MATH110BH Homework 8

Boran Erol

March 2024

1 Problem 1

Lemma 1.1. Let F be a free (left) R-module with basis $\{x_1, x_2, ..., x_n\}$ and let M be an R-module. Then, for all $m_1, ..., m_n \in M$ there is a unique R-module homomorphism $f : F \to M$ such that $f(x_i) = m_i$.

Proof. Our homomorphism will be defined as follows. For every $s \in F$, we'll express s as an R-linear combination of $\{x_1, x_2, ..., x_n\}$ uniquely as

$$s = a_1x_1 + a_nx_n$$

Then, we'll let $f(s) = a_1m_1 + ... + a_nm_n$. Let's first prove that this is a module homomorphism.

Let $s, t \in F$ and $r \in R$. Then, there's unique $a_1, ..., a_n, b_1, ...b_n$ such that

$$s = a_1x_1 + a_nx_n$$

and

$$t = b_1x_1 + b_nx_n$$

Then,

$$f(s + rt) = f(a_1x_1 + ... + a_nx_n + rb_1x_1 + ... + rb_nx_n)$$

$$= (a_1 + rb_1)m_1 + ... + (a_n + rb_n)m_n = a_1m_1 + ... + a_nm_n + r(b_1m_1 + ... + b_nm_n) = f(s) + rf(t)$$

Notice that uniqueness immediately follows by the properties of a module homomorphism. More formally, let $g : F \to M$ such that $g(x_i) = m_i$. Then, for any $s \in M$, we have that

$$g(s) = g(a_1x_1 + ... + a_nx_n) = a_1m_1 + ... + a_nm_n = f(s)$$

We thus conclude the proof. □

Notice that the proof above goes through with minor modifications when we consider infinite bases.

2 Problem 2

Lemma 2.1. Let $f : M \to N$ be a surjective homomorphism of (left) R-modules. If N is free, there's a homomorphism of (left) R-modules $g : N \to M$ such that $f \circ g$ is the identity of N.

Proof. Let S be a (possibly infinite) basis for N with an index set I. Then, for every $n_i \in S$, there's some $m_i \in M$ such that $g(m_i) = n_i$. From Problem 1, we get a module homomorphism $f : N \to M$ such that $f(n_i) = m_i$. Then, clearly, $f \circ g$ is the identity on N. □

3 Problem 3

Lemma 3.1. *Let f be a linear operator in a vector space V over $\mathbb{R}$ such that $\forall v \in V : f(f(v)) = -v$. V has the structure of a vector space over $\mathbb{C}$ such that $\forall v \in V : f(v) = iv$.*

There are many ways to solve this. Let's first sketch the most straightforward way.

Proof. Define $\mathbb{C} \times V \to V$ by $(a + bi, v) \mapsto av + bf(v)$. Clearly, this agrees with the structure of V over $\mathbb{R}$. We can now check the module axioms. ... □

Let's now prove it using a more elegant strategy.

Proof. Recall that linear operators f on a vector space are in bijection with $F[x]$-modules over V where $x \cdot v = f(v)$. Then, there's a ring isomorphism from $\mathbb{R}[x]$ to the $\mathbb{Z}$-module endomorphisms of V. Since $f^2 + 1 = 0$, the ring homomorphism preserves its structure and gives a ring homomorphism from $\mathbb{R}[x]/(x^2 + 1)$ to the $\mathbb{Z}$-module endomorphisms of V. Since $\mathbb{R}[x]/(x^2 + 1) \cong \mathbb{C}$, V is a complex vector space. $f^2 + 1 = 0$ immediately produces $f = \pm i$. □

4 Problem 4

Lemma 4.1. *Let R be a PID and M be an R-module. M is cyclic if and only if $M \cong R/(a)$ for some $a \in R$.*

Proof. Assume M is cyclic. Then, there's some $x \in M$ such that x generates M. Consider the module homomorphism $\phi_x : R \to M$ given by $\phi(r) = rx$. Since x generates M, ϕ is surjective. Since R is a PID, $ker(\phi_x) = (a)$ for some $a \in R$.

Then, by the first isomorphism theorem for modules, $M \cong R/(a)$.

For the converse, notice that a is a generator for the module $R/(a)$. □

Corollary 4.1.1. *Let R be a PID and M be a cyclic R-module. Then, every submodule of M is also cyclic.*

Proof. Let M be a cyclic module over a PID R. Then, $M \cong R/aR$ for some $a \in R$. Let N be a submodule of M. Then, N is an ideal of R/aR. Recall that every ideal in the ring R/aR corresponds to an ideal in the ring R that contains aR. Since R is a PID, every ideal in R/aR is also principal. Then, there's a single element that generates N. □

5 Problem 5

Lemma 5.1. *Let a, b be nonzero elements of a PID R. Let $d = gcd(a, b)$ and $c = lcm(a, b)$, where c, d are unique modulo multiplication by a unit. Then*

$$R/aR \oplus R/bR \cong R/cR \oplus R/dR$$

Proof. Let $a = p_1^{\alpha_1} ... p_n^{\alpha_n}$ and $b = p_1^{\beta_1} ... p_n^{\beta_n}$ be prime factorizations of a and b, where $\alpha_i, \beta_i \geq 0$ and $p_i \neq p_j$. Let $\gamma_i = \max\{\alpha_i, \beta_i\}$ and $\delta_i = \min\{\alpha_i, \beta_i\}$. Notice that $\gamma_i = \alpha_i \wedge \delta_i = \beta_i$ or $\gamma_i = \beta i \wedge \delta_i = \alpha i$. Then, by CRT, the elementary divisors of these two modules are equivalent, so these two modules are also equivalent. □

