CLASS 7, FRIDAY FEBRUARY 23RD: MODULE HOMOMORPHISM AND QUOTIENTS

Definition 0.1. Let M and N be R-modules. Then an **R-module homomorphism** from M to N is a map $\varphi : M \to N$ such that

- $\varphi(m + m') = \varphi(m) + \varphi(m')$
- $\varphi(rm) = r\varphi(m)$

In addition, we define the following quantities to a module homomorphism:

- $\ker(\varphi)$ to be the set of $m \in M$ such that $\varphi(m) = 0$.
- $\operatorname{im}(\varphi)$ is the set of $n \in N$ such that there exists $m \in M$ with $\varphi(m) = n$.

In the case that $\ker(\varphi) = 0$ and $\operatorname{im}(\varphi) = N$, we call φ an isomorphism. Finally, we call the group of module homomorphisms $\operatorname{Hom}_R(M, N)$.

We can immediately say even more:

Proposition 0.2. *The set $\operatorname{Hom}_R(M, N)$ has the structure of an R-module.*

Proof. We give it the structure of an R-module as follows: We define

$$\varphi + \psi : M \to N : m \mapsto \varphi(m) + \psi(n)$$

$$r\varphi : M \to N : m \mapsto r\varphi(m)$$

One quickly verifies the axioms of a module: based on that of M and N. □

Example 0.3. There is a natural isomorphism between $\operatorname{Hom}_R(R, M)$ and M, given by $\varphi \mapsto \varphi(1)$ and $m \mapsto (\varphi : R \to M : 1 \mapsto m)$.

Example 0.4. Consider the module $\operatorname{Hom}_{\mathbb{Z}}(\mathbb{Z}/m\mathbb{Z}, \mathbb{Z}/n\mathbb{Z})$ is module isomorphic to $\mathbb{Z}/\gcd(m, n)\mathbb{Z}$. This can be seen as follows:

1) Every such map is determined by where $1 \in \mathbb{Z}/m\mathbb{Z}$ is sent in $\mathbb{Z}/n\mathbb{Z}$.
2) To be a well defined map, $m \cdot \varphi(1) = 0$, or equivalently, $n | m \cdot \varphi(1)$.
3) We note that there must exist $k \in \mathbb{Z}$ such that $kn = mx$, or equivalently, $x = \frac{kn}{m}$ (which must be an integer).
4) Two homomorphisms agree if $\frac{kn}{m} \equiv \frac{k'n}{m} \pmod{n}$.
5) Looking at the prime factorization, we can see that there are $\gcd(m, n)$ many possibilities.
6) Finally, we can create the map
$$\mathbb{Z}/\gcd(m, n)\mathbb{Z} \to \operatorname{Hom}_{\mathbb{Z}}(\mathbb{Z}/m\mathbb{Z}, \mathbb{Z}/n\mathbb{Z}) : a \mapsto (\varphi : 1 \mapsto an/\gcd(m, n))$$
7) This map has an inverse given by $\varphi \mapsto \frac{\varphi(1)\gcd(m,n)}{n} \pmod{\gcd(m, n)}$

As a special note, if m, n are relatively prime, then there exist NO non-zero Homs from $\mathbb{Z}/m\mathbb{Z}$ to $\mathbb{Z}/n\mathbb{Z}$.

Proposition 0.5. *There is a natural map $\operatorname{Hom}_R(N, P) \times \operatorname{Hom}_R(M, N) \to \operatorname{Hom}_R(M, P)$ given by composition.*

In addition, $\operatorname{End}_R(M) := \operatorname{Hom}_R(M, M)$ has a natural structure as an R-algebra.

Proof. See homework. ☐

Next up, I summarize a few results which are very similar to the case of rings.

Definition 0.6. A subset $N \subseteq M$ is called a **submodule** of M if N is a module in it's own right. That is, $rn_1 + n_2 \in N$ if $n_1, n_2 \in N$ and $r \in R$.

We can then consider M/N to be the set of cosets of N inside M. This is a R-module in it's own right.

Proposition 0.7. *Let $\varphi : M \to N$. Then $ker\varphi \subseteq M$ and $\mathrm{im}(\varphi) \subseteq N$ are submodules.*

As a result, every morphism $\varphi : M \to N$ factors through module homomorphisms

$$M \xrightarrow{q} M/\ker(\varphi) \xrightarrow{\varphi'} \mathrm{im}(\varphi) \xrightarrow{i} N$$

where q is a surjective map, φ' is an isomorphism, and i is an injection.

Proof. We can define q to be the quotient map $q(m) = m+\ker(\varphi)$, $\varphi'(m+\ker(\varphi)) = \varphi(m)$ (which is well defined!), and i to be the inclusion map of $\mathrm{im}(\varphi)$ into N. This is nearly identical to the case of rings just with one addition map. ☐

Example 0.8. We can define $\mathbb{Z} \to \mathbb{Z}/p\mathbb{Z}[x]$ as $\mathbb{Z}$-modules by sending 1 to 1 in $\mathbb{Z}/p\mathbb{Z}$. This above factorization would then be

$$\mathbb{Z} \to \mathbb{Z}/p\mathbb{Z} \cong \mathbb{Z}/p\mathbb{Z} \hookrightarrow \mathbb{Z}/p\mathbb{Z}[x].$$

Proposition 0.9. *If $N, N' \subseteq M$ are submodules, then $N + N'$ and $N \cap N'$ are also submodules.*

Proof. Exercise. ☐

Finally, this allows us to write down the module isomorphism theorems. The proofs of each are almost identical to the case of rings/groups.

Theorem 0.10. *1) The map φ' in Proposition 0.7 is an isomorphism.*

2) If $N, N' \subseteq M$ are submodules, then

$$(N + N')/N' \cong N/N \cap N'$$

3) If $N \subseteq N' \subseteq M$ are a chain of submodules, then

$$(M/N)/(N'/N) \cong M/N'$$

4) If $N \subseteq M$, then there is a natural bijection

$$\{\textit{submodules of } M \textit{ containing } N\} \leftrightarrow \{\textit{submodules of } M/N\}$$

Proof. I will only prove the first of the set of isomorphism theorems. First, I will show φ' is well defined:

$$\varphi'(m + k + \ker(\varphi)) = \varphi(m + k) = \varphi(m) + \varphi(k) = \varphi(m) = \varphi'(m + \ker(\varphi))$$

φ' is surjective by design: it is the set of objects that are $\varphi(m)$ for some $m \in M$. It is also injective: if $\varphi'(m + \ker(\varphi)) = \varphi(m) = 0$, then $m \in ker(\varphi)$. ☐