Riv. Mat. Univ. Parma (5) 5 (1996), 77-84

H. P. Goeters and C. J. Maxson (*)

Maximal submodules of finitely generated modules (**)

1 - Introduction

We are concerned with determining all maximal submodules of a given finitely generated module over a Dedekind domain R. We do this in general, and are able to show consequently that if R is a Dedekind domain with $|R/pR|$ finite for a particular prime element p of R, then given any finitely generated module F, there are only finitely many maximal submodules K for which F/K is bounded by p. Moreover, we are able to give a precise description of the possibilities for K in this case. Once we resolve the problem for finite rank free modules, the remaining issues follow from standard arguments.

Mainly our results pertain to counting the number of maximal submodules of F, a free R-module of rank n, and although our results go through under the general context mentioned initially, the assumption R/pR is a finite field when p is a prime element of R brings forth the strength in the discussions below. For example, such is the case when R is a subring of an algebraic number field since R/rR is finite for any $0 \neq r \in R$. Furthermore, the results obtained here are applicable elsewhere such as in the subject of extending R-homogeneous functions to homomorphisms.

(*) Dept. of Math., Auburn Univ., Auburn, AL. 36849, USA; Dept. of Math., Texas A & M., College Station, TX. 77843, USA.

(**) Received May 20, 1996. AMS classification 16 D 30.

2 - When R is a principal ideal domain

Throughout this section, F will represent R^n where R is a PID and we will be concerned with describing the maximal submodules K of F. For any submodule K of F, the stacked basis theorem applies. This means there is a basis $x_1, \ldots, x_n$ of F and elements $k_1, \ldots, k_n$ of R for which the non-zero elements among $k_1 x_1, \ldots, k_n x_n$ constitute a basis for K. We will refer to the basis $x_1, \ldots, x_n$ as a *stacked basis* for F over K in this case.

Our first comment is just a direct application of the stacked basis theorem.

Proposition 1. *$K \subseteq F$ is maximal if and only if there is a prime p of R and a basis $x_1, x_2, \ldots, x_n$ of F such that $px_1, x_2, \ldots, x_n$ is a basis for K.*

Proof. To prove that K is maximal, just note that in the present case we have $F/K \simeq R/pR$. To prove the converse, we remark that by the stacked basis theorem, there is a basis $x_1, \ldots, x_n$ of F and elements $k_1, \ldots, k_n$ of R such that $k_1 x_1, \ldots, k_n x_n$ is a basis for K. Because K is maximal, all but one of $k_1, \ldots, k_n$ are units and the remaining k_j must be prime.

When $F/K \simeq R/pR$ we will refer to K as *p-maximal*. Actually one can be very explicit concerning the p-maximal submodules of F; our intent will be realized in Theorem 1. A submodule H of F is called *pure*, written $H \lhd F$, if for any $0 \neq r \in R$ and $x \in F$ with $rx \in H$, one has $x \in H$. The following is well-known and follows easily from the stacked basis theorem.

Lemma 1. *If $x \in K$ is such that $\langle x \rangle \lhd F$, then $\langle x \rangle$ is a direct summand of K.*

Proof. By the stacked basis theorem, there is a basis $x_1, \ldots, x_n$ of F and ring elements $k_1, \ldots, k_n$ for which the nonzero elements among $k_1 x_1, \ldots, k_n x_n$ form a basis for $\langle x \rangle$. Then, only one of $k_1 x_1, \ldots, k_n x_n$ is nonzero, say $k_1 x_1 \neq 0$, and since $k_1 x_1 \in \langle x \rangle \lhd F$, $x_1 \in \langle x \rangle$. This implies k_1 is a unit and $x, x_2, \ldots, x_n$ is a basis for F. The restriction to K of the projection map from F onto $\langle x \rangle$ is split by the embedding of $\langle x \rangle$ in K.

We remark that for any basis $x_1, \ldots, x_n$ of F and ring elements $a_2, \ldots, a_n$, the collection $x_1, x_2 - a_2 x_1, \ldots, x_n - a_n x_1$ constitutes a basis for F.

Lemma 2. *If $x \in K$ extends to a stacked basis $x = x_1, x_2, \ldots, x_n$ for F over K, then for all $a_2, \ldots, a_n \in R$, $x, x_2 - a_2 x, \ldots, x_n - a_n x$ is a stacked basis for F over K.*

Proof. Let $k_2, \ldots, k_n$ belong to R, such that $x, k_2x_2, \ldots, k_nx_n$ is a basis for K. Then $x, k_2x_2 - k_2a_2x, \ldots, k_nx_n - k_na_nx$ is also a basis for K, and $x, x_2 - a_2x, \ldots, x_n - a_nx$ is a basis for F.

