Section 10.2

3. Give an explicit example of a map from one R-module to another which is a group homomorphism but not an R-module homomorphism.

   Example:(Buchholz)

   Let $R = \mathbb{Z}[i]$ and view R as a module over itself. Let $\varphi : R \to R$ where $\varphi(a + bi) = a$. For φ to be an R-module homomorphism φ must be operation preserving with respect to addition and have the property that $r\varphi(r) = \varphi(r * r)$ for all $r \in R$.

   Now consider the elements $x = a_1 + b_1 i$, and $y = a_2 + b_2 i \in R$. We have

   $$\varphi(x + y) = a_1 + a_2 = \varphi(x) + \varphi(y).$$

   Hence φ is operation preserving with respect to addition. But,

   $$\varphi(i * i) = \varphi(-1) = -1$$

   and

   $$i\varphi(i) = i(0) = 0.$$

   Since $-1 \neq 0$, φ is not an R-module homomorphism. However, φ is a group homomorphism since φ is operation preserving with respect to addition.

5. Exhibit all $\mathbb{Z}$-module homomorphisms from $\mathbb{Z}/30\mathbb{Z}$ to $\mathbb{Z}/21\mathbb{Z}$.

   (Bastille) Note that $(30, 21) = 3$, so by Exercise 10.2.6,

   $$\mathrm{Hom}_{\mathbb{Z}}(\mathbb{Z}/30\mathbb{Z}, \mathbb{Z}/21\mathbb{Z}) = \{\sigma_k : \ \mathbb{Z}/30\mathbb{Z} \to \mathbb{Z}/21\mathbb{Z} \mid \sigma_k(\bar{1}) = 7k + 21\mathbb{Z}, 0 \leq k < 3\}.$$

   Concretely, there are 3 distinct $\mathbb{Z}$-module homomorphisms, entirely determined by:

   $$\sigma_1(\bar{1}) = \bar{7}, \qquad \sigma_2(\bar{1}) = \overline{14}, \qquad \sigma_3(\bar{1}) = \bar{0}.$$

6. Prove that $\mathrm{Hom}_{\mathbb{Z}}(\mathbb{Z}/n\mathbb{Z}, \mathbb{Z}/m\mathbb{Z}) \cong \mathbb{Z}/(n, m)\mathbb{Z}$.

   Proof. (Bastille) Consider $\mathrm{Hom}_{\mathbb{Z}}(\mathbb{Z}/n\mathbb{Z}, \mathbb{Z}/m\mathbb{Z})$ as an Abelian group under addition. Note that $\sigma \in \mathrm{Hom}_{\mathbb{Z}}(\mathbb{Z}/n\mathbb{Z}, \mathbb{Z}/m\mathbb{Z})$ if and only if the following applies:

   (a) $\sigma : \ \mathbb{Z}/n\mathbb{Z} \to \mathbb{Z}/m\mathbb{Z}$;

   (b) $\sigma(\bar{b} + \bar{c}) = \sigma(\bar{b}) + \sigma(\bar{c})$ for all $\bar{b}, \bar{c} \in \mathbb{Z}/n\mathbb{Z}$; since $\langle \bar{1} \rangle = \mathbb{Z}/n\mathbb{Z}$, note that satisfying condition (b) implies that σ is entirely determined by $\sigma(\bar{1})$;

   (c) σ is well-defined, i.e. in this case, we must have $\sigma(\bar{b}) = \sigma(\bar{c})$ whenever $\bar{b} = \bar{c}$.

