



كلية : التربية للعلوم الصرفة

القسم او الفرع : الرياضيات

المرحلة : الرابعة

أستاذ المادة : ا.م.د. ماجد محمد عبد

اسم المادة باللغة العربية : مقاسات

اسم المادة باللغة الإنكليزية : **MODULES**

اسم المحاضرة الأولى باللغة العربية : المقاس المنته التولد

اسم المحاضرة الأولى باللغة الإنكليزية : **finitely generated module**

محتوى المحاضرة الثالثة

Definition ( $IM$ , module quotients, annihilators). Let  $M$  be an  $R$ -module.

(a) For an ideal  $I \in R$  we set

$$IM := \{ \sum_{i=1}^n a_i m_i : a_i \in I; m_i \in M \}$$

$$= \{ \sum_{i=1}^n a_i m_i + \sum_{j=1}^m a_j n_j : n_j \in N; a_1, \dots, a_n \in I; m_1, \dots, m_n \in M; n_1, \dots, n_m \in N \}$$

Note that  $IM$  is a submodule of  $M$ , and  $M/IM$  is an  $R/I$ -module in the obvious way.

(b) For two submodules  $N, N_0 \subseteq M$  the module quotient (not to be confused with the quotient modules of Definition 3.3 (d)) is defined to be

$$N_0 : N := \{ a \in R : aN \subseteq N_0 \} \subseteq R$$

In particular, for  $N_0 = 0$  we obtain the so-called annihilator

$$\text{ann} N := \text{ann}_R N := \{ a \in R : aN = 0 \} \subseteq R$$

of  $N$ . The same definition can also be applied to a single element  $m \in M$  instead of a submodule

$N$ : we then obtain the ideals

$N_0 := \{fa \in R : am \in N_0\}$  and  $\text{ann } m := \{fa \in R : am = 0\}$   
of  $R$ .

Example

(a) If  $M, N$ , and  $N_0$  are submodules of the  $R$ -module  $R$ , i. e. ideals of  $R$  the product  $IM$  and quotient  $N_0 : N$  are exactly the product and quotient of ideals as in

(b) If  $I$  is an ideal of a ring  $R$  then  $\text{ann}_R(R/I) = I$ .

Let us recall again the linear algebra of vector spaces over a field  $K$ . At the point where we are now, i. e. after having studied subspaces and morphisms in general, one usually restricts to finitely generated vector spaces and shows that every such vector space  $V$  has a finite basis. This makes  $V$  isomorphic to  $K^n$  with  $n = \dim_K V \in \mathbb{N}$ . In other words, we can describe vectors by their coordinates with respect to some basis, and linear maps by matrices — which are then easy to deal with.

For a finitely generated module  $M$  over a ring  $R$  this strategy unfortunately breaks down. Ultimately, the reason for this is that the lack of a division in  $R$  means that a linear relation among generators of  $M$  cannot necessarily be used to express one of them in terms of the others (so that it can be dropped from the set of generators). For example, the elements  $m = 2$  and  $n = 3$  in the  $\mathbb{Z}$ -module  $\mathbb{Z}$  satisfy the linear relation  $3m + 2n = 0$ , but neither is  $m$  an integer multiple of  $n$ , nor vice versa. So although  $\mathbb{Z} = \langle m, n \rangle$  and these two generators are linearly dependent over  $\mathbb{Z}$ , neither  $m$  nor  $n$  alone generates  $\mathbb{Z}$ .

The consequence of this is that a finitely generated module  $M$  need not have a linearly independent set of generators. But this means that  $M$  is in general not isomorphic to  $R^n$  for some  $n \in \mathbb{N}$ , and thus there is no obvious well-defined notion of dimension. It is in fact easy to find examples for this:  $\mathbb{Z} \in \mathbb{Z}$  as a  $\mathbb{Z}$ -module is certainly not isomorphic to  $\mathbb{Z}^n$  for some  $n$ .

So essentially we have two choices if we want to continue to carry over our linear algebra results on finitely generated vector spaces to finitely generated modules:

### Modules

- \_ restrict to  $R$ -modules that are of the form  $R^n$  for some  $n \in \mathbb{N}$ ; or
- \_ go on with general finitely generated modules, taking care of the fact that generating systems cannot be chosen to be independent, and thus that the coordinates with respect to such

systems are no longer unique.

In the rest of this chapter, we will follow both strategies to some extent, and see what they lead to. Let us start by considering finitely generated modules that do admit a basis.

### Finitely generated R-module

Definition (Bases and free modules). Let  $M$  be a finitely generated  $R$ -module.

(a) We say that a family  $(m_1; \dots; m_n)$  of elements of  $M$  is a basis of  $M$  if the  $R$ -module homomorphism

(b) If  $M$  has a basis, i. e. if it is isomorphic to  $R^n$  for some  $n$ , it is called a free  $R$ -module.

Example If  $I$  is a non-trivial ideal in a ring  $R$  then  $R=I$  is never a free  $R$ -module: there can be no isomorphism

Exercise Let  $R$  be an integral domain. Prove that a non-zero ideal  $I \in R$  is a principal ideal if and only if it is a free  $R$ -module.

Remark (Linear algebra for free modules). Let  $M$  and  $N$  be finitely generated, free  $R$  modules.

(a) Any two bases of  $M$  have the same number of elements: assume that we have a basis with  $n$  elements, so that  $M \cong$

$R^n$  as  $R$ -modules. Choose a maximal ideal  $I$  of  $R$

Then  $R=I$  is a field and  $M=IM$  is an  $R=I$ -vector space

(a). Its dimension is

$$\dim_{R=I} M = \dim_{R=I} IM = \dim_{R=I} IR^n = \dim_{R=I} (R=I)^n = n;$$

and so  $n$  is uniquely determined by  $M$ . We call  $n$  the rank  $\text{rk} M$  of  $M$ .

