Last time - Defined what it means for a set X in an R-module M to
- generate M
- to be linearly independent
- to be a basis (X generates M and is linearly independent)

- An R-module is cyclic iff it's generated by 1 element.
Proved M is a cyclic R-module $\iff$ $M \cong R/I$ as modules, where $I \subseteq R$ is an ideal.

Direct sums of modules

Definition Let $M_1, \ldots M_n$ be R-modules. Their [external] direct sum is the set $M_1 \times M_2 \times \cdots \times M_n = \{(m_1, \ldots m_n) \mid m_i \in M_i, i = 1, \ldots n\}$ with addition and scalar multiplication defined "coordinate-wise":

$$(m_1, \ldots m_n) + (m_1', m_2', \ldots, m_n') := (m_1 + m_1', \ldots, m_n + m_n')$$
$$r(m_1, \ldots m_n) := (rm_1, \ldots rm_n)$$

Notation $M_1 \oplus \cdots \oplus M_n$ denotes the direct sum of $M_1, \ldots M_n$.

Note There are canonical inclusions $i_j : M_j \hookrightarrow M_1 \oplus \cdots \oplus M_n$

$$i_j(m) = (0 \ldots 0, \underset{\uparrow \text{ jth slot}}{m_j}, 0 \ldots 0)$$

, which are R-module homomorphisms.

Lemma (Universal property of $M_1 \oplus \cdots \oplus M_n$).
Let L be an R-module, $\{f_j : M_j \to L\}_{j=1}^{n}$ R-module homomorphisms. Then $\exists$ unique R-module homomorphism

$$f : M_1 \oplus \cdots \oplus M_n \to L$$

so that $(f \circ i_j)(m_j) = f_j(m_j)$ $\forall j$ $\forall m_j \in M_j$.

Proof (Existence) Define $f : M_1 \oplus \cdots \oplus M_n \to L$ by

$$f(m_1, \ldots m_n) = f_1(m_1) + f_2(m_2) \ldots + f_n(m_n)$$

f is a homomorphism of R-modules.

(Uniqueness) if $h: M_1 \oplus \cdots \oplus M_n \to L$ is another homomorphism so that $h \circ i_j = f_j \quad \forall j$. Then

$$h(m_1, \ldots m_n) = h((m_1, 0 \ldots 0) + (0, m_2, \ldots 0) + \cdots + (0, \ldots 0, m_n))$$
$$= h(m_1, 0, \ldots 0) + h_2(0, m_2, 0 \ldots 0) + \cdots + h_n(0, \ldots 0, m_n)$$
$$= (h \circ i_1)(m_1) + (h \circ i_2)(m_2) + \cdots + (h \circ i_n)(m_n)$$
$$= f_1(m_1) + \cdots + f_n(m_n) = f(m_1, \ldots m_n). \qquad \square$$

<u>Proposition 32.1.</u> Let M be an R-module, $N_1, \ldots N_k \subseteq M$ R-submodules. The following are equivalent.

1) The homomorphism $f: N_1 \oplus \cdots \oplus N_k \to M$, $f(n_1, \ldots n_k) = n_1 + \cdots + n_k$ is an isomorphism.

2) $\forall m \in M \quad \exists$ unique $n_1 \in N_1, \ldots n_k \in N_k$ so that
$$m = n_1 + n_2 + \cdots + n_k.$$

3) $N_1 + \cdots + N_k = M$ and $N_j \cap (N_1 + \cdots + N_{j-1} + N_{j+1} + \cdots + N_k) = 0 \quad \forall j$.

(here and elsewhere $N_1 + \cdots + N_k = \{n_1 + \cdots + n_k \mid n_j \in N_j \ \forall j\}$; it's a submodule of M)

<u>Proof</u> ((1)⇒(2)) Suppose (1): f is an isomorphism. Then $\forall m \in M$ $\exists!$ $(n_1, \ldots n_k) \in N_1 \oplus \cdots \oplus N_k$ s.t. $m = f(n_1, \ldots n_k) = n_1 + \cdots + n_k$. Hence (2).

((2)⇒(1)) Suppose (2). Then $f: N_1 \oplus \cdots \oplus N_k \to M$ is 1-1 and onto, hence an isomorphism of R modules. Hence (1).

((1)⇒(3)) Since f is onto, $M = f(N_1 \oplus \cdots \oplus N_k) = N_1 + \cdots + N_k$.

Suppose $N_j \cap (N_1 + \cdots + N_{j-1} + N_{j+1} + \cdots + N_k) \neq 0$.