   We claim that $\mathrm{Hom}_{\mathbb{Z}}(\mathbb{Z}/n\mathbb{Z}, \mathbb{Z}/m\mathbb{Z}) = S$ where

   $$S := \left\{\sigma_k : \ \mathbb{Z}/n\mathbb{Z} \to \mathbb{Z}/m\mathbb{Z} \mid \sigma_k \text{ satisfies (b) and } \sigma_k(\bar{1}) = k\frac{m}{(n, m)} + m\mathbb{Z}, \ k \in \mathbb{Z}, \ 0 \leq k < (n, m)\right\}.$$

   Denote $\bar{a} = \sigma(\bar{1})$. Since there are only m distinct cosets in $\mathbb{Z}/m\mathbb{Z}$, we can assume WLOG $0 \leq a < m$. If $\sigma \in \mathrm{Hom}_{\mathbb{Z}}(\mathbb{Z}/n\mathbb{Z}, \mathbb{Z}/m\mathbb{Z})$ then σ is well-defined, so in particular, since $\bar{0} = \bar{n}$ in $\mathbb{Z}/n\mathbb{Z}$, we must have in $\mathbb{Z}/m\mathbb{Z}$: $\bar{0} = \sigma(\bar{0}) = \sigma(\bar{n}) = \sigma(n\bar{1}) = n\sigma(\bar{1}) = n\bar{a}$. Hence $na = qm$ for some $q \in \mathbb{Z}$. Now we also have $n = (n, m)k_1$ for some $0 < k_1 \leq n$, and hence $a = \frac{q}{k_1}\frac{m}{(n,m)}$. Since $\frac{m}{(n,m)} \in \mathbb{Z}$, it must be that $\frac{q}{k_1}$ is also an integer. Furthermore since $0 \leq a < m$, it follows that $a = k\frac{m}{(n,m)}$ for k an integer such that $0 \leq k < (n, m)$. Hence $\sigma \in S$ and $\mathrm{Hom}_{\mathbb{Z}}(\mathbb{Z}/n\mathbb{Z}, \mathbb{Z}/m\mathbb{Z}) \subseteq S \quad (1)$.

Now if $\sigma_k \in S$, conditions (a) and (b) are met so we need only show that σ_k is well-defined. Assume $\bar{b}, \bar{c} \in \mathbb{Z}/n\mathbb{Z}$ such that $\bar{b} = \bar{c}$. Then $b = c + np$ for some $p \in \mathbb{Z}$ and

$$\begin{aligned}
\sigma_k(\bar{b}) = \sigma_k(b\bar{1}) = b\sigma_k(\bar{1}) &= (c+np)\left(k\frac{m}{(n,m)} + m\mathbb{Z}\right) = (c+np)k\frac{m}{(n,m)} + m\mathbb{Z} \\
&= ck\frac{m}{(n,m)} + npk\frac{m}{(n,m)} + m\mathbb{Z} = ck\frac{m}{(n,m)} + k_1pkm + m\mathbb{Z} = ck\frac{m}{(n,m)} + m\mathbb{Z} \\
&= c\left(k\frac{m}{(n,m)} + m\mathbb{Z}\right) = c\sigma_k(\bar{1}) = \sigma_k(\bar{c}).
\end{aligned}$$

Therefore $\sigma_k \in \mathrm{Hom}_{\mathbb{Z}}(\mathbb{Z}/n\mathbb{Z}, \mathbb{Z}/m\mathbb{Z})$ and $S \subseteq \mathrm{Hom}_{\mathbb{Z}}(\mathbb{Z}/n\mathbb{Z}, \mathbb{Z}/m\mathbb{Z})$ (2). Combining (1) and (2) leads to our claim. Now clearly $\sigma_k \neq \sigma_{k'}$ whenever $k \neq k^{'}$ where $0 \leq k, k^{'} < (n,m)$, so

$$|\mathrm{Hom}_{\mathbb{Z}}(\mathbb{Z}/n\mathbb{Z}, \mathbb{Z}/m\mathbb{Z})| = (n,m).$$

Note also that σ_1 generates $\mathrm{Hom}_{\mathbb{Z}}(\mathbb{Z}/n\mathbb{Z}, \mathbb{Z}/m\mathbb{Z})$ since for any $0 \leq k < (n,m)$, $\sigma_k = k\sigma_1$. Therefore as an additive group, $\mathrm{Hom}_{\mathbb{Z}}(\mathbb{Z}/n\mathbb{Z}, \mathbb{Z}/m\mathbb{Z})$ is Abelian and cyclic of order (n,m) so $\mathrm{Hom}_{\mathbb{Z}}(\mathbb{Z}/n\mathbb{Z}, \mathbb{Z}/m\mathbb{Z}) \cong \mathbb{Z}/(n,m)\mathbb{Z}$ and the isomorphism carries over to $\mathbb{Z}$-modules (since multiplication by an element of $\mathbb{Z}$ can be written as an addition), and so we have the desired result. $\square$

Comment: There are other ways to do this, though perhaps less concrete. Think about the way we talked about this problem before class last week.

