Take: Home exam

From the Chinese remainder theorem to (other basis)
6 problems given at the end of class
Wednesday, due by 12 noon Thursday
to Bert O'Neil (undergraduate office).

- No collaboration please!
- Can use Purnm it - too only quote only material done in class.

Wednesday's Class meet in 4088 EH.
The Hom functor

Let \( R \) be a commutative ring, let \( M, N \) be \( R \)-modules.

\[ \text{Hom}_R(M, N) = \{ f : M \to N \text{ homomorphisms of } R\text{-modules} \} \]

\[ (f + g)(x) := f(x) + g(x). \]

Verify: \( f + g \) is a homomorphism of \( R \)-modules.

\[ (\lambda f)(x) := \lambda(f(x)) = f(\lambda x) \]

because \( f \) is a homomorphism of \( R \)-modules.

Axioms immediately verified.
Functionality: Suppose we have a homomorphism of \( R \)-modules \( g: N_1 \rightarrow N_2 \). Then I have a canonical map (a homomorphism of \( R \)-modules)

\[
\text{Hom}_R(M, N_1) \rightarrow \text{Hom}_R(M, N_2)
\]

\[f: M \rightarrow N_1 \rightarrow (h \xrightarrow{g} N_1 \xrightarrow{f} N_2)\]

Now let \( g: M_1 \rightarrow M_2 \)

\[
\text{Hom}_R(M_1, N) \leftarrow \text{Hom}_R(M_2, N)
\]

\[\left(h \xrightarrow{g} M_1 \xrightarrow{f} N\right) \leftarrow \left(f: M_2 \rightarrow N\right)\]
The category obtained from a given category $C$ by "reversing arrows" (reverse the roles of $S$, $T$ and composition) is the opposite category $C^{op}$.

So $\text{Hom}_{C^{op}}(?, ?) : R\text{-Mod}^{op} \times R\text{-Mod} \rightarrow R\text{-Mod}$ is a functor.

Terminology: Let $C$, $D$ be categories. Then a functor $C^{op} \rightarrow D$ is the same thing as a functor $C \rightarrow D^{op}$. So we call it a contravariant functor from $C$ to $D$. By contrast, just a functor $C \rightarrow D$ is also called a covariant functor.
Exactness: let $0 \to M_1 \to M \to M_2 \to 0$
be a short exact sequence and let $N$ be an $R$-module. Then the following sequence is exact:

$$0 \to \text{Hom}_R(M_2, N) \to \text{Hom}_R(M, N) \to \text{Hom}_R(M_1, N)$$

This just means that $\text{Hom}_R(M_2, N) = \text{Ker}(\text{Hom}_R(M_1, N))$.

This is just the homomorphism theorem:

a homomorphism $M_2 \to N$ is the same thing as $M/M_1 \to N$ a homomorphism $M \to N$ which vanishes on $M_1$.
Why is $\text{Hom}_R(i_1 N)$ not necessarily onto? A homomorphism $M_1 \to N$ may not extend to a homomorphism $M_2 \to N$.

Example: $R = \mathbb{Z}$, $0 \to \mathbb{Z} \xrightarrow{2} \mathbb{Z} \to \mathbb{Z}/2\mathbb{Z} \to 0$

A homomorphism

$2\mathbb{Z} \to A$ may not extend to $\mathbb{Z}$

$2\mathbb{Z} \to \mathbb{Z}$

$m \mapsto m/2$. 
(1) **HW**: Prove that if \( 0 \rightarrow N_1 \xrightarrow{i} N \xrightarrow{j} N_2 \rightarrow 0 \) is a short exact sequence of \( R \)-modules (\( R \) commutative) and \( N \) is an \( R \)-module, then

\[
0 \rightarrow \text{Hom}_R(M, N) \xrightarrow{\text{Hom}_R(i)} \text{Hom}_R(M, N_1) \xrightarrow{\text{Hom}_R(j)} \text{Hom}_R(M, N_2) \xrightarrow{\text{Hom}_R(j)} \text{Hom}_R(M, N_1) \xrightarrow{\text{Hom}_R(i)} 0
\]

is exact.