Given a submodule H of F, the pure submodule of F generated by H is

$$\langle H\rangle_* = \{x \in F \mid rx \in H, \text{ for some non-zero } r \in R\}.$$

Following the usual convention, we will use the notation $e_1, \ldots, e_n$ to represent the standard basis of F.

Theorem 1. *Let S be a complete set of representatives of cosets in R/pR for a given prime p of R. Then, $K \subseteq F$ is p-maximal if and only if there exists an index i, and $k_j \in S$ for $j \neq i$, such that $\{e_j + k_je_i \mid j \neq i\} \cup \{pe_i\}$ is a basis for K.*

Proof. We prove first the existence of an index i as required in the statement. By Proposition 1, there is a stacked basis $x_1, \ldots, x_n$ for F such that $px_1, x_2, \ldots, x_n$ is a basis for K. Regarding $x_j \in R^n$ as an n-tuple, write $x_j = \begin{pmatrix} a_j \\ * \end{pmatrix}$ where the $*$ represents entries of the *don't care* variety.

Case 1: $p \nmid a_j$ for some $j \geq 2$.

Since e_1 belongs to span $\{x_1, \ldots, x_n\}$, $gcd(a_1, \ldots, a_n) = 1$. In this case, $gcd(pa_1, a_2, \ldots, a_n) = 1$, so there are elements $u_1, \ldots, u_n$ of R, for which $u_1pa_1 + \sum_2^n u_ia_i = 1$. Then, $x = u_1px_1 + \ldots + u_nx_n = \begin{pmatrix} 1 \\ * \end{pmatrix} \in K$.

Clearly this implies that $\langle x\rangle \lhd F$, so by Lemma 1, $K = \langle x\rangle \oplus K_0$ for a particular submodule K_0. With $F_0 = \langle K_0\rangle_*$, $\langle x\rangle \cap F_0 = \{0\}$ and $\langle x\rangle \oplus F_0$ properly contains K, and due to the maximality of K, $\langle x\rangle \oplus F_0 = F$. We may, of course, obtain a stacked basis $y_2, \ldots, y_n$ for F_0 over K_0. Let b_j = first entry of y_j, viewing $y_j \in R^n$ (as above). By Lemma 2, since $x, y_2, \ldots, y_n$ is a stacked basis for F over K, $x, y_2 - b_2x, \ldots, y_n - b_nx$ is a stacked basis for F over K. Therefore, since $y_i - b_ix \in \bigoplus_{j\geq 2} Re_j$ for $i \geq 2$, $K = \langle x\rangle \oplus K'$ where $K' = K \cap \bigoplus_{j\geq 2} Re_j$ is a maximal submodule of $F' = \bigoplus_{j\geq 2} Re_j$.

By induction, for some index $i \geq 2$, and representatives $k_j \in S, j \neq i, j \geq 2$, we have that $\{e_j + k_je_i \mid j \geq 2, \ j \neq i\} \cup \{pe_i\}$ is a basis for K'. Let $c_j = j^{th}$ entry of $x \in R^n$, and define, $k_i = 0$ (temporarily) for notational purposes. Select k_1 to be the residue mod p of $-\Sigma_{j\geq 2} c_jk_j$ in S and let $b \in R$ so that $pb = -k_1 - \Sigma_{j\geq 2} c_jk_j$. Using Lemma 2 one can then replace x in the basis

$$\{x\} \cup \{e_j + k_je_i \mid j \geq 2, j \neq i\} \cup \{pe_i\}$$

for K, by $x' = x - \Sigma_{j\geq 2} c_j(e_j + k_je_i) - bpe_i$. Noting that $x' = e_1 + k_1e_i$, we now have obtained a basis as prescribed in the statement of the theorem.

Case 2: $p \mid a_j$ for all $j \geqslant 2$.

In this case $K = Rpx_1 \oplus Rx_2 \oplus \ldots \oplus Rx_n \subseteq Rpe_1 \oplus (\oplus_{j \geqslant 2} Re_j)$ so that $K = Rpe_1 \oplus (\oplus_{j \geqslant 2} Re_j)$ by the p-maximality of K.

The proof of the converse is very short. Given the basis for K as stated, $\{e_j + k_j e_i \mid j \neq i\} \cup \{e_i\}$ is a stacked basis for F over K. By Proposition 1, K is p-maximal.