Section 11.1

1. Let $V = \mathbb{R}^n$ and let $(a_1, a_2, \cdots, a_n)$ be a fixed vector in V. Prove that the collection D of elements $(x_1, x_2, \cdots, x_n) \in V$ where $a_1x_1 + a_2x_2 + \cdots + a_nx_n = 0$ is a subspace of V. Find the dimension and a basis of this subspace.

Proof. (Allman) For ease, let $\mathbf{a} = (a_1, \cdots, a_n) \in V$. If $\mathbf{a} = \mathbf{0}$, then $D = V$ and $\dim_{\mathbb{R}}(D) = n$. (Every vector in V is orthogonal to the zero vector.)

Now suppose that $\mathbf{a} \neq \mathbf{0}$, and define $W = \mathrm{Span}(\mathbf{a})$. Since $\mathbf{a} \in V$, W is a vector sub-space of V. Note that $\dim(W) = 1$. Define $W^{\perp} = D = \{v = (x_1, \ldots, x_n) \in V \mid a_1x_1 + \cdots + a_nx_n = 0\} = \{v \in V \mid \mathbf{a} \cdot v = \mathbf{0}\}$. (We say D is W *perp* meaning the collection of vectors perpendicular to all vectors in W.)

Claim: $W^{\perp} = D$ is a vector subspace of V of dimension $n-1$.

Clearly, the zero vector is an element of $W^{\perp}$. Suppose x, $y \in W^{\perp}$, then $\mathbf{a} \cdot (x+y) = \mathbf{a} \cdot x + \mathbf{a} \cdot y = \mathbf{0}$ and so the vector sum $x + y \in W^{\perp}$. Let $r \in \mathbb{R}$ be a scalar and $x \in W^{\perp}$, then $\mathbf{a} \cdot rx = r(\mathbf{a} \cdot x) = r\mathbf{0} = \mathbf{0}$. Thus, $rx \in W^{\perp}$ and W is a vector subspace of V.

For the 'Find' part of this problem, probably the most sophisticated way to proceed is to argue that $V = W \oplus W^{\perp}$. Notice if $w \in W \cap W^{\perp}$, then $\mathbf{a} \cdot w = \mathbf{0}$ and $w = r\mathbf{a}$ for some scalar $r \in \mathbb{R}$. Thus,

$$\mathbf{a} \cdot w = \mathbf{a} \cdot r\mathbf{a} = r(\mathbf{a} \cdot \mathbf{a}) = \mathbf{0}.$$

Now if $r = 0$, then w is the zero vector. If $r \neq 0$, then we must have that $\mathbf{a} \cdot \mathbf{a} = 0$. But this is a contradiction since only the zero vector satisfies $\mathbf{a} \cdot \mathbf{a} = 0$. (Only the zero vector has length zero.) Thus, the only vector in the intersection $W \cap W^{\perp}$ is the zero vector.

To obtain a basis for $V^{\perp}$, start with a basis $\mathcal{B}' = \{v_1, v_2', \cdots, v_n'\}$ for V with the first basis vector given by $v_1 = \mathbf{a}$ and then extend to a basis for V. You can use Gram-Schmidt or just general ideas on projections to replace the basis elements $v_2', \ldots, v_n'$ with $v_2, \ldots, v_n$ which are orthogonal to $v_1 = \mathbf{a}$. Thus, $\mathcal{B} = \{v_1, v_2, \cdots, v_n\}$ is a basis for $V = W \oplus W^{\perp}$.