---

(2) **HW**: Prove that if \( M, N, P \) are \( R \)-modules (\( R \) commutative) then there exists a natural isomorphism of \( R \)-modules

\[
\text{Hom}_R(M \otimes_R N, P) \cong \text{Hom}_R(M, \text{Hom}_R(N, P))
\]
$R \otimes R \otimes R \otimes \text{Mod} \to \text{R-Mod}$.

I am not covering the case when $R = F$ is a field (F-module = vector space, linear algebra).

It is covered in the book.

We do want to cover the case when $R$ is a PID.

Theorem: If $R$ is a PID then the submodule of any free $R$-module is free.
Proof: Let \( M = R(S) \) be a free \( R \)-module on a set \( S \).

Let \( N \subseteq M \) be a submodule. We consider pairs \( (I, f) \) where \( \tilde{f} : \tilde{I} \rightarrow R(S) \) is \( R(I) \cap N \), such that \( R(I) \cap N \) is a free \( R \)-module on \( f(I) \).

A partial ordering: \( (I, f) \leq (J, g) \) if \( I \subseteq J \) and \( g \mid I' \leq f \).

In particular, totally ordered.

If we have a well ordered subset \( W \) of \( P \) then

\( \left( U \mid (I, f) \in W \right), \ U \left\{ \tilde{I} \mid (I, f) \in W \right\} \in P. \)
So by Zorn's lemma, $P$ has a maximal element.

$(I, f) \quad I \subseteq S, \quad f : I \to R(I) \cap N$ and

that $R(I) \cap N$ is free on $f(I), I \subseteq I$.

If $R(I) \cap N = N$ (i.e. $N \subseteq R(I)$) then we are done (because then $N$ is free). Suppose $R(I) \cap N \neq N$.

Then there must exist $s_1, \ldots, s_r \in S \setminus I$ such that $R(I + s_1, \ldots, s_r) \cap N \neq R(I) \cap N$ (since every element of $N$ is an $R$-valued linear combination of finitely many elements of $S$).
Choose such $s_i$'s with $r$ minimal possible.

Let

$$z = a_1 s_1 + \cdots + a_r s_r + x \in \mathbb{N}$$

(*)

for some $x \in R(I)$,

$$a_i \neq 0 \text{ for some } i.$$ 

and

$$t = b_1 s_1 + \cdots + b_r s_r + y \in \mathbb{N}$$

for some $y \in R(I)$,

$$b_i \neq 0 \text{ for some } i.$$ 

Then, by minimality of $r$, $a_i b_i \neq 0$ for all $i$, and

Furthermore, the vectors

$$(a_1, \ldots, a_r) \in R \{ s_1, \ldots, s_r \}$$

$$(b_1, \ldots, b_r) \in R \{ s_1, \ldots, s_r \}$$

are $Q$-multiples of each other, where $Q$ is the field of
fractions of \( R \) (otherwise, \( b \cdot x - a \cdot t \) would have the same property, contradicting the minimality of \( r \)). Therefore, by taking \( R \)-valued linear combinations, we may find an element \( z \) for which \( a_r \) is the gcd of all the coefficients at \( s_r \) of elements satisfying \((*)\). It follows that \( f(I') \cup \{2\} \) is a basis of \( R(I \cup \{s_1, \ldots, s_r\}) \cap N \), so putting \( J = I \cup \{s_1, \ldots, s_r\} \), \( J' = I' \cup \{s_r\} \), \( g(x) = f(x) \) for \( x \in I' \), \( g(s_r) = t \), we have
\[
(J, g) \neq (I, f),
\]
Contradicting maximality. 

HW: See lecture above (2 problems).