Math 540 Homework 6 *Stephen Cornelius*

1. Let V be a vector space and $V_j < V$, $j = 1, \dots, k$ subspaces.

   (a) **Definition:** We say that V is a direct sum (denoted $V = V_1 \oplus V_2 \oplus \cdots \oplus V_k$) of the subspaces V_j if every $v \in V$ can be written uniquely as $v = v_1 + v_2 + \cdots + v_k$ with $v_j \in V_j$.

   (b) *Proof.* ($1 \implies 2$): Let V be the direct sum of the subspaces V_j. Then for any $v \in V$, there exist unique $v_j \in V_j$ such that $v = v_1 + v_2 + \cdots + v_k$. Define the projectors $P_j : V \to V_j$ by $P_j(v) = v_j$. Then we have

   $$(P_1 + P_2 + \cdots + P_k)(v) = P_1(v) + P_2(v) + \cdots + P_k(v) = v_1 + v_2 + \cdots + v_k = v,$$

   so $Id_V = P_1 + P_2 + \cdots + P_k$. Furthermore, for $i \neq j$, we have

   $$P_i(P_j(v)) = P_i(v_j) = 0,$$

   since $v_j \in V_j$ and P_i projects onto V_i. Thus, $P_i \circ P_j = 0$ for $i \neq j$.
   ($2 \implies 1$): Now suppose there exist projectors P_i on the subspaces V_i such that $Id_V = P_1 + P_2 + \cdots + P_k$ and $P_i \circ P_j = 0$ for $i \neq j$. For any $v \in V$, we can write

   $$v = Id_V(v) = (P_1 + P_2 + \cdots + P_k)(v) = P_1(v) + P_2(v) + \cdots + P_k(v).$$

   Since each $P_i(v) \in V_i$, this expresses v as a sum of elements from the subspaces V_i. To show uniqueness, suppose

   $$v = v_1 + v_2 + \cdots + v_k = w_1 + w_2 + \cdots + w_k,$$

   with $v_i, w_i \in V_i$. Applying P_j to both sides, we get

   $$P_j(v) = P_j(v_1 + \cdots + v_k) = v_j,$$

   and similarly

   $$P_j(v) = P_j(w_1 + \cdots + w_k) = w_j.$$

   Hence, $v_j = w_j$ for all j, proving uniqueness. Therefore, $V = V_1 \oplus V_2 \oplus \cdots \oplus V_k$. □

   (c) *Proof.* ($1 \implies 2$): Suppose $V = \bigoplus_{\lambda \in \text{spec}(T)} V_\lambda$. For each eigenvalue λ, define the projector $P_\lambda : V \to V_\lambda$ by projecting onto the eigenspace V_λ. Then, by the direct sum property, we have

   $$Id_V = \sum_{\lambda \in \text{spec}(T)} P_\lambda,$$

   and for $\lambda \neq \mu$, $P_\lambda \circ P_\mu = 0$. Furthermore, for any $v \in V$,

   $$T(v) = T\left(\sum_\lambda P_\lambda(v)\right) = \sum_\lambda T(P_\lambda(v)) = \sum_\lambda \lambda P_\lambda(v),$$

   so

   $$T = \sum_\lambda \lambda P_\lambda.$$

   ($2 \implies 1$): Now suppose there exist projectors P_λ satisfying the given conditions. For any $v \in V$, we can write

   $$v = Id_V(v) = \sum_\lambda P_\lambda(v).$$

   Each $P_\lambda(v) \in V_\lambda$, so this expresses v as a sum of elements from the eigenspaces. To show uniqueness, suppose

   $$v = v_{\lambda_1} + v_{\lambda_2} + \cdots + v_{\lambda_k} = w_{\lambda_1} + w_{\lambda_2} + \cdots + w_{\lambda_k},$$

with $v_{\lambda_i}, w_{\lambda_i} \in V_{\lambda_i}$. Applying P_μ to both sides, we get

