

Homework 7

D. Zack Garza

November 6, 2019

Contents

1	Problem 1	1
1.1	Part 1	1
1.2	Part 2	2
2	Problem 2	3
2.1	Part 1	3
2.2	Part 2	3
3	Problem 3	3
3.1	Part 1	3
3.2	Part 2	4
3.3	Part 3	5
4	Problem 4	6
5	Problem 5	7
5.1	Part (a)	7
5.2	Part (b)	8
5.3	Part (c)	8
5.4	Part (d)	9
6	Problem 6	9
7	Problem 7	10

1 Problem 1

1.1 Part 1

In order for IS to be a submodule of A , we need to show the following implication:

$$x \in IS, a \in A \implies xa, ax \in IS.$$

Suppose $x \in IS$. Then by definition, $x = \sum_{i=1}^n r_i a_i$ for some $r_i \in R, a_i \in A$.

But then

$$\begin{aligned}
xa &= \left(\sum_{i=1}^n r_i a_i \right) a \\
&= \sum_{i=1}^n r_i a_i a \\
&:= \sum_{i=1}^n r_i a'_i,
\end{aligned}$$

where $a'_i := a_i a$ for each i , which is still an element of A since A itself is a module and thus closed under multiplication.

But this expresses xa as an element of IS . Similarly, we have

$$\begin{aligned}
ax &= a \left(\sum_{i=1}^n r_i a_i \right) \\
&= \sum_{i=1}^n a r_i a_i a \\
&:= \sum_{i=1}^n r_i a a_i, \\
&:= \sum_{i=1}^n r_i a'_i,
\end{aligned}$$

and so $ax \in IS$ as well.

1.2 Part 2

Letting $R/I \curvearrowright A/IA$ be the action given by $r + I \curvearrowright +IA := ra + IA$, we need to show the following:

- $r.(x + y) = r.x + r.y$,
- $(r + r').x = r.x + r'.x$,
- $(rs).x = r.(s.x)$, and
- $1.x = x$.

Letting \oplus denote the addition defined on cosets, we have

$$\begin{aligned}
r \curvearrowright (x + IA \oplus y + IA) &:= r \curvearrowright x + y + IA \\
&:= r(x + y) + IA \\
&= rx + ry + IA \\
&:= rx + IA \oplus ry + IA \\
&:= (r \curvearrowright x + IA) \oplus (r \curvearrowright y + IA).
\end{aligned}$$

$$\begin{aligned}
(r + s) \curvearrowright x + IA &:= (r + s)x + IA \\
&:= rx + sx + IA \\
&:= rx + IA \oplus sx + IA \\
&:= (rs \curvearrowright IA) \oplus (sx \curvearrowright IA).
\end{aligned}$$

$$\begin{aligned}
(rs) \curvearrowright x + IA &:= rsx + IA \\
&= r(sx) + IA \\
&:= r \curvearrowright (sx + IA) \\
&= r \curvearrowright (s \curvearrowright x + IA).
\end{aligned}$$

$$1 \curvearrowright x + IA := 1x + IA = x + IA.$$

2 Problem 2

2.1 Part 1

We want to show that every simple R -module M is cyclic, i.e. if the only ideals of M are (0) and M itself, that $M = \langle m \rangle$ for some element $m \in M$.

Towards a contradiction, let M be a simple R -module and suppose M is not cyclic, so $M \neq \langle m \rangle$ for any $m \in M$. But then let $a \in M$ be an arbitrary nontrivial element; then (a) is a non-empty ideal (since it contains a), so $(a) \neq 0$. Since M is simple, we must have $(a) = M$, a contradiction.

2.2 Part 2

Let $\phi : A \rightarrow A$ be a module endomorphism on a simple module A . Then $\text{im } \phi := \phi(A)$ is a submodule of A . Since A is simple, we have either $\text{im } \phi = 0$, in which case ϕ is the zero map, or $\text{im } \phi = A$, so ϕ is surjective. In this case, we can also consider $\ker \phi$, which is a submodule of A . Since A is simple, we can again only have $\ker \phi = A$, which can not happen if ϕ is not the zero map, or $\ker \phi = 0$, in which case ϕ is both a surjective and an injective map and thus an isomorphism of modules.

