TRANSACTIONS OF THE
AMERICAN MATHEMATICAL SOCIETY
Volume 224, Number 2, 1976

UNIQUE FACTORIZATION IN MODULES AND SYMMETRIC ALGEBRAS

BY

DOUGLAS L. COSTA

ABSTRACT. Necessary and sufficient conditions are given for a torsion-free module M over a UFD D to admit a smallest factorial module containing it. This factorial hull is $\bigcap M_P$, the intersection taken over all height one primes of D. In case M is finitely generated, the hull is M^{**}, the bidual of M.

It is shown that if the symmetric algebra $S_D(M)$ admits a hull, then the hull is the smallest graded UFD containing $S_D(M)$. $S_D(M)$ is a UFD if and only if it is a factorial D-module. If M is finitely generated over D, but not necessarily torsion-free, then $\oplus_{i\geq 0}(S^i(M))^{**}$ is a graded UFD.

Examples are given to show that any finite number of symmetric powers of M may be factorial without $S_D(M)$ being factorial.

Introduction. Anne-Marie Nicolas defined and discussed factorial modules over unique factorization domains in [6], and in [7] extended this concept to that of factorable modules over arbitrary integral domains. A factorable module M over an integral domain D is a torsion-free module with the property that each nonzero element of M may be written uniquely (up to units) as the product of an element of D and an element of M which is divisible only by units of D. A factorial module is a factorable module over a unique factorization domain. These have the property that elements of the module have unique factorizations.

Not every torsion-free module over a UFD may be embedded in a factorial module. We shall see, however, that if a torsion-free module M is a submodule of a factorial module, then there is a unique smallest factorial module $\hat{M}$ containing M. In fact $\hat{M} = \bigcap M_P$, where P ranges over the principal prime ideals of D. We shall also relate the existence of $\hat{M}$ to some other conditions on M and in the process arrive at an internal construction for $\hat{M}$.

Factorable modules were studied under the name "type 0 modules" in [2]. It was shown there that for M torsion-free over a UFD D, the symmetric algebra $S_D(M)$ is a UFD if and only if it is a factorial D-module. Here we shall

---

Presented to the Society, November 7, 1975; received by the editors September 12, 1975.

AMS (MOS) subject classifications (1970). Primary 13C10, 13F15; Secondary 15A78.

Key words and phrases. Factorial module, symmetric algebra.

prove that if the module $\widehat{S_D(M)}$ exists, then it is a graded UFD, and in fact the smallest one containing $S_D(M)$ as a graded D-subalgebra.

Since the factoriality of $S_D(M)$ is equivalent to the factoriality of the symmetric powers $S_D^i(M)$ as D-modules, one might hope for some bound on the number of symmetric powers which must be checked. We shall conclude with a family of examples to dispel that hope.

Before proceeding we list here some other characterizations of factorial modules which we shall use freely in the sequel. For D a UFD and M a torsion-free D-module the following are equivalent:

(1) M is factorial.

(2) Each nonzero element $x \in M$ has a greatest divisor $d \in D$, in the sense that any other divisor of x must be a factor of d. (We shall use g.d.(x) to denote the greatest divisor of x.)

(3) Every maximal rank one submodule of M is cyclic [6, Theorem 8.1], [7, Theorem 3.7].

(4) M satisfies the ascending chain condition on cyclic submodules (a.c.c.c.), and every D-sequence of two elements is an M-sequence [6, Theorem 1.7, Proposition 4.1, Proposition 4.5].

If M is factorial, elements of M which are divisible only by units of D are called primitive. Each nonzero element $x \in M$ has the unique representation $x = \text{g.d.}(x)x^*$, where x^* is primitive.

1. Let D be a UFD with quotient field K. Let M be a torsion-free D-module and set $KM = K \otimes_D M$.

1.1. DEFINITION. A D-module $\hat{M}$ is a factorial hull of M if $M \subseteq \hat{M}$, $\hat{M}$ is factorial, and $M \subseteq \hat{M} \subseteq N$ whenever $M \subseteq N$ with N factorial.

If a factorial hull exists, it is unique and so may be referred to as the factorial hull. Not every torsion-free module has a factorial hull. The quotient field K, for example, is a maximal rank one submodule of any module in which it sits, but is cyclic only if $D = K$.

1.2. PROPOSITION. *If $\{M_i \mid i \in I\}$ is a family of factorial submodules of a torsion-free D-module M, then $\bigcap M_i$ is factorial.*

PROOF. $\bigcap M_i$ is torsion-free. Let $x \in \bigcap M_i$. For each $i \in I$ write $x = d_i x_i^*$, with $d_i \in D$ and x_i^* primitive in M_i. Let $d = \text{g.c.d.}\{d_i \mid i \in I\}$. Then $x = dc_i x_i^*$ for each $i \in I$, and since M is torsion-free, $c_i x_i^* = c_j x_j^*$ for $i, j \in I$. Thus $x/d \in \bigcap M_i$. If $x/c \in \bigcap M_i$, $c \in D$, then $c \mid d_i$ for every $i \in I$ and hence $c \mid d$. This shows that d is a greatest divisor for x.