(b) In the same way as for vector spaces, we see that  $\text{Hom}_R(R^m; R^n)$  is isomorphic to the  $R$ -module

$\text{Mat}(n \times m; R)$  of  $n \times m$ -matrices over  $R$ . Hence, after

choosing bases for  $M$  and  $N$  we also have  $\text{Hom}_R(M; N) \cong$

$\text{Mat}(n \times m; R)$  with  $m = \text{rk} M$

and  $n = \text{rk} N$

(c) An  $R$ -module homomorphism  $j : M \rightarrow N$  is an isomorphism if and only if its matrix  $A \in$

$\text{Mat}(n \times m; R)$  as in (b) is invertible, i. e. if and only if there is a matrix  $A^{-1} \in \text{Mat}(n \times m; R)$

such that  $A^{-1} A = A A^{-1} = E$  is the unit matrix. As expected, whether this is the case can be

checked with determinants as follows.

(d) For a square matrix  $A \in \text{Mat}(m \times m; R)$  the determinant  $\det A$  is defined in the usual way

It has all the expected properties; in particular there is an adjoint matrix  $A^\# \in \text{Mat}(m, m; R)$  such that  $A^\# A = A A^\# = \det A \cdot E$  (namely the matrix with  $(i, j)$ -entry  $\delta_{ij} \det A$ ). With this we can see that  $A$  is invertible if and only if  $\det A$  is a unit in  $R$ :

If there is an inverse matrix  $A^{-1}$  then  $1 = \det E = \det(A^{-1} A) = \det A^{-1} \det A$ , so  $\det A$  is a unit in  $R$ .

If  $\det A$  is a unit, we see from the equation  $A A^\# = A A^\# = \det A \cdot E$  that  $(\det A)^{-1} A^\#$  is an inverse of  $A$ .

So all in all finitely generated, free modules behave very much in the same way as vector spaces. However, most modules occurring in practice will not be free — in fact, submodules and quotient modules of free modules, as well as images and kernels of homomorphisms of free modules, will in general not be free again. So let us now also find out what we can say about more general finitely generated modules.

First of all, the notion of dimension of a vector space, or rank of a free module as in Remark 3.17 (a), is then no longer defined. The following notion of the length of a module can often be used to substitute this.

**Definition (Length of modules).** Let  $M$  be an  $R$ -module.

(a) A composition series for  $M$  is a finite chain

$$0 = M_0 \subset M_1 \subset M_2 \subset \dots \subset M_n = M$$

of submodules of  $M$  that cannot be refined, i. e. such that there is no submodule  $N$  of  $M$  with  $M_i \subset N \subset M_i$  for any  $i = 1, \dots, n$ , this is equivalent to  $M_i = M_{i-1} \oplus R/\mathfrak{m}_i$  having no non-trivial submodules for all  $i$ , and to  $M_i = M_{i-1} \oplus R/\mathfrak{m}_i$  being isomorphic to  $R$  modulo some maximal ideal for all  $i$ .

The number  $n$  above will be called the length of the series.

(b) If there is a composition series for  $M$ , the shortest length of such a series is called the length of  $M$  and denoted  $\text{lr}(M)$  (in fact, we will show that then all composition series have this length). Otherwise, we set formally  $\text{lr}(M) = \infty$ .

If there is no risk of confusion about the base ring, we write  $\text{lr}(M)$  also as  $l(M)$ .

**Exercise .** Let  $M$  be an  $R$ -module of finite length, i. e. an  $R$ -module that admits a composition series. Show that:

- (a) If  $N < M$  is a proper submodule of  $M$  then  $l(N) < l(M)$ .
- (b) Every composition series for  $M$  has length  $l(M)$ .
- (c) Every chain  $0 = M_0 < M_1 < M_2 < \dots < M_n = M$  of submodules of  $M$  can be refined to a composition series for  $M$ .

Example

(a) Let  $V$  be a vector space over a field  $K$ . If  $V$  has finite dimension  $n$ , there is a chain  $0 = V_0 < V_1 < \dots < V_n = V$  of subspaces of  $V$  with  $\dim_K V_i = i$  for all  $i$ . Obviously, this chain cannot be refined. Hence it is a composition series for  $V$ , and we conclude that  $l(V) = n = \dim_K V$ .

On the other hand, if  $V$  has infinite dimension, there are chains of subspaces of  $V$  of any length. this is only possible if  $l(V) = \infty$ .

So for vector spaces over a field, the length is just the same as the dimension.

(b) There is no statement analogous to (a) for free modules over a ring: already  $Z$  has infinite length over  $Z$ , since there are chains

$$0 < (2^n) < (2^{n-1}) < \dots < (2) < Z$$

of ideals in  $Z$  of any length.

(c) Certainly, a module  $M$  of finite length must be finitely generated: otherwise there would be infinitely many elements  $(m_i)_{i \in \mathbb{N}}$  of  $M$  such that all submodules  $M_i = \langle m_1, \dots, m_i \rangle$  are distinct. But then  $0 = M_0 < M_1 < M_2 < \dots$  is an infinite chain of submodules, which by

Exercise is impossible for modules of finite length.

On the other hand, a finitely generated module need not have finite length, as we have seen in

(b). In fact, we will study the relation between the conditions of finite generation and finite length in more detail in Chapter 7.

Exercise. What are the lengths of  $Z_8$  and  $Z_{12}$  as  $Z$ -modules? Can you generalize this statement to compute the length of any quotient ring  $R/I$  as an  $R$ -module, where  $I$  is an ideal in a principal ideal domain  $R$ ?