *Let D be an integral domain. Then $\overline{D}$ satisfies the primitive criterion if and only if one is in the stable range of $\overline{D}$ and* $\operatorname{Pic} \overline{D}$ *is trivial.*

Proof. If $\overline{D}$ satisfies the primitive criterion, then clearly one is in the stable range. Moreover, $\operatorname{Pic} \overline{D}$ is trivial by [**4**, 2.6 and 3.5].

Conversely, if $\operatorname{Pic} \overline{D}$ is trivial, then in the factorization of Lemma 5.1 each $C(g_i)$ is principal. Thus it follows that any primitive polynomial $f(x)$ is of the form $\pi(a_i x - b_i)$ where $\overline{D} = a_i \overline{D} + b_i \overline{D}$. Since one is in the stable range, $\overline{D}$ is U-irreducible by [**4**, Theorem 4.4] and so f represents a unit.

The next result shows that $\operatorname{Pic} \overline{D}$ is trivial whenever it is torsion.

PROPOSITION 5.3. *Let D be an integrally closed integral domain with quotient field K. Let G be the group of invertible fractional ideals of D, and let H be the subgroup of principal ideals.*

(a) *G is a torsionfree group.*

(b) *If K has no nontrivial separable algebraic extensions (e.g. if K is algebraically closed), then H is divisible, and so $G \cong H \oplus \operatorname{Pic} D$. In particular, $\operatorname{Pic} D$ is torsionfree.*

Proof. (a) The identity of G is D. Suppose $I \in G$ and $I^t = D$. We claim $I = D$. It suffices to prove this locally. If D is local, then $I = aD$ for some $a \in K$ and so a^t is a unit in D. Since D is integrally closed, it follows that a is a unit in D as desired.

(b) Let $I = aD$ be an element of H. Let p be a prime. We need to show $I = J^p$ for some $bD = J$ in H. If p is different from the characteristic of K, then K contains b with $b^p = a$. Now assume p is the characteristic of K. By multiplying a by an appropriate c^p, we can assume a is in D. Consider $f(x) = x^p - ax + 1$ in $D[x]$. Since f is separable, f has a solution u in D. Moreover, since $u(u^{p-1} - a) = -1$, u is a unit in D. Thus $aD = auD = (u^p + 1)D = (u + 1)^pD$, as desired.

THEOREM 5.4. *Let D be an integrally closed integral domain. The following are equivalent:*

(1) *$\overline{D}$ satisfies the primitive criterion.*

(2) *One is in the stable range of $\overline{D}$ and $\operatorname{Pic} \overline{D}$ is trivial.*

(3) *If S is a module finite D-algebra and M and N are finitely presented S-modules with $M \vee N$, then $M^{(t)} \cong N^{(t)}$ for some $t > 0$.*

(4) *If S is a module finite D-algebra and M and N are finitely presented S-modules with $M \vee N$, then $M \otimes_D D[\theta] \cong N \otimes_D D[\theta]$ as $S \otimes_D D[\theta]$-modules for some $\theta \in \overline{D}$.*

Proof. (1) and (2) are equivalent by Lemma 5.2. Since D is integrally closed, $\theta \in \overline{D}$ implies $D[\theta]$ is a free rank t D-module, where t is the degree of the minimal polynomial of θ over D. Hence (4) implies (3).

Note (3) implies one is in the stable range by Proposition 2.3 and [**4**, Theorem 3.2]. Moreover, if $I = \sum a_i\overline{D}$ is an invertible ideal of $\overline{D}$ then $J = I \cap E = \sum a_i E$ is an invertible ideal of some module finite extension E of D. Hence (3) implies $J^{(t)} \cong E^{(t)}$, whence J^t is a principal ideal of E. Hence I^t is principal in $\overline{D}$. Since $\operatorname{Pic} \overline{D}$ is torsionfree by Proposition 5.3, this implies I is principal. Thus (3) implies (2).