6 Problem 6

Lemma 6.1. *Let M be a finitely generated torsion module over a PID R and let $n = |IF(M)|$. M can be generated by n elements and can't be generated by less than n elements.*

Proof. Let M be a finitely generated torsion module over a PID R and let $n = |IF(M)|$. Then,

$$M \cong R/d_1R \oplus ...R/d_nR$$

for some $d_i \in R$ such that $d_i \mid d_{i+1}$. Notice that the set $\{e_1, ..., e_n\}$ generates the right hand side.

We'll now prove that M can't be generated by $n-1$ elements. Assume by contradiction that M can be generated using $m < n$ elements. Then, $M \cong R^m/N$ where N is a submodule of R^m. However, this immediately implies that M has at most m invariant factors, which is a contradiction. □

7 Problem 7

Definition 1. A module is called **indecomposable** if it can't be expressed as a direct sum of its submodules.

Lemma 7.1. Let M be a finitely generated module over a PID R.

M is indecomposable if and only if $M \cong R$ or $M \cong R/P^n$.

Proof. Let M be a finitely generated module over a PID R. Then,

$$M \cong R/d_1R \oplus ...R/d_nR \oplus R^s$$

for some $n, s \geq 0$.

Assume M is decomposable. Then, clearly $s \leq 1$. If $s = 1$, $n = 0$ so $M \cong R$. If $s = 0$, $M \cong R/d_1R$. Then, the prime decomposition of d_1 can't have two primes, since this contradicts the indecomposability of M. Then, $M \cong R/p^mR$ for some prime p and $m \geq 0$. By the uniqueness of the elementary divisor form, it follows that M is decomposable, since otherwise the elementary divisor form wouldn't be unique.

Now, assume $M \cong R$ or $M \cong R/p^nR$. Both these groups are cyclic. Thus, they can't be the direct product of their submodules, since that would imply that they aren't cyclic by Problem 6, which is a contradiction. □

8 Problem 8

Lemma 8.1. Let A be an additive Abelian group with $nA = 0$ for some n. Then, A is a $\mathbb{Z}/n\mathbb{Z}$ module.

Proof. We'll define $k \cdot a = ka$ for any $k \in \mathbb{Z}/n\mathbb{Z}$. This is independent of the representative of the equivalence class since $n \cdot a = na = 0$. Let's now check the four axioms of a module. The existence of the identity element is immediate since $\forall a \in A : 1 \cdot a = a$.

Let $k \in \mathbb{Z}/n\mathbb{Z}$ and $a, b \in A$. Then,

$$k \cdot (a + b) = k(a + b) = ka + kb = k \cdot a + k \cdot b$$

Let $k, m \in \mathbb{Z}/n\mathbb{Z}$ and $a \in A$. Then,

$$(k + m) \cdot a = (k + m)a = ka + ma = (k \cdot a) + (m \cdot a)$$

Associativity is trivial. □

9 Problem 9

Let G be a $\mathbb{Z}/n\mathbb{Z}$-module. Then, G is an Abelian group since it's also a $\mathbb{Z}$ module. Let $a \in G$. Then, $na = 0$, so the order of a is n. Thus, every element of G has an order m such that $m \mid n$.

10 Problem 10

Lemma 10.1. Let M be a subgroup of a free Abelian group F of finite rank. Assume that for all prime integers p, $M \cap pF = pM$. Then, F/M is free.

Here's an illuminating false attempt:

Since F is a free Abelian group of finite rank, $F \cong \mathbb{Z}^s$. Since M is a submodule of a module over a PID, $M \cong \mathbb{Z}^m$ for some $m \leq s$. Thus, $F/M \cong \mathbb{Z}^{s-m}$ and is free.

This is clearly false, since letting $F = \mathbb{Z}$ and $M = 2\mathbb{Z}$ produces a contradiction. The mistake comes at the last step: it's not important that $M \cong \mathbb{Z}$, what matters for F/M to be free is the inclusion of M into F. Therefore, we can't work with modules isomorphic to M, we have to work directly with M.

Proof. We'll prove that there's no p^n torsion element in F/M for any prime p and $n > 0$ by inducting on n. By considering elementary divisor form, this is a sufficient argument. Let $f + M \in F/M$. Let p be a prime such that $p(f + M) = 0$. Then, $pf \in M$. Since $pf \in pF$, it's also in pM by assumption. Then, $f \in M$. Therefore, $f + M = 0$. Now, assume that there are no p^n torsion element in F/M for some n. Let $f + M \in F/M$ such that $p^{n+1}(f + M) = 0$. Then, $p^n f \in M$. By the inductive assumption, $f \in M$.

We thus conclude the proof. $\square$

We can also do a third proof by considering module homomorphisms from $\mathbb{Z}^n$ into F such that the image is M. This proof is in Notability.