More concretely, to show $\dim_{\mathbb{R}}(W^{\perp}) = n-1$ for $\mathbf{a} \neq \mathbf{0}$, we can without loss of generality assume that the last coordinate a_n of $\mathbf{a}$ is non-zero, $a_n \neq 0$. Then for any choice of real numbers, $x_1, \cdots, x_{n-1}$, let $x_n = \frac{-1}{a_n}(a_1x_1 + \cdots + a_{n-1}x_{n-1})$ and $x = (x_1, \ldots, x_n)$. It is easy to check that $\mathbf{a} \cdot x = 0$ and so $x \in W^{\perp}$. Finally, since there were $n-1$ free choices $(x_1, \ldots, x_{n-1})$, this means that $\dim_{\mathbb{R}}(W^{\perp}) = n-1$. $\square$

2. Let V be the collection of polynomials with coefficients in $\mathbb{Q}$ in the variable x of degree at most 5. Prove that V is a vector space over $\mathbb{Q}$ of dimension 6, with $1, x.x^2, \ldots, x^5$ as a basis. Prove that $1, 1+x, 1+x+x^2, \ldots, 1+x+x^2+x^3+x^4+x^5$ is also a basis for V.

   Proof. (Allman/Gillispie) By definition we know that $\{1, x, x^2, \ldots x^5\} = \mathcal{A}$ is a linearly independent subset of $\mathbb{Q}[x]$, which was shown to span a vector space in e.g. 11.1.1.

   Moreover, letting $p(x) \in V$, by definition $p(x) = p_5x^5 + p_4x^4 + p_3x^3 + p_2x^2 + p_1x + p_0$ where $p_i \in \mathbb{Q}$, we see that $\mathcal{A}$ spans V. Thus, $\mathcal{A}$ is a basis for V. Since $|\mathcal{A}| = 6$, $\dim_{\mathbb{Q}}(V) = 6$.

   Let $\mathcal{B} = \{1, 1+x, 1+x+x^2, \ldots, 1+x+x^2+x^3+x^4+x^5\}$.

   Note that

$$\begin{aligned}
1 &= 1 \\
x &= -1(1) + 1(1+x) \\
x^2 &= -1(1+x) + 1(1+x+x^2) \\
&\vdots \\
x^5 &= -1(1+x+x^2+x^3+x^4) + 1(1+x+x^2+x^3+x^4+x^5).
\end{aligned}$$

   That is, each basis element in $\mathcal{A}$ can be expressed as a linear combination of elements in $\mathcal{C}$ and vice versa.

   It follows that $\mathcal{C}$ is also a basis for V. $\square$

3. Let φ be the linear transformation $\varphi : \mathbb{R}^4 \to \mathbb{R}$ such that
   $\varphi((1,0,0,0)) = 1$ $\quad$ $\varphi((1,-1,0,0)) = 0$
   $\varphi((1,-1,1,0)) = 1$ $\quad$ $\varphi((1,-1,1,-1)) = 0$.
   Determine $\varphi((a,b,c,d))$.

   (Baggett) We have that
   $-d(1,-1,1,-1) + (c+d)(1,-1,1,0) + (-b-c)(1,-1,0,0) + (a+b)(1,0,0,0)$
   $= (-d+c+d-b-c+a+b, d-c-d+b+c, -d+c+d, d)$
   $= (a,b,c,d)$.

   Thus,
   $\varphi((a,b,c,d)) = \varphi(-d(1,-1,1,-1) + (c+d)(1,-1,1,0) + (b-c)(1,-1,0,0) + (a+b)(1,0,0,0))$
   $= -d\varphi((1,-1,1,-1)) + (c+d)\varphi((1,-1,1,0)) + (-b-c)\varphi((1,-1,0,0)) + (a+b)\varphi((1,0,0,0))$
   $= -d(0) + (c+d)(1) + (-b-c)(0) + (a+b)(1)$
   $= a+b+c+d$.

8. Let V be a vector space over F and let φ be a linear transformation of the vector space V to itself. A nonzero element $v \in V$ satisfying $\varphi(v) = \lambda v$ for some $\lambda \in F$ is called an *eigenvector* of φ with *eigenvalue* λ. Prove that for any fixed $\lambda \in F$ the collection of eigenvectors of φ with eigenvalue λ together with 0 forms a subspace of V.