1.3. THEOREM. *If M is a submodule of a factorial module N, then there is a smallest factorial submodule $\hat{M}$ of N containing M. $\hat{M}$ is a factorial hull of M. Furthermore, $\hat{M} \subseteq KM$.*

PROOF. The proposition shows that the intersection of the family of factorial submodules of N containing M is factorial, proving the first assertion. Now suppose $M \subseteq L$ with L a factorial D-module. (Note that we may take $L = N$.) Construct the push-out

$$\begin{array}{ccc} KM & \subseteq & KN \\ \cap\mid & & \downarrow f_1 \\ KL & \xrightarrow[f_2]{} & W \end{array}$$

where W is the vector space $KL \oplus KN/\{(x,-x)|x \in KM\}$, $f_1(y) = \overline{(0,y)}$, and $f_2(z) = \overline{(z,0)}$. Then f_1, f_2 are injective and the diagram commutes. So we may consider M, L, N, KM, KL, KN to be submodules of W, with all containment relations holding there. Since W is torsion-free, $L \cap N$ is a factorial submodule of N, whence $\hat{M} \subseteq L \cap N \subseteq L$. Now also $\hat{M} \subseteq L \cap N \subseteq KL \cap KN = KM$ by construction.

1.4. COROLLARY. *Every finitely generated torsion-free module over a UFD has a factorial hull.*

PROOF. Every such module is contained in a free module, and these are all factorial [6, Theorem 3.2].

From now on $\hat{M}$ will denote the factorial hull of M.

1.5. PROPOSITION. *If $\hat{M}$ exists, then $\hat{M} = \bigcap\{M_P | P$ is a height one prime of $D\}$.*

PROOF. First note that for any torsion-free module N over the UFD D, $N = \bigcap\{N_P \mid \mathrm{ht}(P) = 1\}$ if and only if every D-sequence of length 2 is an N-sequence. $\bigcap M_P$ clearly has this property and, since it is factorial, $\hat{M}$ does too. Now $M_P \subseteq (\hat{M})_P$ for every height one prime P, so $\bigcap M_P \subseteq \hat{M}$. Since $\hat{M}$ is factorial, $\bigcap M_P$ inherits from it the a.c.c.c. It follows that $\bigcap M_P$ is factorial and therefore that $\hat{M} = \bigcap M_P$.

1.6. COROLLARY. *If M is finitely generated, then $\hat{M} = M^{**}$, the bidual of M.*

PROOF. This follows from $\bigcap M_P = M^{**}$ [1].

It is by now clear that M has a factorial hull if and only if M is a submodule of a factorial module if and only if $\bigcap M_P$ is factorial. We wish to characterize those torsion-free modules which admit a factorial hull, i.e., those for which $\bigcap M_P$ is factorial. In order to do so it is convenient to introduce the

following notion. Suppose that $\{D_i | i \in I\}$ is a family of integral domains with the same quotient field K, and that, for each $i \in I$, M_i is a factorable D_i-submodule of some vector space V over K. We shall say that the intersection $\bigcap M_i$ is locally finite if each nonzero $x \in \bigcap M_i$ is primitive in all but a finite number of the M_i's.

1.7. PROPOSITION. *Let M be a torsion-free module over a UFD D. $\bigcap \{M_P | \mathrm{ht}(P) = 1\}$ is factorial if and only if each M_P is a factorial D_P-module and the intersection is locally finite.*

PROOF. We may assume that $M = \bigcap M_P$. If M is factorial, then, for each prime ideal P, M_P is factorial as a D_P-module and for each nonzero element $x \in M$, $\mathrm{g.d.}_{D_P}(x) = \mathrm{g.d.}(x)$ [2, Proposition 2.20]. ($\mathrm{g.d.}_{D_P}(x)$ is the greatest divisor in D_P of the element $x \in M_P$.) Thus $\mathrm{g.d.}_{D_P}(x)$ is a unit in D_P for all but a finite number of height one primes P. It follows that $\bigcap M_P$ is locally finite.

Conversely, if $M = \bigcap M_P$ is a locally finite intersection of factorial modules, for any nonzero $x \in M$ and any prime $p \in D$ we may write $\mathrm{g.d.}_{D_{(p)}}(x) = p^{n_p}$ with $n_p \geqslant 0$. Then $n_p = 0$ for all but a finite number of nonassociate primes p. Let $d = \Pi p^{n_p}$. Since $x/d \in M_P$ for each height one prime P, $x/d \in M$. If also $x/c \in M$, then $x/c \in M_{(p)}$ for each prime $p \in D$ and so $c \mid p^{n_p}$ in $D_{(p)}$. Therefore $c \mid d$, so that d is a greatest divisor for x. This shows that M is factorial.

We may extract from the preceding proposition an internal characterization of those modules which have factorial hulls.

1.8. LEMMA. *Let M be a torsion-free module over a UFD D. M has a factorial hull if and only if for each nonzero $x \in M$ there is a nonzero element $d \in D$ such that for any $a \in D$ the divisors of ax must divide ad.*

PROOF. Suppose that $\hat{M}$ exists and let $x \in M$ be nonzero. Then x has a greatest divisor $d \in D$, as an element of $\hat{M}$. If c is a divisor of ax in M, then it is a divisor of ax in $\hat{M}$ and so $c \mid \mathrm{g.d.}(ax) = ad$.

Conversely, let $x \in M$ be nonzero and let $d \in D$ be the element guaranteed by the hypothesis. Let $p \in D$ be a prime. If for some positive integer n, p^n divides x in $M_{(p)}$, then p^n divides tx in M for some $t \in D \backslash (p)$. This forces $p^n \mid td$ and therefore $p^n \mid d$. It follows that n is bounded and that $M_{(p)}$ is a factorial $D_{(p)}$-module. It also follows that x is primitive in $M_{(p)}$ for all but a finite number of (p). By the proposition, $\hat{M}$ exists.

We conclude this section with two simple examples.