Then $\exists\, n_i \in N_i$, $i = 1, \ldots k$ s.t. $n_j = n_1 + \cdots + n_{j-1} + n_{j+1} + \cdots + n_k$

$\Rightarrow 0 = n_1 + \cdots + n_{j-1} + (-n_j) + n_{j+1} + \cdots + n_k = f(n_1, \ldots n_{j-1}, -n_j, n_{j+1}, \ldots n_k)$

Contradiction since f is 1-1 and $f(0, \ldots 0) = 0$.

((3)⇒(1)) $M = N_1 + \cdots + N_k \Rightarrow f$ is onto

$\ker f = \{(n_1, \ldots n_k) \in N_1 \oplus \cdots \oplus N_k \mid n_1 + \cdots + n_k = 0\}$.

If f is not 1-1, $\exists\, (n_1, \ldots n_k) \in N_1 \oplus \cdots \oplus N_k$, not all zero st

$n_1 + \cdots + n_k = 0$. Say $n_j \neq 0$. Then $-n_j = (n_1 + \cdots + n_{j-1} + n_{j+1} + \cdots + n_k)$

which contradicts $N_j \cap (N_1 + \cdots + N_{j-1} + N_{j+1} + \cdots + N_k) = 0$. □

Remark A module M is an internal direct sum of submodules $N_1, \ldots, N_k$ iff $\forall m \in M$ $\exists$ unique $n_1 \in N_1, \ldots, n_k \in N_k$ s.t. $m = n_1 + \cdots + n_k$.

Proposition 32.1 implies:

M is an internal direct sum of $N_1, \ldots, N_k \iff$
M is isomorphic to the external direct sum $N_1 \oplus \cdots \oplus N_k$.

From now on we won't distinguish between external and internal direct sums. □

Aside If $\{M_i\}_{i \in I}$ is a collection of R modules indexed by a set I, one can still define the direct sum $\bigoplus_{i \in I} M_i$ as follows:

$$\bigoplus_{i \in I} M_i := \{(m_i)_{i \in I} \in \prod_{i \in I} M_i \mid m_i = 0 \text{ for all but finitely many } i\text{'s}\}$$

There are injective map $i_j : M_j \to \bigoplus_{k \in I} M_k$ $\quad i_j(m) := (m_i)_{i \in I}$, $m_i = 0$ for $i \neq j$.
Then given a module L and homomorphisms $\{f_i : M_i \to L\}_{i \in I}$ there exists a unique homomorphism

$$f : \bigoplus M_i \to L \quad \text{given by}$$
$$f((m_i)_{i \in I}) = \sum_{i \in I} f_i(m_i)$$

Note that all but finitely many terms in the sum $\sum_{i \in I} f_i(m_i)$ are zero, so there is no worry about convergence.

Structure Theorem for modules over a PID (invariant factor form)

Let R be a PID, and M a finitely generated R-module. Then $\exists$ $r \in \mathbb{N}$ and $a_1, \ldots, a_n \in R$ (nonzero non units) so that

$a_1 \mid a_2$, $a_2 \mid a_3$ $\ldots$ $a_{n-1} \mid a_n$

and $M \simeq \underbrace{R \oplus \cdots \oplus R}_{r} \oplus R/(a_1) \oplus R/(a_2) \oplus \cdots \oplus R/(a_n)$

r is called the free rank of M.

Two finitely generated R-modules are isomorphic $\Leftrightarrow$ they have the same free rank and the same list of the invariant factors $a_1, \ldots a_n$ (up to associates)

It will take us some time to prove the structure theorem.

The structure theorem has another form:

Thm Structure theorem for finitely generated modules over a PID, (elementary divisor form)

Let R be a PID, M a finitely generated R-module. Then

$$M \simeq \underbrace{R \oplus \cdots \oplus R}_{r} \oplus R/\langle p_1^{e_1} \rangle \oplus \cdots \oplus R/\langle p_d^{e_d} \rangle$$

where $p_1, \ldots p_d \in R$ are irreducibles and $e_1, \ldots e_d$ pos integers.

$p_i^{e_i}$'s are called elementary divisors.

Ex $R = \mathbb{Z}$, $M = \mathbb{Z}_6$. Then $M = \mathbb{Z}/\langle 6 \rangle \simeq \mathbb{Z}/\langle 2 \rangle \oplus \mathbb{Z}/\langle 3 \rangle$

The free rank of $\mathbb{Z}_6$ is 0, 6 is the invariant factor, 2, 3 are the elementary divisors.

To show that the two versions of the structure theorem are equivalent, we'll need the Chinese remainder theorem:

Thm R commutative ring, $I_1, \ldots I_k \subseteq R$ ideals with $I_i + I_j = R$ for all $i \neq j$. Then

$$\underset{\text{product of ideals}}{R/I_1 \cdots I_k} \simeq (R/I_1) \oplus \cdots \oplus (R/I_k)$$

(as rings, hence as R-modules)