   Proof. (Mobley) Let W be the collection of eigenvectors of φ with eigenvalue λ together with 0. Let $x, y \in W$. Also let $r \in F$. Then for $(rx+y) \in V$, we have that $\varphi(rx+y) = \varphi(rx)+\varphi(y) = r\varphi(x)+\varphi(y)$, since φ is a linear transformation of V.

   Moreover, since x and y are eigenvectors, $r\varphi(x) + \varphi(y) = r\lambda x + \lambda y = \lambda(rx+y) = \lambda\varphi(rx+y)$. Hence, $(rx+y) \in W$ and W is a subspace of V. $\square$

9. Let V be a vector space over F and let φ be a linear transformation of the vector space V to itself. Suppose for $i = 1, 2, \ldots, k$ that $v_i \in V$ is an eigenvector for φ with eigenvalue $\lambda_i \in F$ and that all the eigenvalues λ_i are distinct. Prove that $v_1, v_2, \ldots, v_k$ are linearly independent. Conclude that any linear transformation on an n-dimensional vector space has at most n distinct eigenvalues.

Proof. (Schamel) We shall proceed by induction on the number of distinct eigenvalues. Note that when $k = 1$, if $a_1 v_1 = 0$ for some $a_1 \in F$ then $a_1 = 0$ since $v_1 \neq 0$ and F is a field. Hence $\{ v_1 \}$ is linearly independent. Suppose any k eigenvectors of φ with distinct eigenvalues are linearly independent and consider the collection $\{ v_i \}_{i=1}^{k+1}$ of eigenvectors of φ with distinct eigenvalues. Suppose $\sum_{i=1}^{k+1} a_i v_i = 0$ for some $a_1, \ldots, a_{k+1} \in F$. But then, applying φ to both sides of the equation yields $\sum_{i=1}^{k+1} a_i \lambda_i v_i = 0$ and we see

$$0 = \sum_{i=1}^{k+1} a_i \lambda_i v_i - \lambda_{k+1} \left(\sum_{i=1}^{k+1} a_i v_i \right) = \sum_{i=1}^{k} a_i (\lambda_i - \lambda_{k+1}) v_i.$$

However, since $\{ v_i \}_{i=1}^{k}$ is linearly independent by hypothesis, we have $a_i(\lambda_i - \lambda_{k+1}) = 0$ for all $1 \leq i \leq k$. Each eigenvalue is distinct, so $(\lambda_i - \lambda_{k+1}) \neq 0$ for all $1 \leq i \leq k$ and thus $a_i = 0$ for $1 \leq i \leq k$. Going back to our original linear independence condition, we now have $a_{k+1} v_{k+1} = 0$, so $a_{k+1} = 0$ since $v_{k+1} \neq 0$. We conclude $\{ v_i \}_{i=1}^{k+1}$ is linearly independent and by induction any set of k eigenvectors of φ with distinct eigenvalues is linearly independent. Hence any linear transformation on an n-dimensional vector space has at most n distinct eigenvalues, for otherwise it would contain a linearly independent set of vectors of order greater than n. □

Section 11.2

1. Let V be the collection of polynomials with coefficients in $\mathbb{Q}$ in the variable x of degree at most 5. Determine the transition matrix from the basis $1, x, x^2 \ldots, x^5$ for V to the basis $1, 1 + x, 1 + x + x^2, \ldots, 1 + x + x^2 + x^3 + x^4 + x^5$ for V.

   (Hazlett)

   Note, $1 = (1)1, 1 + x = -1(1) + 1(1 + x), 1 + x + x^2 = -1(1 + x) + 1(1 + x + x^2), \ldots,$ and $1 + x + x^2 + x^3 + x^4 + x^5 = -1(1 + x + x^2 + x^3 + x^4) + 1(1 + x + x^2 + x^3 + x^4 + x^5)$. Therefore, the transition matrix from the basis $1, x, x^2 \ldots, x^5$ for V to the basis $1, 1 + x, 1 + x + x^2, \ldots, 1 + x + x^2 + x^3 + x^4 + x^5$ will be:

$$\begin{pmatrix} 1 & -1 & 0 & 0 & 0 & 0 \\ 0 & 1 & -1 & 0 & 0 & 0 \\ 0 & 0 & 1 & -1 & 0 & 0 \\ 0 & 0 & 0 & 1 & -1 & 0 \\ 0 & 0 & 0 & 0 & 1 & -1 \\ 0 & 0 & 0 & 0 & 0 & 1 \end{pmatrix}$$

