Math 517 **Spring 2007** **Radford**

Written Homework # 1 Solution

02/28/07

Throughout R, S are rings with unity and modules are unital.

1. (**20 points**) Let I be a non-empty set and let $\{P_i\}_{i\in I}$ be an indexed family of left R-modules. A *product of the family* is a pair $(\{\pi_i\}_{i\in I}, P)$, where

(P.1) P is a left R-module and $\pi_i : P \longrightarrow P_i$ is a homomorphism of left R-modules for all $i \in I$, and

(P.2) If $(\{\pi'_i\}_{i\in I}, P')$ is a pair which satisfies (P.1) then there is a unique R-module homomorphism $\Phi : P' \longrightarrow P$ which satisfies $\pi_i \circ \Phi = \pi'_i$ for all $i \in I$.

Prove the following theorem:

Theorem 1 *Let R be a ring with unity, let I be a non-empty set, and let $\{P_i\}_{i\in I}$ be an indexed family of left R-modules.*

(1) *There is a product of the family $\{P_i\}_{i\in I}$.*

(2) *Suppose that $(\{\pi_i\}_{i\in I}, P)$ and $(\{\pi'_i\}_{i\in I}, P')$ are products of the family $\{P_i\}_{i\in I}$. Then there is a unique isomorphism of left R-modules $\Phi : P' \longrightarrow P$ which satisfies $\pi_i \circ \Phi = \pi'_i$ for all $i \in I$.*

[Hint: Let P be the set of all functions $f : I \longrightarrow \bigcup_{i\in I} P_i$ which satisfy $f(i) \in P_i$ for all $i \in I$. Show that P is a left R-module under the operations

$$(f + g)(i) = f(i) + g(i)$$

and

$$(r\cdot f)(i) = r\cdot(f(i))$$

for all $f, g \in P$ and $i \in I$. Consider $\pi_i : P \longrightarrow P_i$ defined by $\pi_i(f) = f(i)$ for all $f \in P$ and $i \in I$.]

Solution: Part (1) of the theorem (**10**). Let $f, g, h \in P$ and $r, r' \in R$. Then $(f+g)(i) = f(i) + g(i) \in P_i$ and $(r{\cdot}f)(i) = r{\cdot}f(i) \in P_i$ for all $i \in I$ since the P_i's are modules. Thus P is closed under addition and multiplication by elements of R.

Let $0 \in P$ be defined by $0(i) = 0 \in P_i$ for all $i \in I$ and $(-f)(i) = -f(i) \in P_i$ for all $i \in I$. Then

$$(f+g)+h = f+(g+h), \quad f+g = g+f, \quad 0+f = f, \quad f+(-f) = 0,$$

and

$$r{\cdot}(f+g) = r{\cdot}f + r{\cdot}g, \quad (r+r'){\cdot}f = r{\cdot}f + r'{\cdot}f, \quad rr'{\cdot}f = r{\cdot}(r'{\cdot}f), \quad 1{\cdot}f = f$$

are established by showing that both sides of each equation evaluated on $i \in I$ agree. Thus P is a left R-module.

Let $I \in I$. Define $\pi_i : P \longrightarrow P_i$ by $\pi_i(f) = f(i)$ for all $f \in P$. Since

$$\pi_i(f+g) = (f+g)(i) = f(i) + g(i) = \pi_i(f) + \pi_i(g)$$

and

$$\pi_i(r{\cdot}f) = (r{\cdot}f)(i) = r{\cdot}f(i) = r{\cdot}\pi_i(f)$$

show that π_i is a homomorphism of left R-modules. Therefore $(\{\pi_i\}_{i\in I}, P)$ satisfies (P.1).

Suppose that $(\{\pi'_i\}_{i\in I}, P')$ also satisfies (P.1) and $\Phi : P' \longrightarrow P$ is a homomorphism of left R-modules which satisfies $\pi_i \circ \Phi = \pi'_i$ for all $i \in I$. Let $p' \in P'$. Then

$$\Phi(p')(i) = \pi_i(\Phi(p')) = (\pi_i \circ \Phi)(p') = \pi'_i(p') \tag{1}$$

for all $i \in I$ shows the uniqueness part of (P.2). As for existence, let Φ be defined by (1) and let $p', p'' \in P'$. The calculations

$$\begin{aligned} \Phi(p'+p'')(i) &= \pi'_i(p'+p'') \\ &= \pi'_i(p') + \pi'_i(p'') \\ &= \Phi(p')(i) + \Phi(p'')(i) \\ &= (\Phi(p') + \Phi(p''))(i) \end{aligned}$$