$$P_\mu(v) = P_\mu(v_{\lambda_1} + \cdots + v_{\lambda_k}) = v_\mu,$$

and similarly

$$P_\mu(v) = P_\mu(w_{\lambda_1} + \cdots + w_{\lambda_k}) = w_\mu.$$

Hence, $v_\mu = w_\mu$ for all μ, proving uniqueness. Therefore, $V = \bigoplus_{\lambda \in \mathrm{spec}(T)} V_\lambda$. Moreover, for each $\mu \in \mathrm{spec}(T)$, we can express P_μ as

$$P_\mu = \prod_{\substack{\lambda \in \mathrm{spec}(T) \\ \lambda \neq \mu}} \left(\frac{T - \lambda \cdot Id}{\mu - \lambda} \right),$$

which follows from the properties of the projectors and the definition of the eigenspaces. ☐

2. Let $\mathbb{F}$ be a field.

   (a) **Definition:** The ring $\mathbb{F}[X]$ of polynomials with coefficients in $\mathbb{F}$ is the set of all expressions of the form

   $$p(X) = a_n X^n + a_{n-1} X^{n-1} + \cdots + a_1 X + a_0,$$

   where $n \geq 0$, $a_i \in \mathbb{F}$, and X is an indeterminate. Addition and multiplication are defined in the usual way for polynomials.

   (b) *Proof.* To show that $\dim(\mathbb{F}[X])$ is infinite, we need to demonstrate that there is no finite basis for the vector space $\mathbb{F}[X]$. Consider the set of monomials $\{1, X, X^2, X^3, \ldots\}$. This set is linearly independent because no finite linear combination of these monomials can equal zero unless all coefficients are zero.

   Furthermore, any polynomial in $\mathbb{F}[X]$ can be expressed as a finite linear combination of these monomials. Since we can find infinitely many linearly independent vectors (the monomials), it follows that the dimension of $\mathbb{F}[X]$ is infinite. ☐

   (c) *Proof.* Let R be a ring and $R[X]$ the ring of polynomials with coefficients in R.

      i. Let $f, g \in R[X]$ with $\deg(f) = m$ and $\deg(g) = n$. Then we can write

      $$f = a_m X^m + a_{m-1} X^{m-1} + \cdots + a_0,$$

      $$g = b_n X^n + b_{n-1} X^{n-1} + \cdots + b_0,$$

      where $a_m, b_n \neq 0$. The product fg is given by

      $$fg = (a_m X^m + \cdots)(b_n X^n + \cdots) = a_m b_n X^{m+n} + (\text{lower degree terms}).$$

      If the characteristic of R is such that $a_m b_n \neq 0$, then $\deg(fg) = m + n$. However, if $a_m b_n = 0$, then the highest degree term may cancel out, leading to $\deg(fg) < m + n$. Thus, we have

      $$\deg(fg) \leq \deg(f) + \deg(g).$$

      In an integral $a_m \times b_n = 0$ implies that either $a_m = 0$ or $b_n = 0$ by definition, which contradicts our assumption. Therefore, in an integral domain, we have equality:

      $$\deg(fg) = \deg(f) + \deg(g).$$

      ii. Let $f, g \in R[X]$ with $\deg(f) = m$ and $\deg(g) = n$. Without loss of generality, assume $m \geq n$. Then we can write

      $$f = a_m X^m + a_{m-1} X^{m-1} + \cdots + a_0,$$
      $$g = b_n X^n + b_{n-1} X^{n-1} + \cdots + b_0,$$

The sum $f+g$ is given by

$$\begin{aligned} f+g &= (a_m X^m + \cdots) + (b_n X^n + \cdots) \\ &= a_m X^m + \cdots + b_n X^n + \cdots . \end{aligned}$$

If $a_m + b_n \neq 0$, then $\deg(f+g) = m$. If $a_m + b_n = 0$, then the highest degree term cancels out, and we need to consider the next highest degree terms. In any case, we have $\deg(f+g) \leq \max(\deg(f), \deg(g))$, as desired.

$\square$

3. Let $\varphi : R \to S$ be a homomorphism of rings.

   (a) **Definition:** The kernel of a ring homomorphism $\varphi : R \to S$ is defined as $\ker(\varphi) = \{a \in R \mid \varphi(a) = 0\}$.