2. (Lawless) Let V be the vector space of the preceding exercise. Let $\varphi = d/dx$ be the linear transformation of V to itself given by usual differentiation of a polynomial with respect to x. Determine the matrix of φ with respect to the two bases for V in the previous exercise.

   The differentiation matrix will have as its ith column the coordinates of the image if the ith basis element under the differentiation map. For example, $x^4 \mapsto 4x^3$, so the 5th column of the matrix with respect to the first basis will have a 4 in the 4th row, and zeros elsewhere. The other columns are defined similarly, as is the matrix with respect to the second basis.

   The matrix with respect to the first basis:

$$\begin{bmatrix} 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 2 & 0 & 0 & 0 \\ 0 & 0 & 0 & 3 & 0 & 0 \\ 0 & 0 & 0 & 0 & 4 & 0 \\ 0 & 0 & 0 & 0 & 0 & 5 \\ 0 & 0 & 0 & 0 & 0 & 0 \end{bmatrix}$$

The matrix with respect to the second basis:

$$\begin{bmatrix} 0 & 1 & -1 & -1 & -1 & -1 \\ 0 & 0 & 2 & -1 & -1 & -1 \\ 0 & 0 & 0 & 3 & -1 & -1 \\ 0 & 0 & 0 & 0 & 4 & -1 \\ 0 & 0 & 0 & 0 & 0 & 5 \\ 0 & 0 & 0 & 0 & 0 & 0 \end{bmatrix}$$

4. Let φ be the linear transformation of $\mathbb{R}^2$ to itself given by rotation counterclockwise around the origin through an angle θ. Show that the matrix of φ with respect to the standard basis for $\mathbb{R}^2$ is:

$$\begin{pmatrix} \cos\theta & -\sin\theta \\ \sin\theta & \cos\theta \end{pmatrix}$$

Proof (Granade). Let $e_1, e_2 \in \mathbb{R}^2$ be the elements of the standard basis $\mathcal{B}$. That is, let e_1, e_2 have coordinates: $e_1 = \begin{pmatrix} 1 \\ 0 \end{pmatrix}_{\mathcal{B}}$ and $e_2 = \begin{pmatrix} 0 \\ 1 \end{pmatrix}_{\mathcal{B}}$. Then, e_1 has unit length and makes an angle of 0 with the $\hat{x}$-axis, and so $\varphi(e_1) = \begin{pmatrix} \cos\theta \\ \sin\theta \end{pmatrix}_{\mathcal{B}}$. Similarly, e_2 has unit length and makes an angle of $\pi/2$ with the $\hat{x}$-axis, and so $\varphi(e_2) = \begin{pmatrix} \cos(\theta + \pi/2) \\ \sin(\theta + \pi/2) \end{pmatrix}_{\mathcal{B}} = \begin{pmatrix} -\sin\theta \\ \cos\theta \end{pmatrix}_{\mathcal{B}}$ by the sum of angle identities for sine and cosine:

$$\begin{aligned} \cos\left(\theta + \frac{\pi}{2}\right) &= \cos\theta\cos\frac{\pi}{2} - \sin\theta\sin\frac{\pi}{2} \\ &= 0\cos\theta - 1\sin\theta \\ \sin\left(\theta + \frac{\pi}{2}\right) &= \sin\theta\cos\frac{\pi}{2} + \cos\theta\sin\frac{\pi}{2} \\ &= 0\sin\theta + 1\cos\theta \end{aligned}$$

Thus, since the action of φ on the basis has been established, we can write the matrix $(M_\varphi)_{\mathcal{B}}$:

$$\begin{pmatrix} \cos\theta & -\sin\theta \\ \sin\theta & \cos\theta \end{pmatrix}$$

$\square$