Finally, let us show (1) implies (4). So assume M and N are finitely presented S-modules with $M \vee N$. Let V be the localization of $D[x]$ at the set of primitive polynomials. Then V satisfies the primitive criterion [**20**]. Since $M \otimes_D V$ and $N \otimes_D V$ are in the same genus (as $S \otimes_D V$-modules where $S \otimes_D V$ is considered as a module finite V-algebra), it follows by [**4**, 2.6 and 3.5] that they are in fact isomorphic. Set $M[x] = M \otimes_D D[x]$. Since M and N are finitely presented S-modules, $M[x]$ and $N[x]$ are finitely presented $S[x]$-modules. Since V is a localization of $D[x]$, this implies there exists $\alpha \in \operatorname{Hom}_{D[x]}(M[x], N[x])$ and $\beta \in \operatorname{Hom}_{D[x]}(N[x], M[x])$ such that $\alpha\beta$ and $\beta\alpha$ are multiplication by a primitive polynomial $f(x)$. Choose $\theta \in \overline{D}$ such that $f(\theta)$ is a unit. Then $M \otimes_D D[\theta] \cong N \otimes_D D[\theta]$ as desired.

Examples of D satisfying Theorem C include $D = \mathbb{Z}$, $k[x]$, k an algebraic extension of a finite field, or any Dedekind domain satisfying the Jordan-Zassenhaus theorem (see [**11**]). Other examples include D local and integrally closed or $D = R[x]$ localized at the set of primitive polynomials for R integrally closed. There are examples of Dedekind domains which satisfy the conclusions of Theorems A and B but not those of Theorem C (see [**4**]). In fact, such examples exist with all residue fields finite (see [**7**]).

6. The Jordan-Zassenhaus theorem.

Let D be a Dedekind domain with quotient field K. One says D satisfies the Jordan-Zassenhaus theorem if for every D-order S in a finite-dimensional semisimple K-algebra, there are only a finite number of isomorphism classes of S lattices of bounded D-rank. The problem can be split into two parts:

(1) Determine when the number of distinct genera of S-lattices of bounded rank is finite.

(2) Determine when every genus is finite.

Problem (1) is quite easy to solve.

LEMMA 6.1. *The number of genera of S-lattices of bounded rank is finite for all orders S in a semisimple K-algebra A if and only if all residue fields of D are finite and each S is contained in a maximal order.*

Proof. If D/P is infinite, then consider $S = D + M_2(PD)$. Let M be the natural module for $M_2(D)$. Then there are infinitely many S-sublattices N with $PM \subset N \subset M$, and no two are locally isomorphic.

If S is not contained in a maximal order, then there is an infinite chain of orders $S = S_0 \subset S_1 \subset S_2 \ldots$ in A. Clearly, S_i and S_j are not locally isomorphic for $i \neq j$.

For the converse, see the proofs of the Jordan-Zassenhaus theorem for Z and $k[x]$, k a finite field in [**2**, **18**, **19**].

Of course, if A is a separable K-algebra, then the second condition is guaranteed. There are examples of local principal ideal domains, $U \subset V$, such that $v \in V$ implies $v^2 \in U$ but V is not module finite over U [**13**, Theorem 100]. Thus any U-order S with the same quotient field as V is not contained in a maximal order (recall orders are module finite). Moreover, this can be arranged so that the residue field of U contains 2 elements. Since U is local, the genus of any U-lattice is trivial. Thus U will satisfy a weak version of the Jordan-Zassenhaus theorem; it will hold for all U-orders in a separable K-algebra.

Problem (2) seems a bit harder. If D is semilocal (or more generally an LG-ring, see [**4**]), then in fact the genus will always be trivial. Unlike (1), in Problem (2), one need not be restricted to D-orders and lattices. In fact by [**11**, Proposition 3.5], the condition

(2$'$) The genus of S is finite for every D-order S in a semisimple K-algebra is equivalent to

(2$''$) The genus of M is finite for every $M \in \mathrm{Mod}_{\mathrm{f}} S$ for all module finite S-algebras.

Moreover, if we also assume the conditions of Lemma 6.1, it suffices to determine (cf. [**18**] or [**19**]) whether

(2$'''$) The genus of S is finite for S a maximal order in a division algebra.

We close this section with two questions. Can (2$'''$) be weakened by considering only maximal orders in fields? If the residue fields of D are finite and $\bar{D}$ is Bezout, is every genus finite? (Note if every genus is finite, then $\bar{D}$ is Bezout by Theorem C.)