(1) Let D be a UFD which is not a PID, and let M be any ideal of D of height at least two. Then M is not a principal ideal and is therefore not a

factorial module. $\bigcap M_P = D$ is factorial, however, so that $\hat{M} = D$.

(2) Let D be any UFD and M the submodule of its quotient field consisting of all fractions with square-free denominators. For each prime $p \in D$, $M_{(p)} = (1/p)D_{(p)}$ is factorial, and $\bigcap M_P = M$. The intersection is not locally finite, however, since $1 \in M$ is divisible by every prime.

2. **The finite divisor property.** We shall say that a torsion-free module over a UFD has the finite divisor property (f.d.p.) if each nonzero element of the module has, up to units, only a finite number of proper divisors. Equivalently, a module has the f.d.p. if and only if each nonzero element is divisible by only a finite number of primes and only by a finite power of each. (One should perhaps define a notion of type as in [4, §85], and call modules with the f.d.p. "homogeneous of type $(\ldots, 0, 0, \ldots)$".)

Consider the following conditions on a torsion-free module M over a UFD D:

(a) M is factorial.

(b) M has a factorial hull.

(c) M has the f.d.p.

(d) M satisfies the a.c.c.c.

In this section we hope to shed some light on the relations between these conditions. Some conclusions are immediate. First, it is clear that (a) implies (b) implies (c) implies (d). Second, if M is flat, every D-sequence of length two is an M-sequence; hence (a), (b), (c) and (d) are equivalent for flat modules. In particular, all are equivalent over a PID. Third, we have already seen an example in §1 to show that (a) and (b) are not equivalent in general.

For any torsion-free module M over a UFD D, we may construct an enlargement of M in the following manner. For every prime $p \in D$ and every $x \in M$ let $o_p(x) = \sup\{n \mid x \in p^n M\}$. We allow $o_p(x) = \infty$. Note that $o_p(x + y) \geqslant \inf\{o_p(x), o_p(y)\}$; and for $d \in D$, $o_p(dx) \geqslant v_p(d) + o_p(x)$ (v_p is the p-adic valuation on D). Set $\widetilde{M} = \{x/d \in KM \mid x \in M, d \in D, d \neq 0$ and $v_p(d) \leqslant o_p(x)$ for every prime $p \in D\}$. Then $M \subseteq \widetilde{M} \subseteq KM$ and $\widetilde{M}$ is a D-module. If M has the finite divisor property, then $\widetilde{M}$ consists of all fractions x/d, where d is a divisor of the least common multiple of the (finite) set of divisors of x.

2.1. LEMMA. *Let M be torsion-free over the UFD D. Then $\widetilde{M} = \bigcap\{M_P \mid \operatorname{ht} P = 1\}$.*

PROOF. Let $x \in M$ and $d \in D$ be such that $v_p(d) \leqslant o_p(x)$ for every prime $p \in D$. Then for any prime p, $p^{v_p(d)}$ is a divisor of x. It follows that $x/d \in M_{(p)}$. This shows that $\widetilde{M} \subseteq \bigcap M_P$.

Next let $z \in \bigcap M_P$ and write $z = x/d$ with $x \in M$ and $d \in D$. Let

$p_1, \ldots, p_n$ be those primes which divide d. For $1 \leqslant i \leqslant n$ we may write $x/d = x_i/d_i$, where $p_i \nmid d_i$. Let $c = d_1 \cdots d_n$ and $c_i = d_1 \cdots \hat{d}_i \cdots d_n$. Then $cx = dc_i x_i$, for each i, and so $o_{p_i}(cx) = o_{p_i}(dc_i x_i) \geqslant v_{p_i}(dc_i) + o_{p_i}(x) \geqslant v_{p_i}(dc_i) = v_{p_i}(cd)$. If p is a prime which does not divide d, then $o_p(cx) \geqslant v_p(c) = v_p(cd)$. Hence $x/d = cx/cd \in \widetilde{M}$.

From the lemma it is clear that $\widetilde{\widetilde{M}} = \widetilde{M}$. The lemma, together with the results of §1, also yields the following corollary.

2.2. COROLLARY. *Let M be a torsion-free module over a UFD. The following are equivalent.*

(1) *M has a factorial hull.*

(2) *$\widetilde{M}$ is factorial.*

(3) *$\widetilde{M}$ has the f.d.p.*

(4) *$\widetilde{M}$ satisfies the a.c.c.c.*

Moreover, if any of these conditions hold, then $\widetilde{M} = \hat{M}$.

We can now give an example to show that (c) does not imply (b).

2.3. EXAMPLE. *A module with the f.d.p. which has no factorial hull.* Let D be a noetherian UFD which is not a PID. Let p, q be primes of D such that $Dp + Dq \neq D$. Then $D[q/p]$ consists of the elements in the quotient field of D of the form $\Sigma_{i=0}^{n} a_i p^{n-i} q^i / p^n$. Note that each such element is either in D or may be written in the above form with $n > 0$ and $p \nmid a_n$.

Consider the D-module $D[q/p]$. For $m \geqslant 0$, q^m is divisible by both q^m and p^m. Hence $1/p^m = q^m/p^m q^m \in D[q/p]$, for $m > 0$. This shows that $D[q/p]$ has no factorial hull.

