DECOMPOSABILITY OF MODULES[1]

IRVING KAPLANSKY

It is an old theorem, essentially due to Prüfer [5], that any torsion-free module of countable rank over a complete discrete valuation ring is a direct sum of modules of rank one. In [2] I generalized this to maximal valuation rings. In seeking to perfect this theorem, it is natural to ask: for what integral domains is it true that any torsion-free module of rank two is a direct sum of modules of rank one? There does not appear to be a simple answer. By changing the problem slightly, and confining the investigation to Noetherian domains, it is possible to single out the pleasant class of rings of the theorem below. However, the real reason for publishing this note is that the proof of Theorem 19 in [3] is, to put it politely, unconvincing.

THEOREM. *For any Noetherian integral domain R the following two statements are equivalent*: (1) *R is local, complete, and of Krull dimension ≤ 1.* (2) *Any torsion-free R-module of rank two which is not finitely generated is a direct sum of modules of rank one.*

That (1) implies (2) is not the contribution being made here; Matlis [4, Corollary 3 to Theorem 4] has proved from (1) the stronger result that any torsion-free R-module of finite rank is the direct sum of a divisible module and a finitely generated module.

The first part of the proof that (2) implies (1) will be devoted to showing that R has at most two maximal ideals. This portion could be replaced by later arguments plus a suitable localization procedure. However, I think the construction is worth recording since it is comparatively simple and may admit useful generalizations. In essence the construction is an adaptation of a standard way of getting an indecomposable module of rank two over a principal ideal ring with at least three primes.

Suppose then that M_i ($i=1, 2, 3$) are distinct maximal ideals in R. Let a be any element in M_1 but not in M_2 or M_3; choose b and c similarly with respect to M_2 and M_3. We work within V, a two-dimensional vector space with basis u, v over the quotient field Q of R. Let M be the submodule of V spanned by u/a^i, v/b^j ($i, j=1, 2, \cdots$) and $(u+v)/c$. It is evident that M is not finitely generated. By hypothesis, M is a direct sum of modules of rank one. We shall see that on the contrary M is indecomposable.

Note that u is divisible by arbitrarily high powers of a. The same is true for any multiple of u by an element of Q, i.e., for $Qu \cap M$. We claim that these are the only elements of M divisible by arbitrarily high powers of a. Now the general element of M has the form

$$(1) \qquad (xa^{-i} + zc^{-1})u + (yb^{-i} + zc^{-1})v$$

where $x, y, z \in R$. Suppose that (1) is divisible by arbitrarily high powers of a. The coefficient of v has the form w/b^ic. After division by a^n we must have an expression of the same form, i.e., with denominator of the form b^kc. This shows $wb^m \in (a^n)$ for a suitable m. Now $a \in M_1$, and $b \notin M_1$, whence $(b^m, M_1^n) = 1$. Hence $w \in M_1^n$. This is true for every n; since the intersection of the powers of M_1 is 0 (true for any proper ideal in a Noetherian domain), we have $w = 0$, as desired.

It follows that any endomorphism θ of M must send u into Qu. If θ is an idempotent endomorphism, then θu must be u or 0, and similarly $\theta v = v$ or 0. If θ is different from zero or the identity we may assume, by symmetry, that $\theta u = u$, $\theta v = 0$. Applying θ to $(u+v)/c$ we then get $u/c \in M$. On comparing this with (1) we find

$$xa^{-i} + zc^{-1} = c^{-1}, \qquad yb^{-i} + zc^{-1} = 0.$$

From this we deduce $a^ib^i = c(b^ix - a^iy) \in M_3$. But neither a nor b lies in M_3. Hence M admits no nontrivial idempotent endomorphisms. This contradiction shows that R has at most two maximal ideals, as claimed.

We shall next prove that R has Krull dimension ≤ 1 (i.e., the nonzero prime ideals in R are maximal). If this is not the case, then [1, p. 368] there exists in R an infinite number of prime ideals of rank one. Let P_1, P_2, P_3 be three of these and let S be the complement of the set-theoretic union $P_1 \cup P_2 \cup P_3$. Then S is multiplicatively closed and we can form the quotient ring R_S. The latter has exactly three maximal ideals. By what was shown above there exists an indecomposable torsion-free R_S-module M which has rank two and is not finitely generated. Looked at as an R-module, M is still torsion-free, indecomposable and of rank two; and it is true a fortiori that it is not finitely generated over R. This being a contradiction, we have shown that R has Krull dimension ≤ 1.

Only one point remains to be established: the completeness of R (in its topology as a semi-local ring). For a complete semi-local ring is a direct sum of local rings, and, since R is given to us as an integral domain, this will force R to be local. (But actually, the way the proof runs, we find R to be local before finishing the proof that R is complete.) Let t be any nonzero element in the intersection of the maxi-

mal ideals of R. Since R has Krull dimension ≤ 1, the topology of R can equally well be given by the powers of (t). Let $\{\delta_n\}$ be a nontrivial Cauchy sequence in R; we must prove that there is a limit for $\{\delta_n\}$ in R. We may assume (by passing to a suitable subsequence if necessary) that $\delta_{n+1} - \delta_n$ is divisible by t^n. We follow the plan in Theorem 19 of [3]. In the vector space with basis u, v over the quotient field Q of R take the module N spanned by v, w_0, w_1/t, $\cdots$, w_n/t^n, where $w_n = u + \delta_n v$. It is evident that N is not finitely generated. From the decomposability of N we shall extract the desired limit for $\{\delta_n\}$.

