Problem Set 3 solutions

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

Proof. Assume towards a contradiction that R is not a field. Recall that a commutative ring R with $1 \neq 0$ is a field if and only if it has no nonzero proper ideals. Thus there is a nonzero, proper ideal I of R.

Consider the R-module R/I. If $r+I$ is any element, then for any $0 \neq a \in I$ we have $a(r+I) = 0$. Since $I \neq 0$ such an a exists, and thus any singleton set $\{r+I\}$ is linearly dependent. This proves that no nonempty subset of R/I can be linearly independent. So, the only possible basis of R/I is the empty set, which means that $R/I = \{0\}$. But $R/I \neq \{0\}$, since I is proper, a contradiction. □

Problem 2. An abelian group A is called divisible if for each $a \in A$ and integer $n > 1$, there exists $b \in A$ such that $a = nb$. Prove that if $A \neq \{0_A\}$ is a divisible abelian group then A is not a free $\mathbb{Z}$-module. Deduce that $\mathbb{Q}$ is not a free $\mathbb{Z}$-module.

Proof. Let $A \neq \{0_A\}$ be a divisible abelian group and assume towards a contradiction that A is a free $\mathbb{Z}$-module with basis B. Since $A \neq \{0_A\}$, $B \neq \emptyset$, so there exists $0_A \neq a \in B$. By a theorem from class (the UMP for free modules), there exists a $\mathbb{Z}$-module homomorphism $f\colon A \to \mathbb{Z}$ such that $f(a) = 1_{\mathbb{Z}}$. Pick any integer $n > 1$. Since A is divisible, there exists $b \in A$ such that $a = nb$, and thus $1_{\mathbb{Z}} = f(a) = f(nb) = nf(b)$, since f is a $\mathbb{Z}$-module homomorphism. Therefore, $n \mid 1_{\mathbb{Z}}$, which is a contradiction since $n > 1$.

Now notice that $\mathbb{Q}$ is divisible, since for any $q \in \mathbb{Q}$ and $n \in \mathbb{N}$ the element $q' = q/n \in \mathbb{Q}$ satisfies $q = nq'$. By the first part of the proof, $\mathbb{Q}$ is not a free $\mathbb{Z}$-module. □

Problem 3. Let R be a commutative ring with $1 \neq 0$.

a) Show that if M is a nonzero free R-module, then $\operatorname{ann}(M) = 0$.

b) Give an example of a ring R an a module M such that $\operatorname{ann}(M) \neq 0$.

Proof.

a) Suppose towards a contradiction that $M \neq \{0_M\}$ is a free R-module but $\operatorname{ann}_R(M) \neq \{0_R\}$. Let $0_R \neq r \in \operatorname{ann}_R(M)$ and let $b \in M$ be an element of a basis of M. Then $rb = 0_M$ by the definition of the annihilator, and this shows that $\{b\}$ lis linearly dependent. This contradicts the fact that b is a basis element. Therefore, $\operatorname{ann}_R(M) = \{0_R\}$.

b) Let R be any commutative ring with $1 \neq 0$ that is not a field, and let I be a nontrivial ideal. The module R/I is not free, as we showed in Problem 1, and $\operatorname{ann}(R/I) = I$.

   For a more concrete example, take $R = \mathbb{Z}$ and $I = (2)$, and note that $\operatorname{ann}(\mathbb{Z}/(2)) = (2)$.

□

Problem 4. Prove that if R is a commutative ring with $1 \neq 0$ then $R^m \cong R^n$ as R-modules if and only if $m = n$. In order to do that, you will complete he following steps:

a) Show that if I is any ideal of R and M is any R-module, then M/IM is an R/I-module via

$$(r+I) \cdot (m+IM) = rm + IM.$$

Proof. Given the R/I-action defined by $(r+I)\cdot(m+IM) = rm+IM$, we need to show that our proposed action is well-defined, and then that this makes M/IM a module.

- *The action is well defined:* To prove this, suppose $r+I = s+I$ and $m+IM = n+IM$. Then $r-s \in I$ and $m-n \in IM$, hence

  $$rm - sn = rm - rn + rn - sn = r(m-n) + (r-s)n \in IM$$

  since IM is closed under addition and the R-action. This shows that $rm+IM = sn+IM$ and thus
  $$(r+I)(m+IM) = (s+I)(n+IM).$$
- *The module axioms hold true:* This follows from the fact that, since IM is an R-submodule, then M/IM is an R-module with R-action $r(m+IM) = rm+IM$. Since the action of R/I on M/IM is the same as the R-action (meaning, the coset $r+I$ acts on M/IM in the same way its representative r acts on M/IM) and since all the module axioms hold for the R-action, they also hold for the R/I-action.

  For example, here is one of the axioms are in more detail:

  $$\begin{aligned}((r+I)+(s+I))(m+IM) &= ((r+s)+I)(m+IM)\\ &= (r+s)(m+IM)\\ &= r(m+IM)+s(m+IM) && M/IM \text{ is an } R\text{-module}\\ &= (r+I)(m+IM)+(s+I)(m+IM)\end{aligned}$$ □

b) Show that if I is any ideal of R, then $R^n/IR^n \cong (R/I)^n$ as R/I-modules.