From the above theorem there are only finitely many p-maximal submodules of R^n in the situation that R/pR is finite. In order to give a precise accounting of this number, we now investigate which basis′ of the form presented in Theorem 1 yield the same p-maximal submodule.

Lemma 3. *Let K have basis $\{e_i + k_j e_1 \mid j \neq 1\} \cup \{pe_1\}$ with $k_j \in R$, for $j \geqslant 2$, and set $k_1 = -1$. Given $i \neq 1$, the set $\{e_j + l_j e_i \mid j \neq i\} \cup \{pe_i\}$ with $l_j \in R$ forms a basis for K if and only if the system of equations $k_i l_j \equiv -k_j$ mod p $(j \neq i)$ is satisfied.*

Proof. Since without loss of generality we can assume $i = 2$, we start from the basis $\{e_j + l_j e_2 \mid j > 2\} \cup \{pe_2\}$. Represent $e_j + l_j e_2$ as $pc_1 e_1 + \sum_{i \geqslant 2} c_i(e_i + k_i e_1)$ with $c_1, \ldots, c_n \in R$. First assume $j > 2$ (i.e. $j \neq 1$). Comparing coefficients leads to $c_i = 0$ for each $i \neq j, 1, 2$, $c_j = 1$, $pc_1 + \sum_{i \geqslant 2} c_i k_i = 0$, and $c_2 = l_j$. Assimilating these conditions leads to one equation $pc_1 + l_j k_2 + k_j = 0$. Thus $k_2 l_j \equiv -k_j \bmod p$ for each $j > 2$.

For $j = 1$ the representation $e_1 + l_1 e_2 = pc_1 e_1 + \sum_{i \geqslant 2} c_i(e_i + k_i e_1)$ leads to the conditions $c_i = 0$ for $i \geqslant 3$, and $pc_1 + \sum_{i \geqslant 2} c_i k_i = 1$. These conditions reduce to the singleton $pc_1 + l_1 k_2 = 1$. Since k_1 is defined as -1, then $l_1 k_2 \equiv -k_1 \bmod p$ as claimed.

To prove the converse, let K' have basis $\{e_j + l_j e_i \mid j \neq i\} \cup \{pe_i\}$. If we show that $K' \subseteq K$, then by the p-maximality of K' (Theorem 1), $K' = K$. For each j different from i, there exists $a_j \in R$ which provides $k_i l_j + k_j + pa_j = 0$ in R. This equation allows $e_j + l_j e_i = pa_j e_1 + (e_j + k_j e_1) + l_j(e_i + k_i e_1)$ from which $e_j + l_j e_i \in K$ follows. Also, $e_1 + l_1 e_i = pa_1 e_1 + l_1(e_i + k_i e_1) \in K$.

We will refer to a basis for K of the form $\{e_j + k_j e_i \mid j \neq i\} \cup \{pe_i\}$, for some i, where each k_j represents a coset in R/pR, as a *staggered basis* for K. Also, a different staggered basis for K $\{e_j + l_j e_m \mid j \neq m\} \cup \{pe_m\}$ where l_j for all $j \neq m$ are representatives of cosets in R/pR (i.e. $i \neq m$) will be called an *alternate staggered basis* for K.

Let S denote a complete set of representatives of cosets in R/pR. If K has the staggered basis $\{e_j + k_j e_i \,|\, j \neq i\} \cup \{pe_i\}$ with each $k_j \in S$ for a particular i, along with the alternate staggered basis $\{e_j + l_j e_i \,|\, j \neq i\} \cup \{pe_i\}$ where $l_j \in S$, for all $j \neq i$, then we must have $k_j = l_j$ for all j. This is due to the fact that if some $k_j \neq l_j$, then $(k_j - l_j)e_i = e_j + k_j e_i - (e_j + l_j e_i) \in K$ and $0 \neq k_j - l_j$ is relatively prime to p. This will allow $e_i = u(k_j - l_j)e_j + vpe_i \in K$ (for some $u, v \in R$) contradicting the maximality of K.