7. Cancellation. One can ask when cancellation (rather than power cancellation) holds for all module finite D-algebras. There is an answer, albeit not totally satisfactory.

PROPOSITION 7.1. *Let R be a commutative ring. Then every $X \in \mathrm{Mod}_{\mathrm{f}} S$ for every module finite algebra S satisfies cancellation if and only if one is in the stable range of each S.*

Proof. The forward implication follows from Proposition 2.3(a). Set $E = \mathrm{End}_S(X)$. Then E is a direct limit of module finite R-algebras [**4**, Lemma 2.1]. Thus the reverse implication follows by [**3**]. Indeed, the fact that one is in the stable range of E actually implies that X satisfies substitution.

COROLLARY 7.2. *The conditions of Proposition* 7.1 *hold if* R *is* U-*irreducible*.

Proof. Apply Proposition 3.2.

Note that if R is U-irreducible all residue fields of R for are infinite (since $\pi(x - a_j$ must represent a unit in R for any $a_i \in R$, see [**20**]). Since any finite field satisfies the conditions of Proposition 7.1, U-irreducibility is not necessary. We close by posing the problem of characterizing those commutative rings satisfying the criterion in Proposition 7.1.

REFERENCES

[1] E. Artin and J. Tate, *A note on finite ring extensions*, J. Math. Soc. Japan, **3** (1951), 74–77.

[2] C. W. Curtis and I. Reiner, *Methods of Representation Theory*, Vol. I, Wiley-Interscience (New York), 1981.

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

[4] D. R. Estes and R. M. Guralnick, *Module equivalences: local to global when primitive polynomials represent units*, J. Algebra, **77** (1982), 138–157.

[5] D. R. Estes and J. Ohm, *Stable range in commutative rings*, J. Algebra, **7** (1967), 343–362.

[6] E. Formanek, *Noetherian PI-rings*, Comm. in Algebra, **1** (1974), 79–86.

[7] O. Goldman, *On a special class of Dedekind domains*, Topology, **3** (1964), 113–118.

[8] K. R. Goodearl, *Power cancellation of groups and modules*, Pacific J. Math., **64** (1976), 387–411.

[9] K. R. Goodearl and R. B. Warfield, Jr., *Algebras over zero dimensional rings*, Math. Ann., **223** (1976), 157–168.

[10] R. M. Guralnick, *Isomorphism of modules under ground ring extension*, J. Number Theory, **14** (1982), 307–314.

[11] _____, *The genus of a module*, J. Number Theory, **18** (1984), 169–177.

[12] H. Jacobinski, *Uber Geschlechter von Ordnungen*, J. Reine Angew. Math., **230** (1968), 29–39.

[13] I. Kaplansky, *Commutative Rings*, University of Chicago, Chicago, 1974.

[14] L. S. Levy, *Krull-Schmidt uniqueness fails dramatically over subrings of* $Z \oplus Z \oplus \cdots \oplus Z$, Rocky Mountain J. Math., **13** (1983), 659–678.

[15] _____, *Modules over Dedekind-like rings*, J. Algebra, **93** (1985), 1–116.

[16] L. S. Levy and R. Wiegand, *Dedekind-like behavior of rings with* 2-*generated ideals*, J. Pure and Appl. Algebra, **37** (1985), 41–58.

[17] B. R. McDonald and W. C. Waterhouse, *Projective modules over rings with many units*, Proc. Amer. Math. Soc., **83** (1981), 455–458.

[18] I. Reiner, *Maximal Orders*, Academic Press, New York, 1975.
[19] R. G. Swan, *Algebraic K-Theory*, Lect. Notes in Math. **76**, Springer-Verlag, Berlin, 1968.
[20] W. Van der Kallen, *The K_2 of rings with many units*, Ann. Sci. Ecole Norm. Sup., **4** (1977), 473–515.
[21] R. Wiegand, *Cancellation over commutative rings of dimension one and two*, J. Algebra, **88** (1984), 438–459.
[22] O. Zariski and P. Samuel, *Commutative Algebra*, I, II, Springer-Verlag, New York, 1958.

Received May 30, 1984 and in revised form February 10, 1985. Supported in part by an NSF grant.

UNIVERSITY OF SOUTHERN CALIFORNIA
LOS ANGELES, CA 90089-1113