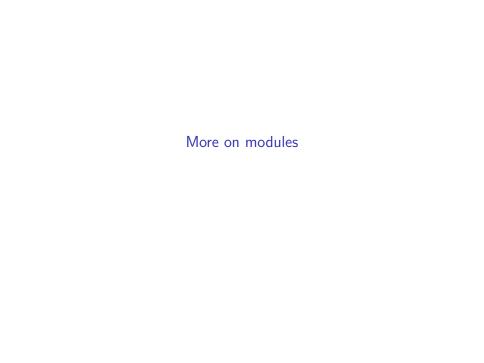
# 2. Modules (continued)



#### Sums of modules

Suppose that R is a ring and M is an R-module. Let  $N_1, \ldots, N_k$  be submodules of M. Then the sum  $N_1 + \ldots + N_k$  is the collection

$$N_1 + \ldots + N_k = \{n_1 + \cdots + n_k : n_i \in N_i\}$$

It is a submodule of M and the smallest submodule containing all the  $N_i$ .

One can also consider infinite collections of submodules:

$$\sum_{i\in I} N_i = \{\sum_{j\in J} n_j : n_j \in N_j, \ J \subset I \ \mathrm{finite} \ \}$$

# Generating submodules (compare vector spaces)

Suppose  $A \subset M$ . Then the submodule RA of M generated by A is the smallest submodule of M containing A. In practice it is the collection

$$RA = \{r_1 a_1 + \dots + r_k a_k : r_1, \dots, r_k \in R, a_1, \dots, a_k \in A, k \in \mathbb{Z}, k \ge 0\}$$

In linear algebra, we would say that RA is the submodule of M that is spanned by A and this terminology can be used here as well.

We can also say that RA is the set of (finite) R-linear combinations of elements of A.

# Generating sets - an example

Suppose that V is a  $\mathbb{Q}$ -vector space of dimension n and  $w_1, \ldots, w_k$  are a set of vectors in V.

Since V is also a  $\mathbb{Z}$  module (by "restriction of scalars") we can consider the sub- $\mathbb{Z}$ -module of V generated by the  $w_i$ . This is all  $\mathbb{Z}$ -linear combinations of the  $w_i$ .

For example if  $V = \mathbb{Q}^2$  and  $A = \{w_1, w_2\}$  are the standard basis elements then  $\mathbb{Z}A$  is the subset of V of vectors with integer coefficients in the standard basis.

# Finite generation

**Definition:** An R-module M is finitely generated if there is a finite subset  $A \subset M$  such that RA = M.

Note that  $\mathbb Q$  is finitely generated as a  $\mathbb Q$ -module (in fact it's generated by one element) but not as a  $\mathbb Z$ -module.

For vector spaces, finitely generated means finite dimensional. A generating set is the same as a spanning set.

# Comparison with vector spaces

A set  $m_1, \ldots, m_k$  in an R-module M is linearly independent if, whenever  $\sum r_i m_i = 0$ , all  $r_i = 0$ .

For vector spaces, a maximal linearly independent set (meaning a linearly independent set which becomes dependent when any nonzero element is added to it) automatically spans the vector space, and we call this a basis.

For modules, this fails. Consider  $\mathbb{Z}^2$  and let  $e_1 = [2, 0]$  and  $e_2 = [0, 2]$ . If e = [a, b] then

$$2e - ae_1 - be_2 = 0$$

so  $e_1, e_2$  is a maximal linearly independent set. But they don't generate all of  $\mathbb{Z}^2$ .

# Cyclic modules

**Definition:** An R module M is cyclic if it is generated by one element: M = Ra for some  $a \in M$ .

- ightharpoonup Cyclic groups are cyclic  $\mathbb{Z}$ -modules.
- ▶ If R is a ring with unity and I is a left ideal, then R/I is a cyclic R-module generated by 1 + I.
- ▶ If *R* is a ring with unity, an ideal *I* is a cyclic module if and only if it is a principal ideal.
- ▶ If  $R = M_n(F)$  for a field F and  $M = F^n$  is the space of column vectors viewed as an R-module, then M is cyclic.

If  $R=\mathbb{Z}[i]$ , then (1+i)R is a cyclic module for R generated by (1+i). But if we view (1+i)R as a  $\mathbb{Z}$ -module inside the  $\mathbb{Z}$ -module  $R=\mathbb{Z}+\mathbb{Z}i$  then (1+i)R is generated over  $\mathbb{Z}$  by 1+i and (1+i)i=i-1; it is not cyclic as a  $\mathbb{Z}$ -module.

# Characterization of cyclic modules

**Proposition:** Let M be a cyclic R-module. Then M is isomorphic to R/I where I is a left ideal of R.

**Proof:** Let  $m \in M$  generate M. Consider the map  $f: R \to M$  defined by f(r) = rm. This is a module homomorphism since

$$f(r_1r_2) = r_1r_2m = r_1(r_2m) = r_1f(r_2m).$$

(Remember that we are thinking of R here as an R-module, not a ring.)

The kernel of this map is the set  $I = \{r \in R : rm = 0\}$ . This is a left ideal since if rm = 0 then srm = 0 for all  $s \in R$ . Since M is cyclic, the map f is surjective. Therefore by the isomorphism theorem M is isomorphic to R/I. ### More on cyclic modules

Recall that a module M for F[x] is the same as an F-vector space V together with a linear map  $T:V\to V$ .

