MATH110BH Homework 6

Boran Erol

February 2024

1 Problem 1

Lemma 1.1. Let M be a cyclic (left) R-module. Then, there is an (left)-ideal I of R such that $M \cong R/I$.

Proof. Let M be a cyclic (left) R-module. By lecture, there is a submodule N of R such that $M \cong R/N$. Since every submodule of R is an ideal of R, we conclude the proof. $\square$

2 Problem 2

Lemma 2.1. Let R be a commutative ring and M, N be R-modules. Then, $Hom_R(M, N)$ is an R-module.

Proof. Let's first show that $Hom_R(M, N)$ is an Abelian group using addition of functions. Let $f, g \in Hom_R(M, N)$ and $x, y \in M$. It suffices to show that $f + g$ is a module homomorphism from M to N. Then, $(f+g)(x+y) = f(x+y)+g(x+y) = f(x)+f(y)+g(x)+g(y) = f(x)+g(x)+f(y)+g(y) = (f+g)(x)+(f+g)(y)$. Let $a \in R$ and $x \in M$. Then, $a(f+g)(x) = a(f(x)+g(x)) = af(x)+ag(x) = f(ax)+g(ax) = (f+g)(ax)$. The fact that it's Abelian follows immediately from the commutativity of R.

Let's now prove that $Hom_R(M, N)$ is an R-module.

Let $r \in R$, $f, g \in Hom_R(M, N)$ and $x \in M$. Then, $r(f+g)(x) = r(f(x)+g(x)) = rf(x)+rg(x)$, where the last equality holds because N is an R-module.

Let $r, s \in R$, $f \in Hom_R(M, N)$ and $x \in M$. Then, $(r+s) \cdot f(x) = rf(x) + sf(x)$, again because N is an R-module.

Similarly, $(rs)f = r(sf)$ and $1 \cdot f = f$ follows from the fact that N is an R-module. $\square$

3 Problem 3

Lemma 3.1. Let M be a (left) R-module and N be a submodule of M. If N and M/N are finitely generated, M is finitely generated.

Proof. Let $\{a_1, a_2, ..., a_n\}$ be a generating set for N and $\{b_1, b_2, ..., b_n\}$ be a generating set for M/N. Let f be the canonical surjective module homomorphism from M to M/N. Since f is surjective, for every non-zero $\hat{x} \in M/N$, there exists $x \in M$ such that $f(x) = \hat{x}$. For every b_i, pick some c_i such that $f(c_i) = b_i$. We'll prove that $\{a_1, a_2, ..., a_n, c_1, c_2, ..., c_m\}$ is a generating set for M. Let $x \in M$. We have the following two cases:

Case 1: $x \in N$. Then, $x = r_1a_1 + r_2a_2 + ... + r_na_n$ for some $r_1, r_2, ..., r_n$ in R.

Case 2: $x \in M - N$. Then, $\hat{x}$ is non-zero in M/N, so there are $r_{n+1}, r_{n+2}, ..., r_{m+n}$ such that $\hat{x} = r_{n+1}b_1 + ..., +r_{m+n}b_m$. Pulling back using f, we have that $x = r_{n+1}c_1 + ... + r_{n+m}c_m$. $\square$

4 Problem 4

Lemma 4.1. Let M be a left R-module. Then, $Hom_R(R, M)$ and M are isomorphic as groups.

Proof. First of all, notice that setting $f(1) = x$ for any $x \in M$ fully determines f since $f(r) = rf(1) = rx$ by module axioms.

Recall from Problem 3 that $Hom_R(R, M)$ is an Abelian group using addition of functions. Consider the following map $\phi : Hom_R(R, M) \to M$ defined by $f \mapsto f(1)$. Clearly, $x \mapsto f$ s.t. $f(1) = x$ is an inverse map. Clearly, ϕ is surjective. We thus conclude the proof. □

5 Problem 5

Lemma 5.1. Let $f : R^n \to R^m$ be a right R-module homomorphism. Then, there exists a unique matrix $A \in M_{mxn}(R)$ such that $f(x) = A \cdot x$.