and

$$\Phi(r{\cdot}p')(i) = \pi'_i(r{\cdot}p') = r{\cdot}\pi'_i(p') = r{\cdot}(\Phi(p')(i)) = (r{\cdot}\Phi(p'))(i)$$

for all $i \in I$ shows that $\Phi(p' + p'') = \Phi(p') + \Phi(p'')$ and $\Phi(r{\cdot}p') = r{\cdot}\Phi(p')$. Therefore Φ is a homomorphism of left R-modules; by (1) note that $\pi_i{\circ}\Phi = \pi'_i$ for all $i \in I$. We have completed the proof of part (1) of the theorem.

To show part (2) of the theorem (**10**), suppose that $(\{\pi_i\}_{i\in I}, P)$ and $(\{\pi'_i\}_{i\in I}, P')$ are products of the family $\{P_i\}_{\imath\in I}$. Then there is a unique isomorphism of left R-modules $\Phi : P' \longrightarrow P$ such that $\pi_i{\circ}\Phi = \pi'_i$ for all $i \in I$. Likewise there is a unique isomorphism of left R-modules $\Phi' : P \longrightarrow P'$ such that $\pi'_i{\circ}\Phi' = \pi_i$ for all $i \in I$. For $i \in I$ the composite $\Phi{\circ}\Phi' : P \longrightarrow P$ satisfies

$$\pi_i{\circ}(\Phi{\circ}\Phi') = \pi_i{\circ}\mathrm{Id}_P \tag{2}$$

as

$$\pi_i{\circ}(\Phi{\circ}\Phi') = (\pi_i{\circ}\Phi){\circ}\Phi' = \pi'{\circ}\Phi' = \pi_i.$$

With $(\{\pi_i\}_{i\in I}, P)$ as the pair of (P.2) it follows by (2) that $\Phi{\circ}\Phi' = \mathrm{Id}_P$. Reversing the roles of $(\{\pi_i\}_{i\in I}, P)$ and $(\{\pi'_i\}_{i\in I}, P')$ we conclude that $\Phi'{\circ}\Phi = \mathrm{Id}_{P'}$ also. Therefore Φ and Φ' are isomorphisms.

2. (**30 points**) Let I be a non-empty set. A *free R-module on I* is a pair $(\imath, F)$, where

(F.1) F is a left R-module and $\imath : I \longrightarrow F$ is a set map, and

(F.2) if $(\imath', F')$ is a pair which satisfies (F.1) then there is a unique R-module homomorphism $\Phi : F \longrightarrow F'$ which satisfies $\Phi{\circ}\imath = \imath'$.

Prove the following theorem:

Theorem 2 *Let R be a ring with unity and let I be a non-empty set.*

(1) *There is a free left R-module $(\imath, F)$ on I.*

(2) *Suppose that $(\imath, F)$ and $(\imath', F')$ are free left R-modules on I. Then there is a unique isomorphism of left R-modules $\Phi : F \longrightarrow F'$ which satisfies $\Phi{\circ}\imath = \imath'$.*

Suppose that $(\imath, F)$ is a free left R-module.

(3) $\mathrm{Im}\,\imath$ *generates F as a left R-module.*

(4) *$\imath$ is injective and $\{\imath(\ell)\}_{\ell \in I}$ is a basis for F.*

[Hint: For part (1), let F be the subset of the product P of the family $\{R_i\}_{i \in I}$, where $R_i = R$ for all $i \in I$, of Exercise 1 consisting of all functions with finite (which includes empty) support. For $f \in P$ the support of f is defined by

$$\operatorname{supp} f = \{i \in I \mid f(i) \neq 0\}.$$

]

Solution: Part (1) of the theorem (**8**) . Let P be the module of Exercise 1 constructed with the family $\{P_i\}_{i \in I}$, where $P_i = R$ for all $i \in I$, and let F be the subset of all functions $f \in P$ with finite support. For $f, g \in P$ and $r \in R$ observe that

$$\operatorname{supp}(f - r{\cdot}g) \subseteq \operatorname{supp} f \cup \operatorname{supp} g; \tag{3}$$

for if $0 \neq (f - r{\cdot}g)(i) = f(i) - r{\cdot}g(i)$ then either $f(i) \neq 0$ or $g(i) \neq 0$. Since $0 \in F$ it follows by (3) that F is a submodule of P.