If M is cyclic then there is an  $m \in M$  so that every  $m' \in M$  is given



# Direct Products (definition)

Suppose that  $M_1, \ldots, M_k$  are R modules. The direct product  $M_1 \times \cdots \times M_k$  of the  $M_i$  is the set of "vectors"  $(m_1, \ldots, m_k)$  with  $m_i \in M_i$ . Addition and multiplication by R are done componentwise.

#### Internal direct sums

Suppose that M is an R-module and  $N_1, \ldots, N_k$  are submodules of M. There is a module homomorphism

$$N_1 \times \cdots \times N_k \to N_1 + \cdots + N_k \subset M$$

defined by sending  $(n_1,\ldots,n_k) o n_1 + \cdots n_k$ .

# Internal direct sums (continued)

**Definition:** The sum map above is an isomorphism if and only if either of the following two conditions are satisfied:

- ►  $N_j \cap (N_1 + \cdots N_{j-1} + N_{j+1} + \cdots N_k) = 0$  for all  $j = 1, 2, \dots, k$
- Any  $x \in N_1 + N_2 + ... + N_k$  can be written *uniquely* as a sum  $x = n_1 + n_2 + ... + n_k$  with  $n_i \in N_i$ .

If M is isomorphic to  $N_1 \times \cdots \times N_k$  via the sum map, we say that

$$M = N_1 \oplus N_2 \oplus \cdots \oplus N_k$$

and say that M is the internal direct sum of the  $N_i$ .



#### **Definitions**

Suppose that I is a set and  $M_i$  is an R-module for each  $i \in I$ .

The direct product  $\prod_{I} M_{i}$  is the collection of all functions  $f: I \to \bigcup_{i \in I} M_{i}$  such that  $f(i) \in M_{i}$ . It is an R-module: (f+g)(i) = f(i) + g(i) and (rf)(i) = r(f(i)).

The direct sum  $\bigoplus_I M_i$  is the submodule of  $\prod_I M_i$  consistsing of functions f with the additional property that there is a finite subset  $J \subset I$  such that f(i) = 0 unless  $i \in J$ .

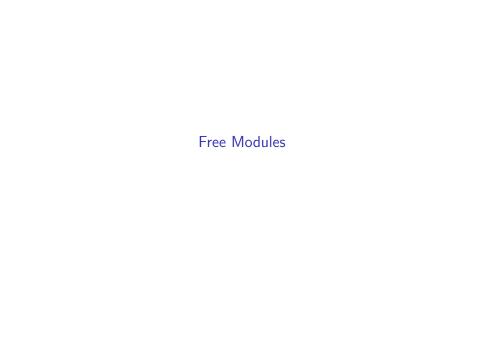
Notice that if *I* is finite then these two things are the same.

### Countable sums and products

Suppose that  $I = \mathbb{N}$ , the natural numbers, and  $M_i$  is a family of R-modules indexed by I. Then:

- ▶  $\prod_{i \in I} M_i$  consists of sequences  $(m_1, m_2, ..., m_k, ...)$  where  $m_i \in M_i$ .
- ▶  $\bigoplus_{i \in I} M_i$  consists of sequences  $(m_1, m_2, \ldots, m_k, \ldots)$  where  $m_i \in M_i$  and there is an N such that  $m_i = 0$  for all  $i \geq N$ .

Notice that, if each  $M_i$  is countable, then so is  $\bigoplus_{i \in I} M_i$ , but  $\prod_{i \in I} M_i$  is not.



#### Definition

**Definition:** A module M is *free* on a set A of generators if, for every element m of M, there are *unique*  $r_1, \ldots, r_k$  in R and  $a_1, \ldots, a_k$  in A such that

$$m = r_1 a_1 + \cdots + r_k a_k$$
.

### Examples and non-examples

If  $A = \{a_1, \dots, a_n\}$  is finite, then M is free on A if the map

$$\bigoplus_{i=1}^{n} R \to M$$

defined by  $(r_1, \ldots, r_n) \mapsto r_1 a_1 + \cdots + r_n a_n$  is an isomorphism. So basically M is free on a set A with n elements if and only if it is isomorphic to  $R^n$ .

If  $R = \mathbb{Z}$ , then  $M = \mathbb{Z}/m\mathbb{Z} \oplus \mathbb{Z}/m\mathbb{Z}$  is not free on (1,0) and (0,1). Every  $m \in M$  is a linear combination  $r_1(1,0) + r_2(0,1)$  for  $r_1, r_2 \in \mathbb{Z}$ , but  $r_1$  and  $r_2$  are not uniquely determined. In fact M is not free on any set of generators.

Any vector space over F is a free F-module.

### Mapping property

Let A be a set. There exists a module F(A), called the *free module* on A, which contains A as a subset.

It satisfies the following property.

Let M be any module and let  $f:A\to M$  be any map of sets. Then there is a unique module homomorphism  $\Phi:F(A)\to M$  such that the following diagram commutes:



# Examples of mapping property

- ▶ If V is a vector space and B is a basis, then V is free on B. A linear map from  $V \to W$  is determined by where you send B. In this situation,  $f: B \to W$  is the map of sets sending the basis of V to a subset of W, and  $\Phi$  is the resulting linear map.
- ▶ If A is any set, then F(A) is the R-module of "formal linear combinations of elements of A": the set of sums  $\sum r_i a_i$  over finite collections  $\{a_1, \ldots, a_n\}$  of elements of A.
- Alternatively it is the set of functions f : A → R that are zero for all but a finite subset of A with pointwise addition and scalar multiplication.

# Uniqueness

Any two free modules on the same set are isomorphic via the module map induced by the identity map on A.