Problem Set 2

Due Thursday, January 29

Instructions: You are encouraged to work together on these problems, but each student should hand in their own final draft, written in a way that indicates their individual understanding of the solutions. Never submit something for grading that you do not completely understand. You cannot use any resources besides me, your classmates, and our course notes.

I will post the .tex code for these problems for you to use if you wish to type your homework. If you prefer not to type, please *write neatly.* As a matter of good proof writing style, please use complete sentences and correct grammar. You may use any result stated or proven in class or in a homework problem, provided you reference it appropriately by either stating the result or stating its name (e.g. the definition of ring or Lagrange's Theorem). Please do not refer to theorems by their number in the course notes, as that can change.

Problem 1. Let R be a ring, let M be an R-module, and N be a submodule of M.

(a) Suppose that M is free with basis B. Suppose that N is free with basis $C \subseteq B$. Show that M/N is free and give a formula for a basis in terms of B and C.

Proof. We claim that M/N is free on the basis $A = \{a + N \mid a \in B \smallsetminus C\}$.

First, we show that A is linearly independent. Let $(a_1 + N), \ldots, (a_n + N) \in A$ and take an R-linear combination

$$r_1(a_1 + N) + \cdots + r_n(a_n + N) = 0_{M/N}.$$

This means

$$(r_1 a_1 + \cdots + r_n a_n) + N = N$$

in M/N, which means that

$$r_1 a_1 + \cdots + r_n a_n \in N,$$

so we can write

$$r_1 a_1 + \cdots + r_n a_n = s_1 c_1 + \cdots + s_m c_m$$

for some $s_i \in R$, and $c_i \in C$, since C spans N. Moving everything to one side, we have

$$r_1 a_1 + \cdots + r_n a_n - s_1 c_1 - \cdots - s_m c_m = 0$$

and since $a_i, c_j \in B$, which is linearly independent, we must have $r_i = s_j = 0$ all i, j. In particular, $r_i = 0$ for all i, so A is linearly independent.

Now we show that A generates M/N. Let $m + N \in M/N$. Since B spans M we can write

$$m = r_1 a_1 + \cdots + r_n a_n + s_1 c_1 + \cdots + s_m c_m$$

for some $r_i, s_j \in R$, $a_i \in B \smallsetminus C$, and $c_j \in C$. Then, since $c_j \in N$,

$$m + N = (r_1 a_1 + \cdots + r_n a_n + s_1 c_1 + \cdots + s_m c_m) + N = r_1(a_1 + N) + \cdots + r_n(a_n + N)$$

in M/N, so A spans M/N. □

(b) Suppose that N is free and M/N is free. Show that M is free.

Proof. Let C be a basis for N, and let A be a basis for M/N. For any element $\alpha \in A$, we can write $\alpha = a + N$ for some $a \in M$; pick some a for each α and let $\widetilde{A}$ be the set of these elements a. We claim that $B = \widetilde{A} \cup C$ is a basis for M.

First we show that B is linearly independent. Let $a_1, \dots, a_n \in A$ and $c_1, \dots, c_m \in C$, and suppose

$$r_1a_1 + \cdots + r_na_n + s_1c_1 + \cdots + s_mc_m = 0.$$

Then we have

$$r_1a_1 + \cdots + r_na_n + s_1c_1 + \cdots + s_mc_m + N = r_1(a_1 + N) + \cdots + r_n(a_n + N) = N$$

in M/N, since $c_i \in N$. Since $\{a_i + N\}$ are linearly independent in M/N, we must have $r_i = 0$ for all i. Returning to our dependence relation, we have

$$s_1c_1 + \cdots + s_mc_m = 0,$$

and since C is linearly independent, we also have $s_j = 0$ for all j. Thus B is linearly independent.

Now we show that B generates M. Let $m \in M$. Since A is a basis for M/N, we can write

$$m + N = r_1(a_1 + N) + \cdots + r_n(a_n + N)$$

for some $r_i \in R$ and $a_i \in A$. This means that

$$m - (r_1a_1 + \cdots + r_na_n) \in N$$

so we can write

$$m - (r_1a_1 + \cdots + r_na_n) = s_1c_1 + \cdots + s_mc_m$$

for some $s_j \in R$ and $c_j \in C$. Then

$$m = r_1a_1 + \cdots + r_na_n + s_1c_1 + \cdots + s_mc_m$$

is generated by B. This shows that B is a basis. □

Problem 2. Let R be a ring, let M be an R-module, and N be a submodule of M.