Next we want to see that $D[q/p]$ has the f.d.p. To check this it is sufficient to check that each nonzero element in D (considered as an element of the module $D[q/p]$) has a finite number of divisors, since for $x \in D[q/p]$ and a suitably chosen N, $p^N x \in D$. Therefore, let $d \in D$, $d \neq 0$, and let r be a prime of D distinct from p. If $d/r^m \in D[q/p]$, then either $d/r^m \in D$ or $d/r^m = a/p^n$ with $n > 0$ and $p \nmid a$. In the latter case $r^m a = p^n d$ implies $r^m \mid d$. Hence the only prime power divisors of the module element d are the prime powers occurring in the factorization of d and, possibly, powers of p. We will be done as soon as we see that d is not divisible by arbitrarily large powers of p. This follows from the ensuing lemma.

LEMMA. *Let D be a UFD and p, q primes of D. A nonzero element $d \in D$ is divisible by arbitrarily large powers of p in $D[q/p]$ if and only if $d \in \bigcap_{n>0}(p, q)^n D$.*

PROOF. Let $d \in D$ and suppose $p \nmid d$. If $d/p^N \in D[q/p]$, then we may

write $d/p^N = \Sigma_{i=0}^{n} a_i p^{n-i} q^i / p^n$ with $n > 0$ and $p \nmid a_n$. Then from $p^n d = p^N \Sigma_{i=0}^{n} a_i p^{n-i} q^i$ we deduce that $n = N$ and $d \in (p, q)^N D$. This is enough to prove the necessity.

Conversely, if $d \in (p, q)^N D$, then $d = \Sigma_{i=0}^{N} a_i p^{n-i} q^i$ and hence $d/p^N \in D[q/p]$.

We conclude this section with an example to show that (d) does not imply (c).

2.4. EXAMPLE. *A module satisfying the a.c.c.c. which does not have the f.d.p.* Let D be a two-dimensional local UFD and $\underline{m}$ its maximal ideal. Then $\bigcap_{k>0} \underline{m}^k = 0$ and $\underline{m}$ contains an infinite number of distinct primes of D. Furthermore, we may choose D, $\underline{m}$ so that $\underline{m}$ contains a sequence $\{p_i\}_{i=1}^{\infty}$ of distinct primes, each having the property that if $x \in \underline{m}^k \backslash \underline{m}^{k+1}$, then $p_i x \in \underline{m}^{k+1} \backslash \underline{m}^{k+2}$. (A polynomial ring in two variables over an infinite field localized at the origin will suffice.)

Let M be the D-module generated by the fractions $1/p_i$, $i \geqslant 1$. Since $1 \in M$ is divisible by every p_i, M does not have the f.d.p. If $Dx_1 \subseteq Dx_2 \subseteq \cdots$ is an ascending chain of cyclic submodules of M, then $x_1 = c_1 x_2 = c_1 c_2 x_3 = \cdots$, where each c_i is a nonunit of D. Let $x_1 = \Sigma_{i=1}^{n} d_i/p_i = d/p_1 \cdots p_n$. Since we may assume that $x_1 \neq 0$, there is a positive integer k such that $d \in \underline{m}^k \backslash \underline{m}^{k+1}$. Now $x_1/c_1 \cdots c_{k+1} = x_{k+2} \in M$ and we may write $x_{k+2} = \Sigma_{i=1}^{N} a_i/p_i = a/p_1 \cdots p_N$, where $a \in \underline{m}^{N-1}$. Then $dp_1 \cdots p_N = ac_1 \cdots c_{k+1} p_1 \cdots p_n$ yields the contradiction that the left-hand side is in $\underline{m}^{k+N} \backslash \underline{m}^{k+N+1}$, while the right-hand side is in $\underline{m}^{k+N+n} \subseteq \underline{m}^{k+N+1}$. This shows that M satisfies the a.c.c.c.

3. **Applications to symmetric algebras.** We first need some lemmas.

3.1. LEMMA. *Let D be a UFD and $M = \bigoplus_{i \in I} M_i$ a torsion-free D-module. $\hat{M}$ exists if and only if $\hat{M}_i$ exists for each $i \in I$, in which case $\hat{M} = \bigoplus_{i \in I} \hat{M}_i$.*

PROOF. This follows easily from the fact that a direct sum is factorial if and only if each summand is factorial [6, Theorem 3.2].

3.2. LEMMA. *Let $D = \bigoplus_{n>0} D_n$ be a graded domain. Then D satisfies the ascending chain condition on principal ideals (a.c.c.p.) if and only if D satisfies the a.c.c.c. as a D_0-module.*

PROOF. Routine.

If $D_0 \subseteq D$ are integral domains we say that D_0 is inert in D if, for $a, b \in D$, $a \neq 0 \neq b$, $ab \in D_0$ implies that $a, b \in D_0$. Observe that if D is a graded

domain with D_0 its elements of degree zero, then D_0 is inert in D.

3.3. LEMMA. *Let $D_0 \subseteq D$ be integral domains with D_0 inert in D. If D is a UFD, then D_0 is a UFD and D is a factorial D_0-module.*

PROOF. It is well known that if D is a UFD, then so is D_0 and every prime of D_0 is a prime of D. For $x \in D, x \neq 0$, write $x = p_1 \cdots p_s \cdot q_1 \cdots q_t$, where the p_i's are primes of D_0 and the q_j's are primes of D not in D_0. Then $p_1 \cdots p_s$ is a greatest divisor for x.

We are now ready for the main result of this section.