For $i \in I$ let $\imath(i) : I \longrightarrow R$ be the function defined by

$$\imath(i)(j) = \begin{cases} 1 & : \; j = i; \\ 0 & : \; j \neq i \end{cases} .$$

Then $\imath(i) \in F$ and $\imath : I \longrightarrow F$ defines an injective function.

We will show that $\{\imath(i)\}_{i \in I}$ is a basis for F. Suppose that $i_1, \ldots, i_n \in I$ are distinct and $r_1, \ldots, r_n \in R$. Set

$$f = \sum_{\ell=1}^{n} r_\ell{\cdot}\imath(i_\ell).$$

Since $f(j) = \sum_{\ell=1}^{n} (r_\ell{\cdot}\imath(i_\ell))(j) = \sum_{i=1}^{n} r_\ell(\imath(i_\ell)(j))$ for all $j \in I$ we have

$$f(j) = \begin{cases} 0 & : \; j \notin \{i_1, \ldots, i_n\}; \\ r_\ell & : \; j = i_\ell \end{cases}$$

Thus $\{i_\ell)\}_{i \in I}$ is independent (take $f = 0$) and spans as $f \in F \backslash 0$ can be written

$$f = \sum_{i \in \operatorname{supp} f} f(i){\cdot}\imath(i). \tag{4}$$

Therefore $\{i_\ell)\}_{i\in I}$ is a basis for F. We have done most of the work at this point.

Suppose that $(\imath', F')$ satisfies (F.2) and $\Phi : F \longrightarrow F'$ is a homomorphism of left R-modules such that $\Phi\circ\imath = \imath'$. Then $\Phi(\imath(i)) = \imath'(i)$ for all $i \in I$. Thus for $i_1, \ldots, i_n \in I$ distinct and $r_1, \ldots, r_n \in R$ we have

$$\begin{aligned} &\Phi(r_1{\cdot}\imath(i_1) + \cdots + r_n{\cdot}\imath(i_n)) \\ &\quad = \; r_1{\cdot}\Phi(\imath(i_1)) + \cdots + r_n{\cdot}\Phi(\imath(i_n)) \\ &\quad = \; r_1{\cdot}\imath'(i_1) + \cdots + r_n{\cdot}\imath'(i_n). \end{aligned} \tag{5}$$

We have shown the uniqueness part of (F.2); that is there is at most one Φ which satisfies (F.2). As for existence, the reader is left with the small exercise of showing that (5) describes a well-defined module homomorphism which satisfies the condition of (F.2).

Part (2) of the theorem (**8**). Let $(\imath, F)$ and $(\imath', F')$ be free left R-modules on I. There is a unique homomorphism of R-modules $\Phi : F \longrightarrow F'$ such that $\Phi\circ\imath = \imath'$ and there unique homomorphism of R-modules $\Phi' : F' \longrightarrow F$ such that $\Phi\circ\imath' = \imath$. Using $(\imath, F)$ for (F.2) we see the identity map $\mathrm{Id}_F : F \longrightarrow F$ is the only R-module homomorphism f such that $f\circ\imath = \imath$.

Observe that

$$(\Phi'\circ\Phi)\circ\imath = \Phi'\circ(\Phi\circ\imath) = \Phi'\circ\imath' = \imath = \mathrm{Id}_F\circ\imath.$$

Thus $\Phi'\circ\Phi = \mathrm{Id}_F$ from which $\Phi\circ\Phi' = \mathrm{Id}_{F'}$ by reversing the roles of $(\imath, F)$ and $(\imath', F')$. Thus Φ is an isomorphism.

Comment: *To do parts (3) and (4) we can use (2) to note that that all free modules on I are isomorphic in a specific way and then transfer the (algebraic) properties of the particular model we constructed for part (1). We follow a different approach – namely we use the "universal mapping property" of free modules instead.*

Part (3) of the theorem (**7**). We first show that $(\imath, F_r)$ is a free left R-module on I, where $F_r = (\mathrm{Im}\,\imath)$. Since $\mathrm{Im}\,\imath \subseteq F_r$, by abuse of notation, we regard $\imath$ as a function $\imath : I \longrightarrow F_r$.

Suppose that $(\imath', F')$ is a pair which satisfies (F.1). Then there homomorphism of R-modules $\Phi : F \longrightarrow F'$ such that $\Phi\circ\imath = \imath'$. The restriction $\Phi_r = \Phi_r|_{F_r} : F_r \longrightarrow F'$ is a homomorphism of left R-modules and $\Phi_r\circ\imath = \imath'$.