Proof. Let $f : R^n \to (R/I)^n$ be the unique R-module homomorphism such that $f(e_i) = \overline{e_i}$, where e_i is the vector with a 1 in the ith position and 0 elsewhere, and $\overline{e}_i$ is the vector with $1+I$ in the ith position and $0+I$ elsewhere. Such a map exists by the UMP for free modules since $\{e_1,\ldots,e_n\}$ form a basis for R^n.

Since the $\overline{e}_i$ form a basis for $(R/I)^n$ and since $\operatorname{im}(f)$ is a subspace of $(R/I)^n$ that contains all the $\overline{e}_i$, it follows that $\operatorname{im}(f) = (R/I)^n$, and thus f is surjective. A vector $(a_1,\ldots,s_n)$ is in the kernel of f if and only if $(a_1+I,\ldots,a_n+I) = (0+I,\ldots,0+I)$, or equivalently $a_i \in I$ for all i. Therefore

$$\ker(f) = \{(a_1,\ldots,a_n) \mid a_i \in I\} = \left\{\sum_{i=1}^n a_i e_i \mid a_i \in I\right\} = IR^n.$$

The last equality follows because the containment $\subseteq$ holds by definition of IR^n and the containment $\supseteq$ is justified by the calculations below:

$$IR^n = \left\{\sum_{i=1}^m b_i r_i \mid b_i \in I, r_i \in R^n\right\} = \left\{\sum_{i=1}^m b_i \sum_{j=1}^n c_{ij} e_j \mid b_i \in I, c_{ij} \in R\right\}$$

$$= \left\{\sum_{j=1}^n \left(\sum_{i=1}^m b_i c_{ij}\right) e_j \mid b_i \in I, c_{ij} \in R \Rightarrow b_i c_{ij} \in I\right\}.$$

So, by the first isomorphism theorem, f induces an R-**module** isomorphism

$$\overline{f} : R^n/IR^n \xrightarrow{\cong} (R/I)^n.$$

Moreover, both the source and target of $\overline{f}$ are R/I-modules: the right-hand side for obvious reasons and the left-hand side by part a). We actually want $\overline{f}$ to be an R/I-module isomorphism. We already know that $\overline{f}$ preserves sums, since it is an R-module homomorphism. All that remains is to check that $\overline{f}$ is R/I-linear. Since $\overline{f}$ is R-linear:

$$\overline{f}((r+I)(m+IR^n)) = \overline{f}((rm+IR^n)) = f(rm) = rf(m) = (r+I)\overline{f}(m+IR^n).$$

The last equality follows since R/I acts on $(R/I)^n$ by $(r+I)t = rt$ for any $t \in (R/I)^n$. ☐

c) Apply the previous part when $I = \mathfrak{m}$ is a maximal ideal of R.

Tip: You will need to use the following fact, which we shall prove in class very soon: if F is a field, then $F^n \cong F^m$ as F-vector spaces if and only if $m = n$.

Proof. We want to show that $R^m \cong R^n$ as R-modules if and only if $m = n$. If $m = n$, then $R^m \cong R^n$ trivially.

Now assume that $\varphi : R^n \to R^m$ is an R-module isomorphism. Take any maximal ideal $\mathfrak{m}$ of R, which exists by a result from Math 817. Consider the quotient map $q \colon R^m \to R^m/\mathfrak{m}R^m$ and the composite map $\psi = q \circ \varphi$. This is an R-module homomorphism, which is surjective since both q and φ are surjective. Let's consider the kernel of ψ. We know that $\ker q = \mathfrak{m}R^m$, since q is the canonical projection. Since φ is injective, the kernel of ψ is just the preimage of $\mathfrak{m}R^n$ via φ:

$$\ker(\psi) = \psi^{-1}(0) = \varphi^{-1}(q^{-1}(0)) = \varphi^{-1}(\mathfrak{m}R^m).$$

But φ^{-1} is an R-module homomorphism as well, so

$$\ker(\psi) = \mathfrak{m}\varphi^{-1}(R^m) = \mathfrak{m}R^n.$$

The First Isomorphism Theorem now gives the existence of an R-module isomorphism

$$\overline{\psi} : R^n/\mathfrak{m}R^n \to R^m/\mathfrak{m}R^m \quad \overline{\psi}(m+\mathfrak{m}R^n) = \psi(m).$$

We claim that $\overline{\psi}$ is in fact an $R/\mathfrak{m}$-module homomorphism; we need to check that this is an $R/\mathfrak{m}$-linear map:

$$\overline{\psi}((r+\mathfrak{m})(m+\mathfrak{m}R^n)) = \overline{\psi}(rm+\mathfrak{m}R^n) = \psi(rm) = r\psi(m) = (r+I)\overline{\psi}(m+\mathfrak{m}R^n),$$

where the last equality uses again the formula for the $R/\mathfrak{m}$-action on $R^m/\mathfrak{m}R^m$.

Using part b), we have the further isomorphisms

$$(R/\mathfrak{m})^n \cong R^n/\mathfrak{m}R^n \cong R^m/\mathfrak{m}R^m \cong (R/\mathfrak{m})^m.$$

Now rewriting the above isomorphism in terms of the field $F = R/\mathfrak{m}$ gives $F^n \cong F^m$ as F-vector spaces, and we know from class that this is true if and only if $m = n$. ☐