3.4. THEOREM. *Let D be a UFD and M a D-module such that the symmetric algebra $S_D(M)$ is torsion-free over D. If $\widehat{S_D(M)}$ exists, then it is a graded UFD.*

PROOF. First observe as in [8] that $S_D(M)$ is a subring of the polynomial ring $S_k(KM)$, where K is the quotient field of D, and hence that $S_D(M)$ is a domain. As $\widehat{S_D(M)} = \bigcap_{\text{ht } P=1}(S_D(M))_{D\setminus P} = \bigcap_{\text{ht } P=1} S_{D_P}(M_P)$, it is a graded domain. Furthermore $\widehat{S_D(M)}_{D\setminus 0} = S_K(KM)$ is a UFD. Since $\widehat{S_D(M)}$ is a factorial D-module, it satisties the a.c.c.p. by Lemma 3.2. Using Nagata's theorem, it now suffices to show that the multiplicative system $D\setminus 0$ is generated by primes i.e., that each prime of D is prime in $\widehat{S_D(M)} = T$. Let $p \in D$ be prime and let $P = pD$. Let $x, y, z \in T$ and suppose that $xy = pz$. This relation remains true in $T_P = S_{D_P}(M_P)$. Note that if N is a finitely generated D_P-submodule of M_P, it is free and hence, by [5, Corollary 3.12], $S_{D_P}(N) \subseteq T_P$. Choose such an N so that $x, y, z \in S_{D_P}(N)$. Since $S_{D_P}(N)$ is a polynomial ring over D_P and p is a prime, $p \mid x$ or $p \mid y$ there and hence in T_P. Say $p \mid x$ in T_P. Then there is a $d \in D\setminus P$ and a $t \in T$ such that $dx = pt$. Since T is a factorial D-module, we must have $p \mid x$ in T. Thus p is prime in T.

Note that if D' is a graded UFD over D which contains $S_D(M)$ as a graded D-subalgebra, then since D' is a factorial D-module (Lemma 3.3) we have $\widehat{S_D(M)} \subseteq D'$. Thus $\widehat{S_D(M)}$ is the smallest graded UFD containing $S_D(M)$ as graded D-subalgebra. A UFD containing D which is also a factorial D-module is called a factorial extension of D in [7]. $\widehat{S_D(M)}$ is clearly the smallest factorial extension of D containing $S_D(M)$.

Let us now derive some corollaries to the theorem.

3.5. COROLLARY [2, THEOREM 2.16]. *Let R be a ring and M an R-module. $S_R(M)$ is a UFD if and only if R is a UFD and $S_R(M)$ is a factorial R-module.*

PROOF. Necessity follows from Lemma 3.3. Sufficiency follows from the theorem.

3.6. COROLLARY. *Let D be a UFD and M a flat D-module. Then $S_D(M)$ is a UFD if and only if $S_D(M)$ satisfies the a.c.c.p.*

PROOF. As M is flat, so is $S_D(M)$ [5, Proposition 2.3]. It now follows from 3.5 and the discussion in §2 that $S_D(M)$ is a UFD if and only if it satisfies the a.c.c.c. as a D-module. Applying Lemma 3.2 finishes the proof.

3.7. COROLLARY. *Let M be a finitely generated module over a UFD D. Then $\bigoplus_{i>0}(S_D^i(M))^{**}$ is a graded UFD.*

PROOF. For any D-module N let $t(N)$ be its torsion submodule. It is easy to check that $\mathrm{Hom}(N, D) \cong \mathrm{Hom}(N/t(N), D)$ and hence that $N^{**} \cong (N/t(N))^{**}$. Thus

$$\bigoplus_{i>0} (S^i(M))^{**} \cong \bigoplus_{i>0} (S^i(M)/t(S^i(M)))^{**} = \overbrace{\bigoplus_{i>0} (S^i(M)/t(S^i(M)))},$$

using the fact that M is finitely generated, Corollary 1.6, and Lemma 3.1. Let $T = \bigoplus_{i>0}(S^i(M)/t(S^i(M))) = S(M)/t(S(M))$. Since T is the canonical image of $S(M)$ in $S(M) \otimes K = S_K(M \otimes K)$, it is a graded domain. (K = quotient field of D.) We wish to see that $\hat{T}$ is a graded UFD.

Toward this end, observe that there is a commutative diagram of graded D-algebras,

$$\begin{array}{ccc} S(M) & \xrightarrow{\alpha} & S(M/t(M)) \\ & \searrow & \downarrow \\ & & T \end{array}$$

in which α is surjective. Applying the functor $F(\cdot) = (\cdot)/t(\cdot)$ to this diagram yields

$$\begin{array}{ccc} T & \xrightarrow{F(\alpha)} & F(S(M/t(M))) \\ & \searrow^{1_T} & \downarrow \\ & & T \end{array}$$

where $F(\alpha)$ is an isomorphism. It follows that the image of $S(M/t(M))$ in $S_K(M \otimes K)$ is T. Thus we may assume that M is torsion-free.

Now for each height one prime P of D, M_P is free and hence $S(M)_P \subseteq S_K(KM)$. Then $T \subseteq S(M)_P$ and since T is the image of $S(M)$ in $S(M)_P$, we have $T_P = S(M)_P$. Thus $\hat{T} = \bigcap_{\mathrm{ht}\, P=1} S(M)_P$ is a graded domain over D. Now $\hat{T} \otimes K = S_K(KM)$, $\hat{T}_P = S_{D_P}(M_P)$ for each height one prime of D, and $\hat{T}$ is a

factorial D-module. Proceeding as in the proof of Theorem 3.4 proves that $\hat{T}$ is a UFD.