First we verify that $Qv \cap N = Rv$, i.e., the only fractional multiples of v present in N are integral multiples. The general element of N has the form

$$(2) \qquad \beta v + \alpha_0 w_0 + \alpha_1 w_1/t + \cdots + \alpha_n w_n/t^n$$

with β, $\alpha_i \in R$. For the coefficient of u to cancel we must have

$$\alpha_0 + \alpha_1/t + \cdots + \alpha_n/t^n = 0,$$

whence α_n is divisible by t. Also

$$(3) \qquad w_n/t^{n-1} = w_{n-1}/t^{n-1} + (\delta_n - \delta_{n-1})v/t^{n-1}$$

where $\delta_n - \delta_{n-1}$ is divisible by t^{n-1}. Substitution of (3) in (2) reduces n by one, and induction on n gives the desired result.

Since N is decomposable we have an idempotent endomorphism ϕ such that $\phi(N)$ is of rank one. Modifying ϕ by a scalar, we may assume that $\phi(u)$ and $\phi(v)$ are integral linear combinations of u and v, say $\phi(u) = r_1 u + r_2 v$, $\phi(v) = r_3 u + r_4 v$, $r_i \in R$. We know that the matrix of ϕ has determinant 0 and trace $\neq 0$, i.e.,

$$(4) \qquad r_1 r_4 = r_2 r_3, \qquad r_1 + r_4 \neq 0.$$

Since $u + \delta_n v$ is divisible by t^n in N, so is

$$(5) \quad \phi(u + \delta_n v) - (r_1 + \delta_n r_3)(u + \delta_n v) = [(r_2 + \delta_n r_4) - \delta_n(r_1 + \delta_n r_3)]v.$$

Hence the coefficient of v in (5) is divisible by t^n. We pass to the limit (in the completion R^* of R), writing $\gamma = \lim \delta_n$:

$$(6) \qquad (r_2 + \gamma r_4) - \gamma(r_1 + \gamma r_3) = 0.$$

We shall first use (6) to establish that R^* has no nilpotent elements. We may suppose that $\gamma^2 = 0$. Then (6) becomes $\gamma(r_1 - r_4) = r_2$. If $r_1 - r_4 \neq 0$ we deduce $\gamma \in R$ (here and several times later we are using the known fact that R^* intersects the quotient field of R in just R). On the other hand if $r_1 = r_4$, then $r_2 = 0$, and (4) is contradicted. Hence R^* has no nilpotent elements. It is known that this implies that the integral closure R' of R is a finitely generated R-module.

We next give R' further attention. We have that R' is a principal ideal ring with a finite number of primes. Suppose (the gap will be filled at the end of the paper) that our theorem is known for principal ideal rings. Then it will follow that R' can have only one prime, for an indecomposable torsion-free non-finitely-generated R'-module of rank two has the same properties when regarded as an R-module. Together with the fact that R' is a finitely generated R-module, this is known to imply that R^* is an integral domain. We can now tackle equation (6) in earnest. If $r_1 = 0$, then by (4), $r_4 \neq 0$ and r_2 or r_3 is 0. In either case we rapidly find $\gamma \in R$. If $r_1 \neq 0$, then

$$r_2 + \gamma r_4 = \frac{r_2}{r_1}(r_1 + \gamma r_3).$$

We find from (6) that γ is equal either to $-r_3/r_1$ or r_2/r_1. Thus $\gamma \in R$.

There remains finally the case where R is a principal ideal ring with exactly two primes p, q (this discussion is just what is missing in [3]). Let k be a unit in R, different from ± 1. Such a unit exists in R, since R has infinitely many units; for instance, $p + q^i$ are all distinct units. The completion R^* of R has the form $R_p^* \oplus R_q^*$. Let γ be the element of R^* which has components k, $1/k$. The module N above is constructed with $\delta_n \to \gamma$. If N is decomposable we have that (4) and (6) hold for $r_i \in R$. Looking at (6) in each summand of R^*, we see that (6) holds with γ replaced by either k or $1/k$. We again distinguish the cases $r_1 = 0$, $r_1 \neq 0$. If $r_1 = 0$, so that $r_4 \neq 0$ and r_2 or r_3 is 0, we rapidly deduce $k = 1/k$, a contradiction. If $r_1 \neq 0$, then (6) is solved as above, and we find that both k and $1/k$ are equal to r_2/r_1 or $-r_3/r_1$. Since $k \neq 1/k$, it must be the case that one is r_2/r_1 and the other $-r_3/r_1$. But then $r_2 r_3 = -r_1^2$, whence $r_1 + r_4 = 0$, contradicting (4). The proof of the theorem is now complete.

I am greatly indebted to Graham Higman for a stimulating conversation which revived my interest in the problem.

References

1. W. Krull, *Jacobsonsche Ringe, Hilbertscher Nullstellensatz, Dimensiontheorie*, Math. Z. **54** (1951), 354–387.

2. I. Kaplansky, *Modules over Dedekind rings and valuation rings*, Trans. Amer. Math. Soc. **72** (1952), 327–340.

3. ——, *Infinite abelian groups*, University of Michigan Press, Ann Arbor, 1954.

4. E. Matlis, *Some properties of Noetherian domains of dimension one*, Canad. J. Math. **13** (1961), 569–586.

5. H. Prüfer, *Theorie der abelschen Gruppen*. II. *Ideale Gruppen*, Math. Z. **22** (1925), 222–249.

University of Chicago