(9)

(or A-linear hom)

Suppose M, N are A-modules. An A-module hom. $\varphi: M \to N$ is a function that respects the A-module structures: I.e. $\varphi(m_1 + m_2) = \varphi(m_1) + \varphi(m_2)$ and $\varphi(a \cdot m) = a \cdot \varphi(m)$.

Given a hom. $\varphi: M \to N$, the image $\mathrm{Im}(\varphi)$ is a submodule of N, the kernel $\mathrm{Ker}(\varphi)$ is a submodule of M, and

$$M/\mathrm{Ker}(\varphi) \cong \mathrm{Im}(\varphi)$$

as A-modules.

<u>Exercise</u> Let A be a ring, $\mathfrak{a} \subset A$ an ideal, and M an A-module.

(1) Define $\mathfrak{a} \cdot M := \left\{ \begin{array}{l} \text{finite sums of elements} \\ am, \text{ for } a \in \mathfrak{a} \text{ and } \\ m \in M \end{array} \right\}$.

Show that $\mathfrak{a} \cdot M$ is an A-submod. of M.

(2) Let $\bar{A} := A/\mathfrak{a}$, the quotient ring; and $\bar{M} := M/\mathfrak{a} \cdot M$, the quotient module.

Show that $\bar{M}$ is an $\bar{A}$-module. More precisely, show that $\bar{M}$ has a unique $\bar{A}$-mod. structure s.t. the can. hom. $M \to \bar{M}$ is A-linear.

10. Let M be an abelian group, and let X be a set. By family of elements of M indexed by X we mean a function $\sigma: X \to M$. The support of σ is the set $\{x \in X \mid \sigma(x) \neq 0\}$.
We often write $\{m_x\}_{x\in X}$ instead of σ, where $m_x := \sigma(x) \in M$.

Example If $X = \mathbb{N} = \{0, 1, \dots\}$, then a family $\{m_x\}_{x\in X}$ is just a sequence.

Suppose $\{m_x\}_{x\in X}$ has finite support. Let $X' \subset X$ be a finite set containing the support. We define

$$\sum_{x\in X} m_x := \sum_{x \in X'} m_x \in M.$$

This sum does not depend on X'.

This notation is good for operations. If $\varphi: M \to N$ is an A-module hom., then $\{\varphi(m_x)\}_{x\in X}$ is a fin. supported family in N, and

$$\varphi\Big(\sum_{x\in X} m_x\Big) = \sum_{x\in X} \varphi(m_x).$$

Likewise $\quad a\cdot\Big(\sum_x m_x\Big) = \sum_x a\cdot m_x.$

If $\{m_x\}$ is any family in M, and $\{a_x\}$ is a finitely supp. family in A, then $\{a_x \cdot m_x\}_{x\in X}$ is fin. supp.
The zero family is the constant family $a_x = 0$.

Def. Let M be an A-module, and let $\{m_x\}_{x\in X}$ be a family in M. Assume the ring A is nontrivial.

(1) We say that $\{m_x\}$ generates M if for any $m \in M$ there exists a finitely supported family $\{a_x\}$ in A, s.t.

$$m = \sum_{x\in X} a_x \cdot m_x.$$

(2) We say that $\{m_x\}$ is linearly independent if the only fin. sup. family $\{a_x\}$ in A satisfying

$$\sum_{x\in X} a_x \cdot m_x = 0$$

is the zero family.

(3) We say that $\{m_x\}$ is a basis of M if it generates M and is linearly independent.

(4) M is called a free module if it has a basis.

Prop.

The family $\{m_x\}$ is a basis of M iff for any $m \in M$ there is a unique fin. supp. family $\{a_x\}$ in A s.t. $m = \sum_x a_x \cdot m_x$.

Pf. Like in linear algebra. $\square$

page 12

Exercise If $\{m_x\}_{x \in X} = \sigma$ is a basis of M, then the function $\sigma : X \to M$ is injective. (Recall that $A \neq \{0\}$.) For this reason we sometimes say that a basis of M is a subset (i.e. $\sigma(X) \subset M$) satisfying ... .

Exercise Let A be a ring, $\mathfrak{a} \subset A$ an ideal, M an A-module, and $\{m_x\}_{x \in X}$ a family in M that generates it. Show that an element $m \in M$ belongs to $\mathfrak{a} \cdot M$ iff there is a fin. supp. family $\{a_x\}$ in $\mathfrak{a}$ s.t. $m = \sum_x a_x \cdot m_x$.

13

Example Let A be a nonzero ring and X a set.
Define
$$F_{fin}(X, A) := \{ \text{finitely supported functions } \sigma : X \to A \}$$
This is an A-module, with operations
$$(\sigma + \tau)(x) := \sigma(x) + \tau(x)$$
$$(a \cdot \sigma)(x) := a \cdot \sigma(x).$$
For any $x \in X$ we have the delta function
$$\delta_x \in F_{fin}(X, A), \quad \delta_x(y) := \begin{cases} 1 & \text{if } y = x \\ 0 & \text{o.w.} \end{cases}$$
Take any $\sigma \in F_{fin}(X, A)$. Then the family $\sigma = \{\sigma(x)\}_{x \in X}$ has finite support, and it the only element of $F_{fin}(X, A)$ s.t.
$$\sigma = \sum_{x \in X} \sigma(x) \cdot \delta_x .$$
We see that $\{\delta_x\}_{x \in X}$ is a basis of $F_{fin}(X, A)$.

(14)

Theorem Let A be a nonzero ring, let M be an A-module, and let $\{m_x\}_{x\in X}$ and $\{n_y\}_{y\in Y}$ be bases of M.
Then $|X| = |Y|$.