Note that if in Corollary 3.7 we had initially assumed $S_D(M)$ to be torsion-free, we would have had $\bigoplus(S_D^i(M))^{**} = \widehat{S_D(M)}$, and 3.7 would have been an immediate consequence of Theorem 3.4. Since in this setting $S_D(M)$ is an integral domain, one wonders whether $\widehat{S_D(M)}$ coincides with the integral closure of $S_D(M)$. That it does not can be seen as follows. Let D_0 be any UFD and let X, Y, Z, U, V be indeterminates over D_0. Set $D = D_0[X, Y]$ and let M be the ideal generated by X and Y. Since $M \cong D \oplus D/\langle(Y, -X)\rangle$, $S_D(M) \cong D[U, V]/(YU - XV)$ which is a Krull domain by [3, Proposition 14.5]. Since M is of rank one but not cyclic, it is not factorial, so neither is $S_D(M)$. In fact $\widehat{S_D(M)} = \bigcap_{\text{ht } P=1} S_{D_P}(M_P) = \bigcap_{\text{ht } P=1} S_{D_P}(D_P) = S_D(D) \cong D[Z]$. (Cf. the discussion at the end of [8].)

3.8. PROPOSITION. *Let D be a UFD and M a finitely generated D-module. $S_D(M)$ is a UFD if and only if*

(i) *$S_D(M)$ is an integral domain, and*

(ii) *$S_{D/pD}(M/pM)$ is an integral domain for each prime p of D.*

PROOF. If $S_D(M)$ is a UFD (i) clearly holds; and since D is inert in $S_D(M)$, $S_{D/pD}(M/pM) = S_D(M)/pS_D(M)$ is a domain for each prime p of D.

Conversely, if (i) and (ii) hold, then $S_D(M)$ is a domain and every prime of D is prime in $S_D(M)$. Also, since $\widehat{S_D(M)}$ exists, $S_D(M)$ satisfies the a.c.c.c. as a D-module, and hence the a.c.c.p. as a ring. By Nagata's theorem $S_D(M)$ is a UFD.

Proposition 3.8 has the effect, for finitely generated modules, of reducing the problem of the factoriality of symmetric algebras to the problem of their integrity. The problem of integrity is a difficult one. Samuel [8] made the observation that $S_D(M)$ is a domain if and only if it is torsion-free, but there is no necessary and sufficient condition on M for $S_D(M)$ to be a domain. Any such condition would have to logically fall strictly between the properties of flatness and torsion-freeness, as examples show.

Proposition 3.8 can be reformulated in the following way.

3.8′. PROPOSITION. *Let D be a UFD; $X_1, \ldots, X_n$ indeterminates over D; and I an ideal of $D[X_1, \ldots, X_n]$ generated by linear forms. Then $D[X_1, \ldots, X_n]/I$ is a UFD if and only if I is prime and (p, I) is prime for every prime $p \in D$.*

4. **A family of examples.** In [7, Example 6.3] Nicolas constructs an example of a rank two torsion-free abelian group which is a factorial module over

the integers, but which is not free or even a submodule of any direct product of copies of the integers. We are going to use the same construction with a few modifications which will enable us to draw conclusions about the symmetric algebra of the resulting module.

Let D be an integral domain with quotient field K. Let $\{p_i\}_{i=1}^{\infty}$ be a sequence of nonzero elements of D. Inductively define a sequence of rank two free D-submodules of $K \oplus K$ as follows. Let $F_1 = D \oplus D$, and once $F_1, \ldots, F_n$ have been chosen, choose F_{n+1} so that the matrix of the inclusion map $F_n \subseteq F_{n+1}$ is

$$\begin{pmatrix} 1 & 0 \\ -1 & p_n \end{pmatrix}.$$

(This is possible since the matrix has nonzero determinant.) Set $M = \bigcup_{i=1}^{\infty} F_i$. We shall refer to M as the module determined by the sequence $\{p_i\}$. Note that M is flat of rank two and is free if and only if it is finitely generated if and only if all but a finite number of the p_i's are units.

Since formation of symmetric algebras commutes with direct limits, $S(M) = \varinjlim S(F_i)$. But by [5, Corollary 3.12] we have $S(F_1) \subseteq S(F_2) \subseteq \cdots$ and hence $S(M) = \bigcup_{i=1}^{\infty} S(F_i)$. Now $S(F_i) = D[X_i, Y_i]$ for each i, where X_i and Y_i are indeterminates. Furthermore we know that $X_1 = X_{i+1}$ and $Y_i = -X_{i+1} + p_i Y_{i+1}$ for each $i \geqslant 1$. Since, for $m \geqslant 0$, the symmetric power $S^m(F_i)$ is the free D-module with basis $X_i^m, X_i^{m-1}Y_i, \ldots, Y_i^m$, the equations in the preceding sentence allow us to compute the matrix for the inclusion map $S^m(F_i) \subseteq S^m(F_{i+1})$. The matrix is the lower triangular $m+1$ by $m+1$ matrix

$$\begin{pmatrix} 1 & 0 & & & \cdots & 0 \\ -1 & p_i & 0 & & & 0 \\ 1 & -2p_i & p_i^2 & 0 & & 0 \\ \cdot & & & \cdot & & \cdot \\ \cdot & & & & \cdot & \cdot \\ \cdot & & & & & \cdot \\ (-1)^m & \binom{m}{1}(-1)^{m-1}p_i & \binom{m}{2}(-1)^{m-2}p_i^2 & \cdots & \binom{m}{r}(-1)^{m-r}p_i^r & \cdots p_i^m \end{pmatrix}$$