Proof. Consider the standard bases for R^n and R^m. Notice that $f(x) = x_1 f(e_1) + ... + x_n f(e_n)$ since f is a module homomorphism. Let A be such that the ith column of A is the column vector $f(e_i)$. Notice that $A \cdot x = x_1 f(e_1) + ... + x_n f(e_n)$, so $f(x) = A \cdot x$. A is unique because the columns of A are fully determined by $f(e_i)$. □

6 Problem 6

Lemma 6.1. Let R be a commutative ring and $I \subsetneq R$ be an ideal. If I is a free R-module, I is principal.

Proof. Let β be a finite basis for I. Assume by contradiction that β has at least two elements. Let $s_1, s_2 \in \beta$. Then, $s_2 s_1 - s_1 s_2 = 0$, which contradicts the linear independence of β. We thus conclude the proof. □

7 Problem 7

Lemma 7.1. $\mathbb{Q}$ is not a free $\mathbb{Z}$-module.

Proof. Recall from a previous homework exercise that the rational numbers can only be generated using infinitely many elements.

Assume by contradiction that there's some basis $\{q_1, q_2, ...,\}$ for $\mathbb{Q}$. Without loss of generality, we can take all q_i to be positive and in simplified form.

We'll now prove that any set containing two rational number is independent, reaching a contradiction. Let $q_1 = \frac{a_1}{b_1}$ and $q_2 = \frac{a_2}{b_2}$. Notice that $b_1 a_2 \cdot q_1 + -b_2 a_1 \cdot q_2 = 0$. We therefore conclude the proof.

□

8 Problem 8

Lemma 8.1. Every free finitely generated R-module has a finite basis.

Proof. Let M be a free finitely generated R-module. Let $x_1, ..., x_n$ be a generating set for M and β be a (possibly infinite) basis for M.

Since β is generating, every x_i can be written as a finite combination of elements in β. Then, putting all of these elements together, we get a finite set such that the span of this set includes $x_1, ..., x_n$. This set is independent since it's a subset of β and generating, so we conclude the proof. □

9 Problem 9

Let M be a (left) R-module and $I \subsetneq R$ be an ideal of R. Let IM be the submodule generated by products of the form sx for all $s \in I$ and $x \in M$.

Lemma 9.1. Assume $IM = 0$. Then, M admits the structure of an R/I-module.

Proof. Let $x \in M$ and $s \in R - I$. Define $(s + I) \cdot x = s \cdot x$.

Let's first show that this is well-defined. Let $r, s \in R$ such that $r \neq s$ and $r + I = s + I$. Then, $r - s \in I \implies (r - s) \cdot x = 0 \implies r \cdot x = s \cdot x$.

Let's now show that the four module axioms hold.

Since I is not a unit ideal, $1 \notin I$. Then,$\forall x \in M : (1 + I) \cdot x = x$.

Let $r, s \in R - I$ and $x \in M$. Then, $((r+I)(s+I))(x) = (rs+I) \cdot x = (rs) \cdot x = r \cdot (s \cdot x) = (r+I)((s+I) \cdot x)$.

Let $r \in R - I$ and $x, y \in M$. Then, $(r + I)(x + y) = r \cdot (x + y) = r \cdot x + r \cdot y = (r + I) \cdot x + (r + I) \cdot y$.

Let $r, s \in R - I$ and $x \in M$. Then, $(r + I + s + I) \cdot x = (r + s + I) \cdot x = (r + s) \cdot x = r \cdot x + s \cdot x = (r + I) \cdot x + (s + I) \cdot x$. □

Lemma 9.2. M/IM admits the structure of a (left) module over the factor ring R/I.

Proof. Since M/IM is an R-module, M/IM is an additive Abelian group.

We define $(r + I) \cdot (x + IM) = rx + IM$. Let's first show that this is well-defined. Let $r, s \in R$ such that $r \neq s$ and $r + I = s + I$ and $x, y \in M$ such that $x \neq y$ and $x + IM = y + IM$. Then, $r - s \in I$ and $x - y \in IM$.