3 Problem 3

3.1 Part 1

We want to show that if A, B are R -modules then $X = (\text{hom}_{R\text{-mod}}(A, B), +)$ is an abelian group. Let $f, g, h \in X$, we then need to show the following:

- a. Closure: $f + g \in X$
- b. Associativity: $f + (g + h) = (f + g) + h$

- c. Identity: $\text{id} \in X$
- d. Inverses: $f^{-1} \in X$
- e. Commutativity: $f + g = g + f$

Closure: This follows from the definition, because $(f + g) \curvearrowright x := f(x) + g(x)$ pointwise, which is well-defined homomorphism $A \rightarrow B$.

Associativity: We have

$$\begin{aligned}
 f + (g + h) \curvearrowright x &:= f(x) + (g + h)(x) \\
 &:= f(x) + (g(x) + h(x)) \\
 &= (f(x) + g(x)) + h(x) \\
 &= (f + g) \curvearrowright x.
 \end{aligned}$$

Identity: We can define $\mathbf{0} : A \rightarrow B$ by $\mathbf{0}(x) = 0 \in B$. Then

$$(f + \mathbf{0}) \curvearrowright x = f(x) + 0 = f(x) = 0 + f(x) = (\mathbf{0} + f) \curvearrowright x.$$

Inverses: Given $f \in X$, we can define $-f : A \rightarrow B$ as $-f(x) = -x$. Then

$$\begin{aligned}
 (f + -f) \curvearrowright x &= f(x) + -f(x) = f(x) - f(x) = x - x = 0 = \mathbf{0} \curvearrowright x \\
 (-f + f) \curvearrowright x &= -f(x) + f(x) = -f(x) + f(x) = -x + x = 0 = \mathbf{0} \curvearrowright x.
 \end{aligned}$$

Commutativity: Since B is a module, by definition $(B, +)$ is an abelian group. Thus

$$(f + g) \curvearrowright x = f(x) + g(x) = g(x) + f(x) = (g + f) \curvearrowright x.$$

3.2 Part 2

By part 1, $(\text{hom}_{R\text{-mod}}(A, A), +)$ is an abelian group, We just need to check that $(\text{hom}_R(A, A), \circ)$ is a monoid, i.e.:

- Associativity: $f \circ (g \circ h) = (f \circ g) \circ h$
- Identity: $\text{id} \circ f = f$
- Closure: $f \circ g \in \text{hom}_{R\text{-mod}}(A, A)$

Associativity: We have

$$\begin{aligned}
 f \circ (g \circ h) \curvearrowright x &:= (f \circ (g \circ h))(x) \\
 &= f((g \circ h)(x)) \\
 &= f(g(h(x))) \\
 &= (f \circ g)(h(x)) \\
 &= ((f \circ g) \circ h)(x) \\
 &:= (f \circ g) \circ h \curvearrowright x.
 \end{aligned}$$

Identity: Take $\text{id}_A : A \rightarrow A$ given by $\text{id}_A(x) = x$, then

$$f \circ \text{id}_A \curvearrowright x = f(\text{id}_A(x)) = f(x) = \text{id}_A(f(x)) = \text{id}_A \circ f \curvearrowright x.$$

Closure: If $f : A \rightarrow A$ and $g : A \rightarrow A$ are homomorphisms, then $f \circ g : A \rightarrow A$ as a set map, and is an R -module homomorphism because

$$\begin{aligned} f \circ g \curvearrowright (r + s)(x + y) &= f(g((r + s)(x + y))) \\ &= f((r + s)(g(x) + g(y))) \\ &= (r + s)(f(g(x)) + f(g(y))) \\ &= (f \curvearrowright (r + s)(x + y)) \circ (g \curvearrowright (r + s)(x + y)). \end{aligned}$$

3.3 Part 3

For arbitrary $x, y \in A$, we need to check the following:

- a. $f \curvearrowright (x + y) = f \curvearrowright x + f \curvearrowright y$
- b. $(f + g) \curvearrowright x = f \curvearrowright x + g \curvearrowright x$
- c. $f \circ g \curvearrowright x = f \curvearrowright (g \curvearrowright x)$
- d. $\text{id}_A \curvearrowright x = x$

