Midterm solutions

Quick questions

Problem 1. Let R be a ring, M be an R-module, and N be a submodule of M. Describe the submodules of M/N according to the Lattice Isomorphism Theorem.

Solution. The R-submodules of M/N are of the form L/N, where L can be any submodule of M that contains N.

Problem 2. What does the Classification of finitely generated modules over a PID say? State either one of the two theorems we gave this name to.

Solution. See Theorems 3.22 and 3.27 in the class notes.

Problem 3. For each of the following, give an example or briefly explain why one doesn't exist:

a) A ring R and an R-module M such that $\operatorname{ann}(M) = 0$ but M is not free (both R and M).

Solution. $R = \mathbb{Z}$ and $M = \mathbb{Z} \oplus \mathbb{Z}/(2)$.

b) A 3×3 matrix A with entries in $\mathbb{Z}$ that presents a 2-generated $\mathbb{Z}$-module M (both A and M).

Solution. $A = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{bmatrix}$ and $M = \mathbb{Z}^2$.

Problem set questions

Problem 4. Show that a left R-module M is cyclic if and only if $M \cong R/I$ for some left ideal I.

Solution. See Problem Set 1.

Problem 5. Let R be a commutative ring with $1 \neq 0$. Show that if every R-module is free then R is a field.

Solution. See Problem Set 3.

Problem 6. Show that $\mathbb{Q}$ is not a free $\mathbb{Z}$-module.

Solution. See Problem Set 3.

Old qualifying exam questions

Problem 7. Let R be a domain. We say that a subset S of an R-module M is **maximally linearly independent** if it is linearly independent and every subset T of M properly containing S is not linearly independent. Recall that we say a module M is **torsion** if for every $m \in M$ there exists a nonzero $r \in R$ such that $rm = 0$.

a) Let S be a linearly independent set of M and let N be the submodule generated by S. Show that S is maximally linearly independent if and only if M/N is torsion.

b) Suppose that for every R-module M, every maximally linearly independent set of M generates M. Show that R must be a field.

Proof. a) Suppose that S is maximally linearly independent, and let $m + N \in M/N$ be a nonzero element. Thus $m \notin N$, and in particular $m \notin S$. Since S is maximally linearly independent, $S \cup \{m\}$ is linearly dependent, so we can find $r, c_1, \ldots, c_n \in R$ not all zero and $s_1, \ldots, s_n \in S$ such that $rm + c_1 s_1 + \cdots + c_n s_n = 0$. If $r = 0$, then we have found an equation of linear dependence for elements of S, contradicting our assumption that S is linearly independent. Thus $r \neq 0$. Now we have $rm = -(c_1 s_1 + \cdots + c_n s_n) \in N$, so $r(m + N) = rm + N = 0$ and $m + N$ must thus be a torsion element.

Suppose that M/N is torsion, and let $T \supsetneq S$. Consider any $t \in T$ with $t \notin S$. Since $t + N$ is torsion, we can find $r \in R$, $r \neq 0$ such that $r(t + N) = 0$, so $rt \in N$. Thus we can find $s_1, \ldots, s_n \in S$ and $c_1, \ldots, c_n \in R$ such that

$$rt = c_1 s_1 + \cdots + c_n s_n \implies rt + \sum_{i=1}^{n} (-c_n) s_n = 0.$$

Since $r \neq 0$, we conclude that $\{t, s_1, \ldots, s_n\}$ is linearly dependent, and thus T is linearly dependent. Finally, this shows that S is maximally linearly independent.

b) Let $r \in R$ be nonzero. For any $s \in R$, if $sr = 0$ then $s = 0$, since R is a domain. Therefore, $\{r\}$ is linearly independent. On the other hand, given any subset T of R such that $T \supsetneq \{r\}$, there exists some $s \neq r$ in T, and $sr + (-r)s = 0$. Therefore, T is linearly dependent. Thus $\{r\}$ is maximally linearly independent, and by hypothesis this implies that $\{r\}$ generates R. Thus $Rr = R$, and in particular r is invertible. We conclude that R is a field. $\square$

Problem 8. Let R be a commutative ring with $1 \neq 0$. Let $f \colon R^a \to R^b$ be a surjective R-module homomorphism. Show that $a \geqslant b$.

Solution. See Problem Set 4.

New problems

Problem 9. Let R be a commutative ring and let I and J be ideals of R. Show that if $R/I \cong R/J$ then $I = J$.

Proof. First, we claim that for any ideal I we have $\operatorname{ann}(R/I) = I$:

($\supseteq$) If $b \in I$ then $b(a + I) = ba + I = 0 + I$ for any $a \in R$, so $I \subseteq \operatorname{ann}(R/I)$.

($\subseteq$) If $b \in \operatorname{ann}(R/I)$, then $b + I = b(1 + I) = 0$, so $b \in I$.