Theorem 2. *Suppose K has a staggered basis $\{e_j + k_j e_i \,|\, j \neq i\} \cup \{pe_i\}$. Take m to be the number of coefficients k_j for $j \neq i$, which are non-zero. Then, K has exactly m distinct alternate staggered bases.*

Proof. We may assume that $i = 1$ for ease of discussion and we will first consider the case $m > 0$. Recycling the use of the index i, suppose that $\{e_i + l_j e_i \,|\, j \neq i\} \cup \{pe_i\}$ is an alternate staggered basis for the submodule $K = \text{span}\,\{\{e_j + k_j e_1 \,|\, j \neq 1\} \cup \{pe_1\}\}$. Then, taking $k_1 = -1$, Lemma 3 applies and $l_j k_i \equiv -k_j \bmod p$, for each $j \neq i$. Because $m > 0$, the linear equations could not be fulfilled if $k_i = 0$, so an alternate basis like the one prescribed cannot exist under these circumstances. On the other hand, if $k_i \neq 0$, then there is exactly one choice for the sequence of numbers l_j, $j \neq i$ and that is when $l_j \in S$ is congruent to $-k_j k_i^{-1} \bmod p$. This implies that there is exactly one alternate staggered basis for each index i with $k_i \neq 0$. Note that we are not counting k_1 in this instance.

If $m = 0$, then $K = Rpe_1 \oplus (\oplus_{j \geq 2} Re_j)$. All of the linear congruences $l_j k_i \equiv -k_j \bmod p$, $j \neq i$ obtained from Lemma 3, can be satisfied in this case, except when $j = 1$. Therefore, K has no alternate staggered bases.

If $\delta = |R/pR|$ is finite, then there are $n\delta^{n-1}$ staggered bases available. However, this number far exceeds the number of p-maximal submodules of F.

Theorem 3. *Suppose that $\delta = |R/pR|$ where p is a prime element of R. Then F has exactly $\delta^{n-1} + \ldots + \delta + 1$ distinct p-maximal submodules.*

Proof. As above, let S constitute a complete set of representatives of cosets in R/pR. Every p-maximal submodule is determined by some staggered basis $B = \{e_j + k_j e_i \,|\, j \neq i\} \cup \{pe_i\}$ where $k_j \in S$ by Theorem 1. Given such a basis, set $k_i = -1$ as in Lemma 3. Then, by the *support of the basis B* we mean $\{j \,|\, k_j \neq 0\}$ (here, we are counting k_i). From Lemma 3, every alternate staggered basis $B' = \{e_j + l_j e_t \,|\, j \neq t\} \cup \{pe_t\}$ for span B has the same support as B.

Therefore, we can refer to the *support of a p-maximal submodule K* as the support of B when B is a staggered basis for K.

We now count the number of unequal p-maximal submodules whose support is a given subset $I \subseteq \{1, 2, \dots, n\}$. Let $m = |I|$. If $m = 1$, there is only one p-maximal submodule supported by $I = \{i\}$, namely, $pRe_i \oplus (\oplus_{j \neq i} Re_j)$. There are n distinct maximal submodules of this type, one for each $i = 1, \dots, n$. Assume $m > 1$, and without loss of generality, $I = \{1, 2, \dots, m\}$.

We claim that every staggered basis supported by I belongs to a p-maximal submodule with a staggered basis of the form

$$B = \{e_j + k_j e_1 \,|\, 2 \leq j \leq m\} \cup \{e_j \,|\, j > m\} \cup \{pe_1\} \qquad k_j \in S\,.$$

Let $\quad B' = \{e_j + l_j e_i \,|\, j \neq i,\ 1 \leq j \leq m\} \cup \{e_j \,|\, j > m\} \cup \{pe_i\}$

be a staggered basis supported by I. After setting $l_i = -1$, define k_j by setting $k_j \in S$ equal to the representative of $l_j l_1^{-1}$ computed in R/pR for $2 \leq j \leq m$. By Lemma 3, $\operatorname{span} B = \operatorname{span} B'$. There are exactly $(\delta - 1)^{m-1}$ staggered bases of the form $B = \{e_j + k_j e_1 \,|\, 2 \leq j \leq m\} \cup \{e_j \,|\, j > m\} \cup \{pe_1\}$, one for each choice for the ordered sequence $k_2, \dots, k_m$ from $S \backslash pR$.

Finally, there are $(\delta - 1)^{m-1}$ staggered bases supported by $I \subseteq \{1, \dots, n\}$ of cardinality $m > 1$, which are in $1-1$ correspondence with the unequal p-maximal submodules supported by I. From this and the computation from the case $m = 1$, there are then exactly $\sum_{m=2}^{n} \binom{n}{m} (\delta - 1)^{m-1} + n$ unequal p-maximal submodules. Recall $\sum_{m=0}^{n} \binom{n}{m} c^m = (1 + c)^n$, which affords

$$\sum_{m=2}^{n} \binom{n}{m} (\delta - 1)^{m-1} = \sum_{m=2}^{n} \binom{n}{m} \frac{(\delta - 1)^m}{\delta - 1} = \frac{\delta^n - n(\delta - 1) - 1}{\delta - 1}$$

and consequently there are exactly $\dfrac{\delta^n - 1}{\delta - 1} - n + n = \delta^{n-1} + \dots + \delta + 1$ unequal p-maximal submodules.

