Last time: Defined modules over commutative rings.

We say: vector spaces are modules over fields.

Abelian groups are modules over \( \mathbb{Z} \).

An ideal \( I \) in a (commutative) ring \( R \) is a module over \( R \).

\( I \) is a submodule of \( R \) if every comm ring \( R \) is a module over itself.

Example: Let \( F \) be a field, \( V \) a vector space over \( F \) and \( T : V \to V \) a linear map.

We define \( T^0 = \text{id} \), \( T^n = T \circ \cdots \circ T \) for \( n > 0 \).

More generally, \( \text{Hom}(V, V) = \{ S : V \to V \mid S \text{ is linear} \} \) is a ring: the sum of two linear maps and the "multiplication" is composition.

\( \text{Hom}(V, V) \) is a non commutative ring. None the less, for each fixed \( T : \text{Hom}(V, V) \) we have a ring homomorphism \( \text{ev}_T : F[x] \to \text{Hom}(V, V) \)

\[ \text{ev}_T(a_0 + a_1 x + \cdots + a_n x^n) = a_0 \text{id} + a_1 T + \cdots + a_n T^n \]

One usually writes \( p(T) \) for \( \text{ev}_T(p) = p(T) \in F[x] \).

We now make \( V \) into an \( F[x] \) module as follows:

\[ \forall p \in F[x], \forall v \in V, \quad p \cdot v = (p(T)) \cdot v \]

That is, if \( p(x) = a_0 + a_1 x + \cdots + a_n x^n \), then \( p \cdot v = a_0 v + a_1 Tv + \cdots + a_n T^n v \).

A converse is true as well: any module \( M \) over \( F[x] \) in a vector space over \( F \) together with a linear map \( T : M \to M \) is a subring of \( F[x] \). So any \( F[x] \) module is an \( F \) module, i.e., a vector space over \( F \).

Also, \( x \in F[x] \) acts on \( M \): \( \forall m \in M \) we have \( x \cdot m \in M \).

Define \( T(m) = x \cdot m \).

Then \( \forall \lambda \in F, \forall m \in M \)

\[ \lambda \cdot (x \cdot m) = (\lambda x) \cdot m = \lambda \cdot (x \cdot m) \]

and \( x \cdot (m_1 + m_2) = x \cdot m_1 + x \cdot m_2 \), so \( T(m_1 + m_2) = T(m_1) + T(m_2) \).
For any ring $R$, $R^m = \{(a_1, \cdots, a_m) | a_i \in R\}$.

$R^m$ is an $R$-module.

$\cdot$ is defined component-wise.

$\forall r \in R, \quad r \cdot (a_1, \cdots, a_m) := (ra_1, \cdots, ra_m)$.

$R^m$ is an example of a free module over $R$ of rank $n$.

**Kernel and image**

Let $\phi : M \to N$ be a homomorphism of $R$-modules.

We define the image of $\phi$ to be $\phi(M) = \{ n \in N | \exists m \in M : \phi(m) = n \}$.

The kernel of $\phi$ is

$\ker \phi = \{ m \in M | \phi(m) = 0 \}$.

Exercise: $\ker \phi$ is a submodule of $M$.

$\phi(M)$ is a submodule of $N$.

**Lemma** Let $M$ be an $R$-module, $N \subseteq M$ an $R$ submodule.

Then the quotient abelian group $M/N$ is an $R$-module with the "action" of $R$ given by $r \cdot (x+N) = (rx)+N $ for $x+N \in M/N$.

**Proof sketch** We need to check that the action is well-defined.

So suppose $x+ N = y+N$ for some $x, y \in M$.

Then $x-y+N$. Since $N$ is a submodule of $M$.

$r \cdot (x-y) + N$. But $r \cdot (x-y) = r \cdot (x+(-1)y)$

$= r x + (r(-1)) y = r x - ry, \quad \Rightarrow \quad r x - ry + N$

$= r x + N = r y + N$.

$\therefore \ r \cdot (x+N) - (rx)+N$ is well-defined.

The rest is an easy exercise.
For example $r \cdot (x + N) + (y + N) = r \cdot (x + y + N)$

$= r(x + y) + N = (rx + N + (ry + N))$

$= r(x + N) + r(y + N)$

and so on.