Now suppose that R/I and R/J are isomorphic. We showed in a problem set that annihilators are preserved by isomorphisms: if $M \cong N$, then $\operatorname{ann}(M) = \operatorname{ann}(N)$, so $\operatorname{ann}(R/I) = \operatorname{ann}(R/J)$. Therefore, $I = \operatorname{ann}(R/I) = \operatorname{ann}(R/J) = J$. $\square$

Problem 10. Let V be a finite dimensional vector space over a field F and let $t : V \to V$ be a linear transformation. Prove that the following are equivalent:

(1) t is injective,

(2) t is surjective,

(3) for any basis B of V, $t(B)$ is a basis of V.

Proof. For any vector space W, we have $\dim(W) = 0 \iff W = 0$. Moreover, if W is a subspace of V, then any basis of W can be extended to a basis for V, so $\dim(W) = n \iff W = V$.

By the Rank-Nulity Theorem, $\dim(\ker(t)) + \dim(\operatorname{im}(t)) = \dim(V)$. Thus

$$\begin{aligned} f \text{ is injective} &\iff \ker(t) = 0 \\ &\iff \dim(\ker(t)) = 0 \\ &\iff \dim(\operatorname{im}(t)) = \dim(V) \\ &\iff \operatorname{im}(t) = V \\ &\iff f \text{ is surjective.} \end{aligned}$$

This shows (1) $\iff$ (2). In particular, notice that (1) and (2) are thus equivalent to t being an isomorphism. So it remains to show that t is an isomorphism if and only if for any basis B of V, $t(B)$ is a basis of V.

($\Longleftarrow$) Let $B = \{b_1, \ldots, b_n\}$ be a basis for V, and suppose that $t(B)$ is a basis for V. Since B has n elements, $t(B)$ has n elements, so $\operatorname{im}(t)$ has dimension at least n. But $\operatorname{im}(t)$ is a subspace of V and any basis of $\operatorname{im}(t)$ can be extended to a basis of V, so we conclude that $\operatorname{im}(t) = V$, and t is surjective. We have already shown this implies t is also injective.

($\Longrightarrow$) Suppose t is an isomorphism, and let $B = \{b_1, \ldots, b_n\}$ be a basis of V.

• $t(B)$ **spans** V: take any $v \in V$. Then we can find $w \in V$ such that $t(w) = v$, since t is surjective, and thus there exist $c_1, \ldots, c_n$ such that $c_1 b_1 + \cdots + c_n b_n = w$. Thus

$$c_1 t(b_1) + \cdots + c_n t(b_n) = t(c_1 b_1 + \cdots + c_n b_n) = t(w) = v,$$

and $t(V)$ spans B.

• $t(B)$ **is linearly independent**: Let $c_1, \ldots, c_n$ be such that $c_1 t(b_1) + \cdots + c_n t(b_n) = 0$. Then

$$t(c_1 b_1 + \cdots + c_n b_n) = c_1 t(b_1) + \cdots + c_n t(b_n) = 0,$$

but since t is injective we conclude that $c_1 v_1 + \cdots + c_n v_n = 0$. Since B is a basis for V, we conclude that $c_1 = \cdots = c_n = 0$.

Notice in fact that $t(B)$ has $n = \dim(V)$ elements, so it is sufficient to show that $t(B)$ is linearly independent or that it spans V to show that it is a basis. □

Problem 11. Suppose M is an abelian group (that is, a $\mathbb{Z}$-module) such that $|M| = 400$ and $\operatorname{ann}_{\mathbb{Z}}(M) = (20)$. Determine all the possibilities for M, up to isomorphism.

Proof. By the Classification of finitely generated modules over a PID, we know that

$$M \cong \mathbb{Z}^r \oplus \mathbb{Z}/(d_1) \oplus \cdots \oplus \mathbb{Z}/(d_k)$$

for some nonunits $d_1 | \cdots | d_k$. Since M is finite, we know that $r = 0$. Moreover,

$$400 = |M| = d_1 \cdots d_k.$$

We showed in a problem set that $\operatorname{ann}(M) = (d_k)$, so $d_k = 20$. Thus

$$d_1 \cdots d_{k-1} = \frac{400}{20} = 20 = 2^2 5.$$

Notice moreover that $400 = 2^4 5^2$. Since $d_1 | \cdots | d_k$ and $5 | d_i$ for some $i \leqslant k-1$, and 5 is prime, we must have $5 | d_{k-1}$. Similarly, $2 | d_{k-1}$, so $10 | d_{k-1}$. Thus $10 \cdot 20 = 200 | d_{k-1} d_k$ and $d_1 \cdots d_k = 400$. This leaves us with two options:

- $d_1 = 2$, $d_2 = 10$, and $d_3 = 20$, so
$$M \cong \mathbb{Z}/(2) \oplus \mathbb{Z}/(10) \oplus \mathbb{Z}/(20).$$
- $d_1 = 20$ and $d_2 = 20$, so
$$M \cong \mathbb{Z}/(20) \oplus \mathbb{Z}/(20). \quad \square$$