Suppose that $\Phi' : F_r \longrightarrow F'$ is also a homomorphism of left R-modules and $\Phi' \circ \imath = \imath'$. Then $\Phi_r(\imath(\ell)) = \imath'(\ell) = \Phi'(\imath(\ell))$ for all $\ell \in I$. Therefore Φ_r, Φ' agree on generators of F_r which means they are the same. Thus $(\imath, F_r)$ is a free left R-module on I.

Now by the mapping property of free modules on I there is a unique homomorphism $\Phi : F_r \longrightarrow F$ which satisfies $\Phi \circ \imath = \imath$, and this is an isomorphism by part (2). But the inclusion $\mathrm{inc} : F_r \longrightarrow F$ satisfies $\mathrm{inc} \circ \imath = \imath$. Therefore $\mathrm{inc} = \Phi$ and is thus an isomorphism. This means $F_r = F$ as required.

Part (4) of the theorem (**7**). Let $\ell, \ell' \in I$ be distinct and let $\imath' : I \longrightarrow R$ by any function such that $\imath(\ell) = 0$ and $\imath(\ell') = 1$. As $\Phi \circ \imath = \imath'$ we have

$$\Phi(\imath(\ell)) = \imath'(\ell) = 0 \neq 1 = \imath'(\ell') = \Phi(\imath(\ell')).$$

Therefore $\imath(\ell) \neq \imath(\ell')$. We have shown that $\imath$ is one-one.

In light of (3), to show that $\{\imath(\ell)\}_{\ell \in I}$ is a basis we F we need only show independence. Suppose that $\ell_1, \ldots, \ell_n \in I$ are distinct and

$$r_1 \cdot \imath(\ell_1) + \cdots + r_n \cdot \imath(\ell_n) = 0,$$

where $r_1, \ldots, r_n \in R$. Fix $1 \leq i \leq n$ and let $\imath' : I \longrightarrow$ be any function such that $\imath'(\ell_i) = 1$ and $\imath'(j) = 0$ for all $j \in I$, $j \neq \ell_i$. Then the calculation

$$\begin{aligned} 0 &= \Phi(r_1 \cdot \imath(\ell_1) + \cdots + r_n \cdot \imath(\ell_n)) \\ &= r_1 \cdot \Phi(\imath(\ell_1)) + \cdots + r_n \cdot \Phi(\imath(\ell_n)) \\ &= r_1 \imath'(\ell_1) + \cdots + r_n \imath'(\ell_n) \\ &= r_i 1 \\ &= r_i \end{aligned}$$

shows that $r_1 = \cdots = r_n = 0$.

3. (**25 points**) Suppose that $f : R \longrightarrow S$ is a function and for $r \in R$ and $s \in S$ define $r \cdot s = f(r)s$.

(a) (**18**) Show that f is a homomorphism of rings with unity and $\mathrm{Im}\, f$ is in the center of S if and only if S is a left R-module and

$$r \cdot (ss') = (r \cdot s)s' = s(r \cdot s') \tag{6}$$

for all $r \in R$ and $s, s' \in S$.

(b) (**7**) Suppose that S has a left R-module structure $(S, \bullet)$ which satisfies (6). Define $F : R \longrightarrow S$ by $F(r) = r\bullet 1$ for all $r \in R$. Show that F is a homomorphism of rings with unity and $\operatorname{Im} F$ is in the center of S.

The ring S is called an R-*algebra* if ${}_RS$ and (6) is satisfied. The exercise shows there are two ways of describing an R-algebra.

Solution: Suppose that f is a homomorphism of rings with unity and $\operatorname{Im} f$ is in the center of S. Let $r, r' \in R$ and $s, s' \in S$. We have

$$(r + r')\cdot s = f(r + r')s = (f(r) + f(r'))s = f(r)s + f(r')s = r\cdot s + r'\cdot s,$$

$$r\cdot(s + s') = f(r)(s + s') = f(r)s + f(r)s' = r\cdot s + r\cdot s',$$
$$(rr')\cdot s = f(rr')s = f(r)f(r')s = f(r)(f(r')s) = r\cdot(r'\cdot s),$$
$$1\cdot s = f(1)s = 1s = s$$

since f is a homomorphism of rings with unity. Since $\operatorname{Im} f$ is in the center of S we have

$$f(r)ss' = (f(r)s)s' = (sf(r))s' = s(f(r)s')$$

which translates to

$$r\cdot ss' = (r\cdot s)s' = s(r\cdot s').$$

Observe that $f(r) = r\cdot 1$ for all $r \in R$.