**Remark.** The map $\pi : M \rightarrow M/N$, $\pi(x) = x + N$ is an $R$-module homomorphism.

**Remark.** Let $A$, $B$ be two submodules of an $R$-module $M$. Then $A \cap B$ is a submodule of $M$ (check!)

$A + B = \{a + b | a \in A, b \in B\}$ is a submodule of $M$.

**Definition.** A homomorphism $\varphi : M \rightarrow N$ of $R$-modules is an isomorphism if $\varphi$ a homomorphism $\psi : N \rightarrow M$ of $R$-modules so that $\psi \circ \varphi = \text{id}_N$, $\varphi \circ \psi = \text{id}_M$.

**Exercise.** A homomorphism $\varphi : M \rightarrow N$ of $R$-modules is an isomorphism $\iff \varphi$ is a bijection.

**Theorem 1 (Isomorphism theorem for $R$-modules).** Let $\varphi : M \rightarrow N$ be an $R$-module homomorphism. Then $\overline{\varphi} : M/\ker \varphi \rightarrow \varphi(M)$, $\overline{\varphi}(m + \ker \varphi) = \varphi(m)$ is a well-defined bijective homomorphism of $R$-modules, hence an isomorphism of $R$-modules.

**Proof.** Since $M$ and $N$ are abelian groups and $\varphi$ is a homomorphism of groups, $\overline{\varphi} : M/\ker \varphi \rightarrow \varphi(N)$ is a well-defined isomorphism of abelian groups. Moreover, $\forall x \in R$

$\forall (x + \ker \varphi) \in M/\ker \varphi$ $\overline{\varphi} \circ (r \cdot (x + \ker \varphi)) = \overline{\varphi} (r \cdot x + \ker \varphi) =$
\[ e(rx) = r(e(x)) \quad \text{since } e \text{ is an } \mathbb{R} \text{-module homomorphism} \]

\[ = r \, \overline{e}(x + \ker(e)) \]

Intersection of submodules:

Let \( M \) be an \( \mathbb{R} \)-module, \( \mathcal{N} = \{ N_x \}_{x \in M} \) a collection of submodules. Then \( \bigcap N_x \) is an abelian subgroup of \( M \). Moreover it is a \( \mathbb{R} \)-submodule:

\[ x \in N_x, \quad \forall r \in \mathbb{R}, \quad r \cdot x \in \bigcap N_x \]

Definition: Let \( M \) be an \( \mathbb{R} \)-module, and \( X \subseteq M \) a set. A submodule generated by \( X \) is

\[ \langle X \rangle = \bigcap \{ N \subseteq M \mid X \subseteq N \} \]

Example: \( \mathbb{R} = \mathbb{R} \), \( V \) a real vector space, \( X = \{ v_1, \ldots, v_k \} \)

\[ \langle X \rangle = \text{Span}_\mathbb{R} \{ v_1, \ldots, v_k \} \]

Exercise: For a set \( X \) in an \( \mathbb{R} \)-module \( M \)

\[ \langle X \rangle = \left\{ \sum_{i=1}^{n} r_i x_i \mid n \geq 0, \ x_i \in X, \ r_i \in \mathbb{R} \right\} \]

is finite linear combinations of elements of \( \mathbb{R} \).

Example: \( M \) is a \( \mathbb{Z} \)-module, i.e., an abelian group, and \( X \subseteq M \)

Then \( \langle X \rangle \) is a subgroup generated by the set \( X \).

Definition: An \( \mathbb{R} \)-module \( M \) is finitely generated if there is a finite set \( \{ x_1, \ldots, x_k \} \subseteq M \) so that

\[ M = \langle \{ x_1, \ldots, x_k \} \rangle = \left\{ \sum_{i=1}^{k} r_i x_i \mid r_i \in \mathbb{R} \right\} \]

Example: A finite abelian group is a finitely generated \( \mathbb{Z} \)-module.

\( \mathbb{Z}^2 = \mathbb{Z} \times \mathbb{Z} \) is also finitely generated \( \mathbb{Z} \)-module.