Then, $(r - s)x \in IM$, so $(r + I) \cdot (x + IM) = (s + I) \cdot (x + IM)$.

Similarly, $r(x - y) \in IM$, so $(r + I) \cdot (x + IM) = (r + I) \cdot (y + IM)$.

Let's now show that the four module axioms hold.

As in the previous lemma, $1 + I$ is the identity element.

Let $r, s \in R$ and $x \in M$. Then,

$$((r + I)(s + I)) \cdot (x + IM) = (rs + I) \cdot x = (rs) \cdot x = r \cdot (s \cdot x) = (r + I) \cdot ((s + I) \cdot (x + IM)$$

$$((r+I)+(s+I)) \cdot (x+IM) = (r+s+I) \cdot x = (r+s) \cdot x = r \cdot x+s \cdot x = (r+I) \cdot (x+IM)+(s+I) \cdot (x+IM)$$

Lastly, let $r \in R$ and $x, y \in M$. Then,

$$(r + I) \cdot (x + IM + y + IM) = r \cdot (x + y) = r \cdot x + r \cdot y = (r + I) \cdot (x + IM) + (r + I) \cdot (y + IM)$$

□

Lemma 9.3. Let M be a free R-module. Then, M/IM is a free R/I-module.

Proof. Let S be a basis for M. We'll prove that $\hat{S} = \{s + IM : s \in S\}$ is a basis for M/IM.

Let $x \in M$. Then, there exists $r_1, ..., r_n$ and $s_1, ..., s_n$ such that

$$x = r_1 s_1 + ... + r_n s_n$$

Then,

$$x + IM = (r_1 + I) \cdot (s_1 + IM) + ... + (r_n + I) \cdot (s_n + IM)$$

Thus, $\hat{S}$ generates M/IM. Now, let $r_1, ..., r_n \in R$ and $s_1, ..., s_n \in S$ such that

$$(r_1 + I) \cdot (s_1 + IM) + ... + (r_n + I) \cdot (s_n + IM) = 0$$

Then,

$$r_1 s_1 + ... + r_n s_n = 0$$

By the linear independence of S, $r_i = 0$ for all i. Thus, $\hat{S}$ is also independent. □

Lemma 9.4. Let R be a nonzero commutative ring. If $R^n \cong R^m$, $n = m$.

Proof. Let R be a non-zero commutative ring and I be a maximal ideal of R. Then, R/I is a field. Since $R^n \cong R^m$, $IR^n \cong IR^m$ by using the existing isomorphism. Then, $R^n/IR^n \cong R^m/IR^m$. Notice that these are modules over R/I, so they're isomorphic vector spaces. R^n/IR^n has a basis of n elements and R^m/IR^m has a basis of m elements. Since isomorphic vector spaces have the same dimension, $n = m$. □

10 Problem 10

Lemma 10.1. Let A be an Abelian group and $f \in End(A)$. A admits a $Z[x]$-module structure with $x \cdot a = f(a)$.

Proof. We check all four properties of modules.

A is an Abelian group by assumption, so the first condition is trivially satisfied.

For constant polynomials $f(x) = b$ for some $b \in \mathbb{Z}$ define $f \cdot a = ba$. Then, define $x \cdot a = f(a)$. Since $End(A)$ is a ring, any polynomial in $Z[x]$ is an endomorphism (since it's a composition and addition of f).

This immediately produces $\forall a \in A : f \cdot a = a$ where f is the map that's 1 everywhere.

Let $f \in End(A)$ and $x, y \in A$. Since f is a group homomorphism, $f(x + y) = f(x) + f(y)$.

Let $f, g \in End(A)$ and $a \in A$. Since $End(A)$ is an additive Abelian group, $(f + g)(a) = f(a) + g(a)$.

Let $f, g \in End(A)$ and $a \in A$. By the associativity of composition, $(fg)(a) = f(g(a))$.

We have thus satisfied all properties of a module. □