3 - Generalizations and applications

We are now able to extend the results from Section 2 to finitely generated modules over Dedekind domains. Of course the stacked basis theorem does not hold over Dedekind domains, but when considering maximal submodules, we may localize the problem at prime ideals. Throughout this section, R will denote a *Dedekind domain*.

Given a module M and a prime ideal P of R, a *P-maximal* submodule of M is a submodule K such that $M/K \simeq R/P$. Of course, every maximal submodule of M is P-maximal for some prime P of R. We present some of the consequences of

Section 2 under the current context. Recall that any finitely generated module M decomposes as $M = T \oplus M'$ with T torsion, and M' projective.

Lemma 4. *Let M be finitely generated and K a P-maximal submodule of M. Write $M = T' \oplus M_0$ where $T' = \oplus_{P' \neq P} T_{P'}$. Then $K = T' \oplus K_0$ with K_0 P-maximal in M_0.*

Proof. Because $M/K \simeq R/P$ while the order ideals of elements in T' are coprime with P, we must have $T' \subseteq K$. From above, T' is a direct summand of M, so a general computation reveals that $K = T' \oplus K_0$ with $K_0 = K \cap M_0$ when $M = T' \oplus M_0$. The remainder then follows easily.

By $\mu_R(M)$ we will mean the minimal number of generators required to generate M as an R-module.

Theorem 4. *Let R be Dedekind with a non-zero prime ideal P and let M be a finitely generated module. With $M = T' \oplus M_0$ as in Lemma 4, and $n = \mu_{R_P}(M_P)$, we have:*

1. *Let $x_1, \ldots, x_n$ from M_0 generate $M_P = (M_0)_P$ as an R_P-module. The P-maximal submodules of M are precisely the submodules of the form $K = T' \oplus (X_i \cap M)$ where X_i is the R_P-submodule of M generated by $\{x_j + k_j x_i \mid j \neq i\} \cup \{px_i\}$ for some i, where $p \in R$ satisfies $pR_P = PR_P$.*

2. *If $\delta = |R/P| < \infty$, then M has precisely $\delta^{n-1} + \ldots + \delta + 1$ P-maximal submodules.*

Proof. The proof of 2 follows directly via Theorem 3 once we substantiate **1.** Let K represent a P-maximal submodule of M. We note that $M = T' \oplus (M_P \cap M)$ and it then follows from Lemma 2 that $K = T' \oplus K_0$ for $K_0 = K \cap M_P \cap M = K_P \cap M$. It remains to show that $K_P = X_i$ for some i.

We have now reduced consideration to the case that R is a local PID and $M = M_P$ is finitely generated with maximal submodule $K = K_P$. Set $F = R^n$ and define a map from $F \to M$ by sending $e_j \mapsto x_j$. Call the kernel of this map L. Evidently K arises as the image of a maximal submodule of F containing L.

If $L \nsubseteq pF$ where pR is the prime ideal of R, say $x \in L \backslash pF$, then it is not hard to check that $\langle x \rangle \lhd F$. From Lemma 1 we find that $\langle x \rangle$ is a direct factor of L and F, so $(F/\langle x \rangle)/(L/\langle x \rangle) \simeq M$, contradicting the minimality of n. Thus, $L \subseteq pF$ and hence L must be contained in every p-maximal submodule H of F. The remainder of the proof is a consequence of the correspondence theorem and Theorem 1.

A long standing problem in combinatorial group theory is to count the number of subgroups of a finite abelian p-group.

Corollary 1. *A finite abelian p-group with a minimal number of n generators, has exactly* $p^{n-1} + \dots + p + 1$ *maximal subgroups.*

References

[1] H. Bass, *Torsion-free and projective modules*, Trans. Amer. Math. Soc. **102** (1962), 319-327.

[2] L. Fuchs, *Infinite Abelian Groups*, I, II, Academic Press, New York 1970, 1973.

Sommario

Si prova che, se R *è un dominio di Dedekind e* $|R/pR|$ *è finito per un elemento primo* p *di* R, *allora, dato un modulo finitamente generato* F, *esiste solo un numero finito di sottomoduli massimali* K *per cui* $|F/K|$ *è limitato da* p.

Si indica poi il numero dei sottomoduli massimali di F, *con* F *R-modulo libero di rango* n. *In particolare è interessante il caso in cui* R/pR *è un campo finito.*

* * *