By induction one then shows that the matrix for the inclusion map $S^m(F_1) \subseteq S^m(F_{n+1})$ is the lower triangular $m+1$ by $m+1$ matrix

$$\begin{pmatrix} 1 & 0 & & & & 0 \\ -x_n & y_n & 0 & & & 0 \\ x_n^2 & -2x_n y_n & y_n^2 & 0 & & 0 \\ \cdot & & & & & \cdot \\ \cdot & & & & & \cdot \\ \cdot & & & & & \cdot \\ (-x_n)^m & \binom{m}{1}(-x_n)^{m-1}y_n & \binom{m}{2}(-x_n)^{m-2}y_n^2 & \cdots & \binom{m}{r}(-x_n)^{m-r}y_n^r \cdots & y_n^m \end{pmatrix},$$

where $x_n = 1 + p_1 + p_1p_2 + \cdots + p_1p_2 \cdots p_{n-1}$ and $y_n = p_1 \cdots p_n$. (Note that $x_{n+1} = x_n + y_n$ and $y_{n+1} = p_{n+1}y_n$.)

For the remainder of this section we let D be a UFD, and assume that $\{p_i\}$ is a sequence of distinct primes. $S^m(M)$ will be factorial if and only if each symmetric power $S^m(M)$ has the f.d.p. Since for each $x \in S^m(M)$ there is a nonzero element $d \in D$ such that $dx \in S^m(F_1)$, $S^m(M)$ will have the f.d.p. if and only if each nonzero element of $S^m(F_1)$ has a finite number of divisors when considered as an element of $S^m(M)$. Let $x = (a_0, \ldots, a_m)$ be a nonzero element of the free module $S^m(F_1)$. When considered as an element of $S^m(F_{n+1})$, the only prime power divisors of x are those it had as an element of $S^m(F_n)$ and, possibly, a power of p_n. (This follows from knowing the matrix for $S^m(F_n) \subseteq S^m(F_{n+1})$.) Now the image of x in $S^m(F_{n+1})$ has each of its components divisible by p_n except possibly the first one, $a_0 - a_1x_n + \cdots + a_m(-x_n)^m$. Hence x will have a finite number of divisors as an element of $S^m(M)$ if and only if there is an integer N such that $n \geqslant N$ implies $p_n \nmid a_0 - a_1x_n + \cdots + a_m(-x_n)^m$. And from this we arrive at the conclusion that $S^m(M)$ is factorial if and only if for every nonzero polynomial $f(X) \in D[X]$ with $\deg f(X) \leqslant m$ there is an integer N such that $n \geqslant N$ implies $p_n \nmid f(x_n)$. Similarly, $S(M)$ is factorial if and only if for every nonzero polynomial $f(X) \in D[X]$ there is an integer N such that $n \geqslant N$ implies $p_n \nmid f(x_n)$.

Let Z be the ring of integers.

4.1. THEOREM. *There is a rank two torsion-free abelian group M such that $S_Z(M)$ is a UFD, but M is not a submodule of any direct product of copies of Z.*

PROOF. Inductively choose a sequence of primes as follows. Let $p_1 = 2$. Assuming $p_1, \ldots, p_{n-1}$ have been chosen, let $x_n = 1 + p_1 + p_1p_2 + \cdots + p_1 \cdots p_{n-1}$ and choose a prime $p_n > n(1 + x_n + \cdots + x_n^{n-1})$. Then given a nonzero $f(X) = a_0 + \cdots + a_mX^m \in Z[X]$, choose $N > \max\{m, |a_0|, \ldots, |a_m|\}$.

If $n \geqslant N$ we have $|f(x_n)| \leqslant n(1 + x_n + \cdots + x_n^{n-1}) < p_n$, and hence $p_n \nmid f(x_n)$. It follows that $S(M)$ is a UFD, where M is the module determined by $\{p_i\}$. The second assertion about M (i.e., that it is not "torsionless") is proved in [7].

4.2. THEOREM. *For each integer $s \geqslant 1$ there is a rank two torsion-free abelian group M_s such that $S^i(M_s)$ is factorial for $0 \leqslant i < 2^s$, but $S^i(M_s)$ is not factorial for $i \geqslant 2^s$.*

Theorem 4.2 will be proved once we have carefully selected a sequence of primes. This careful selection of primes is number theoretic in nature and so we make it a separate theorem from which 4.2 follows.

4.3. THEOREM. *Given a positive integer s, there is a sequence of distinct primes $\{p_i\}$ such that if $x_n = 1 + p_1 + \cdots + p_1 \cdots p_{n-1}$, then*

(i) $p_{2n+1} | 1 + (x_{2n+1})^{2^s}$ *for all $n \geqslant 0$, and*

(ii) *if $f(X) \in Z[X]$, $f(X) \neq 0$, has degree less than 2^s, then $p_n | f(x_n)$ for only finitely many n.*

PROOF. Choose $p_1 = 2$ and suppose $p_1, \ldots, p_{2n-1}$ have been chosen. Choose a prime $q \equiv 1 \pmod{2^{s+1}}$ such that $q > (x_{2n})^{2^s} + 1$, using Dirichlet's theorem on primes in arithmetic progressions. Note that -1 has a 2^sth root $(\mathrm{mod}\, q)$. Let $w \in Z$ represent this root.