Now the converse follows by part (b). So we do both at once. That f (and thus F) is a homomorphism of rings with unity whose image lies in the center of S follows from

$$(r + r')\cdot 1 = r\cdot 1 + r'\cdot 1$$

$$rr'\cdot 1 = r\cdot(r'\cdot 1) = r\cdot(1(r'\cdot 1)) = (r\cdot 1)(r'\cdot 1),$$
$$1\cdot 1 = 1,$$

and

$$(r\cdot 1)s = r\cdot(1s) = r\cdot(s1) = s(r\cdot 1).$$

4. (**25 points**) Let $\mathbf{Z}$ be the ring of integers and $\mathbf{Q}$ be the field of rational numbers.

(a) (**8**) Let $\imath : 2\mathbf{Z} \longrightarrow \mathbf{Z}$ be the inclusion. Show that $\imath \otimes \mathrm{Id} : 2\mathbf{Z} \otimes_{\mathbf{Z}} (\mathbf{Z}/2\mathbf{Z}) \longrightarrow \mathbf{Z} \otimes_{\mathbf{Z}} (\mathbf{Z}/2\mathbf{Z})$ is not injective.

Solution: Let $\mathbf{Z}_2 = \mathbf{Z}/2\mathbf{Z}$ and $f : \mathbf{Z} \longrightarrow 2\mathbf{Z}$ be the isomorphism of abelian groups (left $\mathbf{Z}$-modules) defined by $f(n) = 2n$ for all $n \in \mathbf{Z}$. The composition of isomorphisms

$$\mathbf{Z}_2 \longrightarrow \mathbf{Z} \otimes_{\mathbf{Z}} \mathbf{Z}_2 \stackrel{f \otimes \mathrm{Id}_{\mathbf{Z}_2}}{\longrightarrow} 2\mathbf{Z} \otimes_{\mathbf{Z}} \mathbf{Z}_2,$$

where the first is the "left version" of the isomorphism of ClassNotes, Proposition 2.1.2, yields $1 \mapsto 1 \otimes 1 \mapsto 2 \otimes 1$. Therefore $0 \neq 2 \otimes 1 \in 2\mathbf{Z} \otimes_{\mathbf{Z}} \mathbf{Z}_2$. As an element of $\mathbf{Z} \otimes_{\mathbf{Z}} \mathbf{Z}_2$ we have $2 \otimes 1 = 1 \cdot 2 \otimes 1 = 1 \otimes 2 \cdot 1 = 1 \otimes 0 = 0$. Therefore $\imath \otimes \mathrm{Id}_{\mathbf{Z}}$ is not injective.

(b) (**8**) Show that $\mathbf{Q} \otimes_{\mathbf{Z}} A = (0)$ for all finite abelian groups A.

Solution: Let $n = |A|$. Then $n \cdot a = 0$ for all $a \in A$. (The multiplicative version of this is $a^n = e$ for all $a \in A$.) For $q \in \mathbf{Q}$ and $a \in A$ we calculate

$$q \otimes a = (q/n)n \otimes a = (q/n) \otimes n \cdot a = (q/n) \otimes 0 = 0.$$

Since the elements of $\mathbf{Q} \otimes A$ are sums of elements of the type $q \otimes a$ it follows that $\mathbf{Q} \otimes_{\mathbf{Z}} A = (0)$.

(c) (**9**) Suppose that $f : M_R \longrightarrow M'_R$ and $g : {}_R N \longrightarrow {}_R N'$ are surjective maps of R-modules. Show that the homomorphism of abelian groups $f \otimes g : M \otimes_R N \longrightarrow M' \otimes_R N'$ is a surjective.

Solution: Let $y \in M' \otimes_R N'$. Then $y = \sum_{i=1}^{s} m'_i \otimes n'_i$, where $m'_i \in M$ and $n'_i \in N'$ for all $1 \leq i \leq s$. Since f and g are surjective there are $m_i \in M$ and $n_i \in N$ such that $f(m_i) = m'_i$ and $g(n_i) = n'_i$ for all $1 \leq i \leq s$. Set $x = \sum_{i=1}^{s} m_i \otimes n_i$ Since $f \otimes g$ is a group homomorphism

$$\begin{aligned} (f \otimes g)(x) &= (f \otimes g)(\sum_{i=1}^{s} m_i \otimes n_i) \\ &= \sum_{i=1}^{s} (f \otimes g)(m_i \otimes n_i) \\ &= \sum_{i=1}^{s} f(m_i) \otimes g(n_i) \\ &= \sum_{i=1}^{s} m'_i \otimes n'_i \\ &= y. \end{aligned}$$

Therefore $f \otimes g$ is surjective.