(i.e. $\mathfrak{a} \neq A$)

Proposition Let $\mathfrak{a} \subset A$ be a proper ideal, and write $\bar{A} := A/\mathfrak{a}$, $\bar{M} := M/\mathfrak{a}\cdot M$. So $\bar{M}$ is an $\bar{A}$-module, and there is an A-linear surjection $\pi: M \to \bar{M}$. Assume $\{m_x\}_{x\in X}$ is a basis of the A-module M. Write $\bar{m}_x := \pi(m_x) \in \bar{M}$.
Then the family $\{\bar{m}_x\}_{x\in X}$ is a basis of the $\bar{A}$-module $\bar{M}$.

Pf. (below)

Pf of Thm. Choose a maximal ideal $\mathfrak{m} \subset A$. By the lemma, the families $\{\bar{m}_x\}_{x\in X}$ and $\{\bar{n}_y\}_{y\in Y}$ are both bases of the $\bar{A}$-module $\bar{M}$. But $\bar{A}$ is a field, so any two bases have the same cardinality Δ

proof of Prop.
Step 1. We show $\{\bar{m}_x\}$ generates $\bar{M}$. Take $\bar{m} \in \bar{M}$, and choose a lifting $m \in M$, i.e. $\pi(m) = \bar{m}$. There is a fin. sup. family

15 (cont.) $\{a_x\}$ in A s.t. $m = \sum_x a_x m_x$. Write $\bar{a}_x :=$ $\pi(a_x) \in \bar{A}$. Then $\{\bar{a}_x\}$ is a fin. sup. family in $\bar{A}$, and $\bar{m} = \pi(m) = \pi(\sum_x a_x m_x) = \sum_x \bar{a}_x \bar{m}_x$.

Step 2. We show that $\{\bar{m}_x\}$ is linearly independent. Suppose $\{\bar{a}_x\}$ is a fin. supp. family in $\bar{A}$ s.t. $\sum_x \bar{a}_x \bar{m}_x = 0$. For any x choose some lifting $a_x \in A$ of $\bar{a}_x$, s.t. $a_x = 0$ if $\bar{a}_x = 0$. So $\{a_x\}$ is a fin. sup family in A. Now

$$\pi\left(\sum_x a_x m_x\right) = \sum_x \bar{a}_x \bar{m}_x = 0,$$

so

$$\sum_x a_x m_x \in \mathfrak{a} \cdot M.$$

According to one of the exercises, there is a fin. supp family $\{b_x\}$ in $\mathfrak{a}$ s.t. $\sum_x a_x m_x = \sum_x b_x m_x$. Thus

$$\sum_x (a_x - b_x) \cdot m_x = 0.$$

Since $\{m_x\}$ is lin. indep., it follows that $a_x - b_x = 0$ for all x. Applying π we get

$$\bar{a}_x = \pi(a_x) = \pi(a_x - b_x) = 0.$$

$\square$

In view of the theorem, the next def. makes sense.

Def. Let M be a free module over the (nontrivial) ring. Let $\{m_x\}_{x \in X}$ be a basis of X. The **rank** of is the cardinality $|X|$.

16

Theorem Let A be a nontrivial ring, let M be an A-module, and let $\{m_x\}_{x\in X}$ be a family in M. The following conditions are equivalent.

(i) The family $\{m_x\}_{x\in X}$ is a basis of M.

(ii) (The Universal Property)

Let N be any A-module, and let $\{n_x\}_{x\in X}$ be a family in N, indexed by the same set X. Then there is a unique A-module hom.

$$\varphi : M \to N$$

s.t. $\varphi(m_x) = n_x$ for all $x \in X$.

Proof. (i) $\Rightarrow$ (ii). Take any $m \in X$, and let $\{a_x\}$ be the unique fin. sup. family in A s.t. $m = \sum_x a_x m_x$. Define $\varphi(m) := \sum_x a_x n_x \in N$. We get a function $\varphi : M \to N$. It is easy to see that φ is A-linear, and that $\varphi(m_x) = n_x$.

If $\varphi' : M \to N$ is another such hom, then for any $m \in M$, with coefficients $\{a_x\}$, we have

$$\varphi'(m) = \varphi'\Big(\sum_x a_x m_x\Big) = \sum_x a_x \cdot \varphi'(m_x) = \sum_x a_x \cdot n_x = \varphi(m).$$

Thus $\varphi' = \varphi$.

(ii) $\Rightarrow$ (i): Let N be a free A-module with basis $\{n_x\}_{x\in X}$. For example we can take $N := F_{\mathrm{fin}}(X, A)$ and $n_x := \delta_x$. Using (i) $\Rightarrow$ (ii), which we already proved, we know

(cont)

17 (cont)

that the universal property holds for $\{n_x\}$.

By the univ. property of $\{m_x\}$ (existence) there is a hom. $\varphi: M \to N$ s.t. $\varphi(m_x) = n_x$. By the univ. pr. of $\{n_x\}$ there is a hom. $\psi: N \to M$ s.t. $\psi(n_x) = m_x$.

Look at the homs. $\psi \circ \varphi, \mathbb{1}_M : M \to M$. ($\mathbb{1}_M$ is the identity.) They satisfy $(\psi \circ \varphi)(m_x) = m_x = \mathbb{1}_M(m_x)$ for all x. By the univ. pr. (uniqueness) we see that $\psi \circ \varphi = \mathbb{1}_M$. Similarly $\varphi \circ \psi = \mathbb{1}_N$. Thus φ is an isom. But then M is free with basis $\{m_x\}_{x \in X}$. $\square$