For (a):

$$\begin{aligned} f \curvearrowright (x + y) &:= f(x + y) \\ &= f(x) + f(y) \quad \text{since } f \text{ is a homomorphism} \\ &= f \curvearrowright x + f \curvearrowright y \end{aligned}$$

For (b):

$$\begin{aligned} (f + g) \curvearrowright x &= (f + g)(x) \\ &= f(x) + g(x) \\ &= f \curvearrowright x + g \curvearrowright x. \end{aligned}$$

For (c):

$$\begin{aligned} f \circ g \curvearrowright x &= (f \circ g)(x) \\ &= f(g(x)) \\ &= f \curvearrowright g(x) \\ &= f \curvearrowright (g \curvearrowright x). \end{aligned}$$

For (d):

$$\text{id}_A \curvearrowright x = \text{id}_A(x) = x.$$

4 Problem 4

Injectivity: We have the following situation:

$$\begin{array}{ccccccc}
 & a' & & a & & x & & 0 \\
 & & & & & & & \\
 A_1 & \longrightarrow & A_2 & \longrightarrow & A_3 & \longrightarrow & A_4 \\
 \downarrow \alpha_1 & & \downarrow \alpha_2 & & \downarrow f & & \downarrow \alpha_4 \\
 B_1 & \longrightarrow & B_2 & \longrightarrow & B_3 & \longrightarrow & B_4 \\
 & & & & & & \\
 & 0 & & \alpha_2(a) & & y = f(x) = 0 & & 0
 \end{array}$$

where we would like to show that f is a monomorphism, i.e. that $\ker f = 0$. So let $x \in \ker f$, so $y := f(x) = 0 \in B_3$.

We will show that $x = 0 \in A_3$:

- Since $y = 0 \in B_3$, applying $B_3 \rightarrow B_4$ yields $y \mapsto 0 \in B_4$ since these maps are homomorphisms and always map zero to zero.
- Pull back $0 \in B_4$ to $0 \in B_3$ along α_4 , which can be done since α_4 is injective, giving $0 \in A_4$.
- Since this is 0 in A_4 , it is in the kernel of $A_3 \rightarrow A_4$, yielding some $x \in A_3$.
- By commutativity of the third square, $x \mapsto f(x)$ under $f : A_3 \rightarrow B_3$.
- Since $x \in \ker(A_3 \rightarrow A_4) = \text{im}(A_2 \rightarrow A_3)$ by exactness, there is some $a \in A_2$ such that $\alpha_2(a) = x \in A_3$.
- By injectivity of α_2 , a maps to a unique element $\alpha_2(a) \in B_2$.
- By commutativity of the middle square, since $a \in A_2 \mapsto 0 \in B_3$, we must have $\alpha_2(a) \mapsto 0 \in B_3$ under $B_2 \rightarrow B_3$.
- Then $\alpha_2(a) \in \ker(B_2 \rightarrow B_3) = \text{im}(B_1 \rightarrow B_2)$, so it pulls back to some $b \in B_1$.
- By surjectivity of α_1 , b pulls back to some $a' \in A_1$.
- By commutativity of square 1, $a' \mapsto a$ under $A_1 \rightarrow A_2$.
- So $a \mapsto x$ under $A_1 \rightarrow A_3$.
- But then $a \in \text{im}(A_1 \rightarrow A_2) = \ker(A_2 \rightarrow A_3)$, so $a \mapsto 0$ under $A_1 \rightarrow A_3$.
- So $x = 0$ as desired.

Surjectivity: We now have this situation:

$$\begin{array}{ccccccc}
 A_2 & \longrightarrow & A_3 & \longrightarrow & A_4 & \longrightarrow & A_5 \\
 \downarrow \alpha_2 & & \downarrow f & & \downarrow \alpha_4 & & \downarrow \alpha_5 \\
 B_2 & \longrightarrow & B_3 & \longrightarrow & B_4 & \longrightarrow & B_5
 \end{array}$$

Let $y \in B_3$; we want to then show that there exists an $x \in A_3$ such that $f(x) = y$.