   (b) *Proof.* To show that φ is injective if and only if $\ker(\varphi) = \{0\}$, we proceed as follows:

   ($\Longrightarrow$) Suppose φ is injective. Then for any $a \in \ker(\varphi)$, we have $\varphi(a) = 0$. Since φ is injective, the only element that maps to 0 in S is 0 itself. Therefore, $a = 0$, and thus $\ker(\varphi) = \{0\}$.

   ($\Longleftarrow$) Now suppose $\ker(\varphi) = \{0\}$. To show that φ is injective, let $a, b \in R$ such that $\varphi(a) = \varphi(b)$. Then,

   $$\varphi(a) - \varphi(b) = 0 \implies \varphi(a-b) = 0.$$

   Since $a - b \in \ker(\varphi)$ and $\ker(\varphi) = \{0\}$, it follows that $a - b = 0$, or equivalently, $a = b$. Thus, φ is injective.

   Therefore, we conclude that φ is injective if and only if $\ker(\varphi) = \{0\}$. $\square$

4. Suppose R is a ring.

   (a) **Definition:** A ring R is said to be a ring with unit (or unital ring) if there exists an element $1_R \in R$ such that for all $a \in R$, we have $1_R \cdot a = a \cdot 1_R = a$.

   (b) *Proof.* Suppose that $a \in R$ is invertible. Suppose, for a contradiction, that there exist $b, c \in R$ inverses for a with $b \neq c$. Then we have that

   $$\begin{aligned} 1_R &= a \cdot b \\ \implies c \cdot 1_R &= c \cdot (a \cdot b) \\ c &= (c \cdot a) \cdot b \\ c &= 1_R \cdot b \\ \implies c &= b \end{aligned}$$

   a contradiction as we assumed that $b \neq c$. Therefore we have that for $a \in R$ invertible there exists a unique inverse. $\square$

   (c) The invertible elements of $\mathbb{Z}_{12}$ will be all of the elements that are coprime to 12. These elements are 1, 5, 7, and 11. Thus, the invertible elements in the ring $\mathbb{Z}_{12}$ are $\{1, 5, 7, 11\}$. The inverses are as follows:

Element	Inverse
1	1
5	5
7	7
11	11

5. Let $\varphi : R \to S$ be a homomorphism of rings.

   (a) **Definition:** A subset $R' \subseteq R$ is called a subring of R if R' is itself a ring under the operations of addition and multiplication defined on R and is nonempty.

   (b) *Proof.* First we show that $\mathrm{Im}(\varphi)$ is a subring of S. To do this we will show that for any $x, y \in \mathrm{Im}(\varphi)$, $x - y \in \mathrm{Im}(\varphi)$ and $xy \in \mathrm{Im}(\varphi)$.
   Let $x, y \in \mathrm{Im}(\varphi)$. Then there exist $a, b \in R$ such that $\varphi(a) = x$ and $\varphi(b) = y$. We have that

$$x - y = \varphi(a) - \varphi(b) \overset{\varphi \text{ is homomorphism}}{=} \varphi(a - b) \in \mathrm{Im}(\varphi),$$

   and

$$xy = \varphi(a)\varphi(b) \overset{\varphi \text{ is homomorphism}}{=} \varphi(ab) \in \mathrm{Im}(\varphi).$$

   Thus, $\mathrm{Im}(\varphi)$ is closed under subtraction and multiplication, and since it is nonempty (it contains $\varphi(0_R) = 0_S$), it is a subring of S.
   Next, we show that $\ker(\varphi)$ is a subring of R. Recall that

$$\ker(\varphi) = \{a \in R \mid \varphi(a) = 0_S\}.$$

   Let $a, b \in \ker(\varphi)$. Then

$$\varphi(a - b) = \varphi(a) - \varphi(b) = 0_S - 0_S = 0_S,$$

   so $a - b \in \ker(\varphi)$. Also,

$$\varphi(ab) = \varphi(a)\varphi(b) = 0_S \cdot 0_S = 0_S,$$

   so $ab \in \ker(\varphi)$. Since $\ker(\varphi)$ contains 0_R and is closed under subtraction and multiplication, it is a subring of R. $\square$