Let $z_n = p_1 \cdots p_{n-1}$. Consider the polynomial $g(X) = 1 + (x_{2n} + z_{2n}X)^{2^s}$. The congruence $g(X) \equiv 0 \pmod q$ has a solution $x = (-x_{2n} + w)/z_{2n}$. (Note that $q > z_{2n}$, so $z_{2n} \not\equiv 0$.) Furthermore, $g(0) = (x_{2n})^{2^s} + 1 \not\equiv 0 \pmod q$, so $x \not\equiv 0 \pmod q$. By Dirichlet's theorem again, there is a prime $p_{2n} > 2n(1 + x_{2n} + \cdots + x_{2n}^{2^s-1})$ such that $p_{2n} \equiv x \pmod q$. This picks p_{2n}. Let $p_{2n+1} = q$.

Note that $p_{2n+1} \neq p_{2n}$ and $p_{2n}, p_{2n+1} > p_i$ for $1 \leqslant i \leqslant 2n - 1$, so all the primes are distinct.

By our choice of p_{2n}, $p_{2n+1} | 1 + (x_{2n} + z_{2n}p_{2n})^{2^s} = 1 + (x_{2n+1})^{2^s}$, so (i) is verified.

To verify (ii), let $f(X) \in Z[X]$, $f(X) \neq 0$ and suppose $\deg f(X) < 2^s$. Let N be an integer surpassing the maximum of the absolute values of the coefficients of $f(X)$. Then if $2n \geqslant N$, $|f(x_{2n})| < N(1 + x_{2n} + \cdots + x_{2n}^{2^s-1}) < p_{2n}$, so $p_{2n} | f(x_{2n})$ only if $f(x_{2n}) = 0$. Since $f(X)$ has only a finite number of roots, this occurs for finitely many n. We have now to see that $p_{2n+1} | f(x_{2n+1})$ for only finitely many n. Keeping in mind that $(x_{2n+1})^{2^s} \equiv -1 \pmod{p_{2n+1}}$ for $n \geqslant 0$, the following lemma will complete the proof.

4.4. LEMMA. *Let $s \geqslant 0$ be an integer, $\{p_i\}$ be a sequence of distinct*

primes, and $\{x_i\}$ *a sequence of integers. If* $f(X) \in Z[X]$ *has degree less than* 2^s, $x_n^{2^s} \equiv -1 \pmod{p_n}$ *for* $n \geqslant 1$, *and* $f(x_n) \equiv 0 \pmod{p_n}$ *for* $n \geqslant 1$, *then* $f(X) = 0$.

PROOF. We use induction on s, the result being clear if $s = 0$. Let $f(X) = \Sigma_{i=0}^{2^s-1} a_i X^i$. From $0 \equiv \Sigma a_i x_n^i \pmod{p_n}$ we get

$$x_n \sum_{(i \text{ odd})} a_i (x_n^2)^{(i-1)/2} \equiv \sum_{(i \text{ even})} a_i (x_n^2)^{i/2} \pmod{p_n}.$$

Squaring both sides we obtain $x_n^2 g^2(x_n^2) \equiv h^2(x_n^2)$, where g, h are the polynomials in x_n^2 appearing in the preceding congruence. Now the highest power of x_n^2 which occurs in $g^2(x_n^2)$ or $h^2(x_n^2)$ is $(x_n^2)^{2^s-2} \equiv (x_n^2)^{2^{s-1}}(x_n^2)^{2^{s-1}-2} \equiv -(x_n^2)^{2^{s-1}-2} \pmod{p_n}$. Hence $x_n^2 g^2(x_n^2) - h(x_n^2)$ can be expressed as a polynomial $r(x_n^2)$ of degree less than 2^{s-1} in x_n^2. Since neither g nor h nor the relations used in reducing to $r(x_n^2)$ depend on n, the polynomial $r(x_n^2)$ does not depend on n. By the induction hypothesis, $r(X) = 0$.

Now let y be a complex 2^{s-1}th root of -1. Then replacing x_n^2 by y in the reduction above we get $yg^2(y) - h^2(y) = r(y) = 0$. Hence $\sqrt{y}\, g(y) = h(y)$. Let $x = \sqrt{y}$. Then $xg(x^2) = h(x^2)$ yields $f(x) = 0$. But x is a 2^sth root of -1, and so has minimal polynomial $X^{2^s} + 1$. Thus $f(X) = 0$.

ACKNOWLEDGEMENT. The author benefited from conversations with G. Keller and R. E. Stong during the writing of this paper.

REFERENCES

1. N. Bourbaki, *Elements of mathematics, Commutative algebra*, Chap. VII, Actualités Sci. Indust., no. 1314, Hermann, Paris; Addison-Wesley, Reading, Mass., 1965, 1972. MR 41 # 5339; 50 # 12997.

2. D. L. Costa, *Symmetric algebras and retracts*, Dissertation, Univ. of Kansas, 1974.

3. R. M. Fossum, *The divisor class group of a Krull domain*, Springer-Verlag, Berlin and New York, 1973.

4. L. Fuchs, *Infinite abelian groups*, Vol. II, Academic Press, New York, 1973. MR 50 # 2362.

5. D. Lazard, *Autour de la platitude*, Bull. Soc. Math. France 97 (1969), 81–128. MR 40 # 7310; erratum, 41, p. 1965.

6. A.-M. Nicolas, *Modules factoriels*, Bull. Sci. Math. (2) 95 (1971), 33–52. MR 44 # 1653.

7. ———, *Extensions factorielles et modules factorable*, Bull. Sci. Math. 98 (1974), 117–143.

8. P. Samuel, *Anneaux gradués factoriels et modules réflexifs*, Bull. Soc. Math. France 92 (1964), 237–249. MR 32 # 4160.

DEPARTMENT OF MATHEMATICS, UNIVERSITY OF VIRGINIA, CHARLOTTESVILLE, VIRGINIA 22903