(a) Give an example of a free module M and a submodule N that is free but M/N is not free.

Proof. One example is given by $R = \mathbb{Z}$, $M = \mathbb{Z}^1$, and $N = (2)$. To see that N is free, we consider the map $\mu : \mathbb{Z} \to \mathbb{Z}$ of multiplication by 2. We have seen that this is an R-module homomorphism. It is injective since $\mathbb{Z}$ is a domain, and its image is (2), so by the First Isomorphism Theorem, $\mathbb{Z} \cong (2)$ as $\mathbb{Z}$-modules, and hence (2) is free. We have seen that $\mathbb{Z}/(2)$ is not free in class, since no nonempty subset is linearly independent, and the empty set does not span. □

(b) Give an example of a free module M and a submodule N that is not free.

Proof. One example is given by $R = M = \mathbb{Z}[x]$ and $N = (2, x)$. To see that N is not free, suppose that N has a basis B. If $|B| \geq 2$, take $a, b \in B$; if $a = 0$ then $1 \cdot a = 0$ shows that B is linearly dependent, and otherwise the relation $b \cdot a - a \cdot b = 0$ shows that B is linearly dependent. If $|B| = 1$, then $(2, x)$ is generated by one element, so $(2, x) = R \cdot f$ for some $f \in R$. Then $(2, x) = (f)$ as ideals, but we showed in Math 818 that this is not a principal ideal. $|B| = 0$ is impossible since $N \neq 0$. We conclude that N is not free. □

Problem 3. A module M is **simple** if the only submodules of M are 0 and M. Let R be a commutative ring. Show that an R-module M is simple if and only if $M \cong R/\mathfrak{m}$ for some maximal ideal $\mathfrak{m}$.

Proof. ($\Rightarrow$) Assume M is simple and pick any element $m \in M$ with $m \neq 0_M$. Consider the submodule Rm of M generated by m. Since $m \neq 0$, then $Rm \neq 0$. Since M is simple, we conclude that $M = Rm$. By a result from class, every cyclic module is isomorphic to R/I for some ideal I. Therefore, $M \cong R/I$ for some ideal I.

By the lattice isomorphism theorem for modules, submodules of R/I are in bijective correspondence with submodules of R that contain I. A submodule of R is the same thing as an ideal, and since R/I is irreducible, we must have that there are no proper ideals of R that properly contain I — that is, I must be maximal. So $M \cong R/\mathfrak{m}$ for a maximal ideal $\mathfrak{m} = I$.

($\Leftarrow$) Assume $M \cong R/\mathfrak{m}$ for some maximal ideal $\mathfrak{m}$ of R. By the Lattice Isomorphism Theorem, the submodules of $R/\mathfrak{m}$ correspond to submodules I of R containing $\mathfrak{m}$. But a submodule of R is the same as an ideal, and since $\mathfrak{m}$ is maximal the only ideals $I \supseteq \mathfrak{m}$ are $\mathfrak{m}$ and R. Therefore, the only submodules of $R/\mathfrak{m}$ are $R/\mathfrak{m}$ and $\mathfrak{m}/\mathfrak{m} = 0$, and thus $R/\mathfrak{m}$ is simple. We conclude that M is simple. □

Problem 4. Prove that $\mathbb{Q}$ is not a free $\mathbb{Z}$-module.

Proof. By way of contradiction, suppose that $\mathbb{Q}$ has a basis B. Let $b = \frac{m}{n} \in B$, and consider $\frac{b}{2} = \frac{m}{2n} \in \mathbb{Q}$. We can write $\frac{b}{2} = \sum_i n_i b_i$ for some $n_i \in \mathbb{Z}$ and $b_i \in B$. Then

$$b = 2(\sum_i n_i b_i) = \sum_i (2n_i) b_i$$

implies

$$(-1)b + \sum_i (2n_i) b_i = 0,$$

contradicting linear independence of B. Thus, no basis exists. □