- Apply $B_3 \rightarrow B_4$ to y to obtain $y_4 \in B_4$.
- By surjectivity of α_4 , this pulls back to some $a_4 \in A_4$.
- Also by exactness of $B_3 \rightarrow B_4 \rightarrow B_5$, y_4 pushes forward to $0 \in B_5$.
- By injectivity of α_5 , this pulls back to $0 \in A_5$.
- By commutativity of the right square, $y_4 \mapsto 0$ under $A_4 \rightarrow A_5$.
- Since $a_4 \in \ker(A_4 \rightarrow A_5)$, it pulls back to some $x \in A_3$ by exactness of $A_3 \rightarrow A_4 \rightarrow A_5$.
- Then $f(x) \in B_3$, and it remains to show that $f(x) = y$.
- By commutativity of the middle square, $f(x) \mapsto y_4$ under $B_3 \rightarrow B_4$.
- Since $a \mapsto y_4$ as well, we have $z := f(x) - y \in B_3$ maps to $0 \in B_4$.
- Since $z \in \ker(B_3 \rightarrow B_4)$, by exactness it pulls back to some $b_2 \in B_2$.
- By surjectivity of α_2 , this pulls back to some $a_2 \in A_2$.
- By commutativity of the first square, $a_2 \mapsto z \in B_3$.
- $a_2 \mapsto a_3 \in A_3$, where a_3 may not equal x , but $f(a_3) = z := f(x) - y$.
- Then $f(a_3) = f(x) - y \implies y = f(x) - f(a_3) = f(x - a_3)$ since f is a homomorphism.
- This shows that $x - a_3 \mapsto y$ under f , which is the element we wanted to produce.

5 Problem 5

5.1 Part (a)

We want to show that if $(p) \trianglelefteq R$ is a prime ideal then $R/(p)$ is a field, so we'll proceed by letting $x + (p) \in R/(p)$ be arbitrary where $x \notin (p)$ and producing a multiplicative inverse.

Since R is a principal ideal domain, prime ideals are maximal, so (p) is maximal. Then $x \in R \setminus (p)$, so define

$$I := \{p + rx \mid p \in (p), r \in R\} \trianglelefteq R,$$

which is an ideal in R .

In particular, since $x \notin (p)$, we have a strict containment $(p) < I$, but since (p) was maximal this forces $I = R$.

Then $1 \in I$, so there exists some p, r such that $p + rx = 1$, i.e. $rx - 1 \in (p)$.

But then

$$r + (p) \cdot x + (p) = rx + (p) = 1 + (p),$$

which says that $(x + (p))^{-1} = r + (p)$ in $R/(p)$.

5.2 Part (b)

Images and kernels of module homomorphisms are always submodules, so define

$$\begin{aligned}\phi : A &\rightarrow A \\ x &\mapsto px.\end{aligned}$$

This is a module homomorphism, and

$$\begin{aligned}\text{im } \phi &:= \{px \mid x \in A\} := pA, \\ \ker \phi &:= \{a \in A \mid pa = 0\} := A[p].\end{aligned}$$

5.3 Part (c)

Since $R/(p)$ is a field, we just need to show that $A/pA \curvearrowright R/(p)$ defines a module.

$$r \cdot (x + y) = rx + ry:$$

$$\begin{aligned}r + (p) \curvearrowright x + pA \oplus y + pA &:= r + (p) \curvearrowright x + y + pA \\ &:= r(x + y) + pA \\ &= rx + ry + pA \\ &:= rx + pA \oplus ry + pA \\ &:= r \curvearrowright x + pA \oplus r \curvearrowright y + pA.\end{aligned}$$

$$(r + s) \cdot x = rx + sx:$$

$$\begin{aligned}r + (p) \oplus s + (p) \curvearrowright x + pA &:= r + s + (p) \curvearrowright x + pA \\ &:= (r + s)x + pA \\ &= rx + sx + pA \\ &:= rx + pA \oplus sx + pA \\ &:= r + (p) \curvearrowright x + pA \oplus s + (p) \curvearrowright x + pA.\end{aligned}$$

$$rs \cdot x = r \cdot (s \cdot x):$$

$$\begin{aligned}r + (p) \cdot s + (p) \curvearrowright x + pA &:= rs + (p) \curvearrowright x + pA \\ &= rsx + pA \\ &:= r + (p) \curvearrowright sx + pA \\ &:= r + (p) \curvearrowright s + (p) \curvearrowright x + pA.\end{aligned}$$

$$1 \cdot x = x:$$

$$1_R + (p) \curvearrowright x + pA = 1_R x + pA = x + pA.$$

5.4 Part (d)

Similarly, since $R/(p)$ is a field, it suffices to show that $R/(p) \curvearrowright A[p]$ defines a module.

$$r \cdot (x + y) = rx + ry:$$

$$\begin{aligned} r + (p) \curvearrowright (a + a') &:= r(a + a') \\ &= ra + ra' \\ &= r \curvearrowright a + r \curvearrowright a'. \end{aligned}$$

$$(r + s) \cdot x = rx + sx:$$

$$\begin{aligned} r + s + (p) \curvearrowright a &= (r + s)a \\ &= ra + sa \\ &= r \curvearrowright a + s \curvearrowright a. \end{aligned}$$

$$rs \cdot x = r \cdot (s \cdot x):$$

$$\begin{aligned} rs + (p) \curvearrowright a &= rsa \\ &= r \curvearrowright sa \\ &= r \curvearrowright s \curvearrowright a. \end{aligned}$$

$$1 \cdot x = x:$$

$$1_R + (p) \curvearrowright a = 1a = a.$$

6 Problem 6

Supposing that $\dim V = n$, let $\mathcal{B} := \{\mathbf{b}_k \mid 1 \leq k \leq n\}$ be a basis for V , and define

$$\mathbf{e}_i := [0, 0, \dots, 1, \dots, 0] \in V^{\oplus m}$$

where the 1 occurs in the i th position. The claim is that $\mathcal{B}^m := \{\mathbf{e}_i \mathbf{b}_k \mid 1 \leq i \leq n, 1 \leq k \leq m\}$ forms a basis for $V^{\oplus m}$.

Elements in \mathcal{B}^m are of the form

$$\begin{aligned} & [\mathbf{b}_1, 0, 0, \dots, 0] \\ & [\mathbf{b}_2, 0, 0, \dots, 0] \\ & \dots \\ & [0, \mathbf{b}_1, 0, \dots, 0] \\ & [0, \mathbf{b}_2, 0, \dots, 0] \\ & \dots, \end{aligned}$$

and by construction, $|\mathcal{B}| = mn = m \dim V$.

To see that this is a spanning set, let $\mathbf{x} \in V^{\oplus m}$, so $\mathbf{x} = [\mathbf{v}_1, \mathbf{v}_2, \dots, \mathbf{v}_m]$ where each $\mathbf{v}_i \in V$.

Then each $\mathbf{v}_i \in \mathcal{B}$, so $\mathbf{v}_i = \sum_{k=1}^n \alpha_{k,i} \mathbf{b}_k$. But then

$$\mathbf{x} = \left[\sum_{k=1}^n \alpha_{k,1} \mathbf{b}_k, \sum_{k=1}^n \alpha_{k,2} \mathbf{b}_k, \dots, \sum_{k=1}^n \alpha_{k,m} \mathbf{b}_k \right] := \sum_{i=1}^m \sum_{k=1}^n \alpha_{k,i} \mathbf{b}_k \mathbf{e}_i,$$

which exhibits $\mathbf{x} \in \mathcal{B}^m$.

To see that it is linearly independent, supposing that $\mathbf{x} = \sum_i \sum_k \alpha_{k,i} \mathbf{b}_k \mathbf{e}_i = 0$, this says that $\mathbf{x} = [0, 0, \dots, 0]$, which forces $\sum_k \alpha_{k,i} \mathbf{b}_k$ to be zero for each i .

But for a fixed i , since $\{\mathbf{b}_k\}$ was a basis for V , this means that $\alpha_{k,i} = 0$ for all k . But then $\alpha_{k,i} = 0$ for all pairs i, k .

7 Problem 7