Math 371 / Problem Set 4 (two pages)

Polynomial functions

Let \( R \subset S \) be rings with identity, and \( R[X] \) be the ring of polynomials in the variable \( X \) over \( R \). Further let \( \mathcal{F}(S,S) \) be the ring of all the maps from \( f : S \to S \) as introduced at Problem 6 of Problem Set 3.

1) Prove / answer the following:

a) For every \( \alpha \in S \) there exists a unique ring homomorphism \( \phi_\alpha : R[X] \to S \) such that \( \phi_\alpha(a) = a \) for all \( a \in R \), and \( \phi_\alpha(X) = \alpha \).

b) What is \( \text{Ker}(\phi_\alpha) \) for \( \alpha = 0 \) and \( \alpha = 1 \)? And what is \( \text{Ker}(\phi_\alpha) \) for arbitrary \( \alpha \in R \)?

[\text{Hint:} \text{Prove by induction that } \phi_\alpha(X^m) = \alpha^m \text{ for all } m; \text{ hence } \phi_\alpha(aX^m) = a\alpha^m \text{ for all } a \in R \text{ and all } m; \text{ hence by induction, if } p(X) = a_0 + a_1X + \ldots + a_nX^n, \text{ then } \phi_\alpha(p(X)) = a_0 + a_1\alpha + \ldots + a_n\alpha^n, \text{ etc.}]

[\text{Language: If } p(X) \in R[X] \text{ is a polynomial, we denote } p(\alpha) := a_0 + a_1\alpha + \ldots + a_n\alpha^n = \phi_\alpha(p(X)), \text{ and call it the value or the evaluation of } p(X) \text{ at } X = \alpha.]

Define \( \phi : R[X] \to \mathcal{F}(S,S) \), by \( p(X) \mapsto f_{p(X)} \), where \( f_{p(X)} : S \to S, \alpha \mapsto f_{p(X)}(\alpha) := p(\alpha) \) for all \( \alpha \in S \).

[\text{Language: The function } f_{p(X)} : S \to S \text{ defined by } f_{p(X)}(\alpha) := p(\alpha) \text{ for all } \alpha \in S, \text{ is called the polynomial function on } S \text{ defined by } p(X).]

2) In the above notations, answer the following:

a) Show that \( \phi \) is a ring homomorphism.

b) Analyze the injectivity/surjectivity of \( \phi : R[X] \to \mathcal{F}(R,R) \) in the following cases:

i) \( R = \mathbb{Q} \), \( R = \mathbb{R} \), \( R = \mathbb{C} \).

ii) \( R = \mathbb{Z}/m\mathbb{Z} \) for \( m = 2, 3, 4, 5, 6, 7 \).

Modules and vector spaces

3) Let \( M \) be an \( R \)-module, and \( N \subseteq M \) a non-empty subset. Prove that the following assertions are equivalent:

a) \( N \) is an \( R \)-submodule of \( M \).

b) For all \( x, y \in N \) and \( r \in R \) one has: \( x - y \in N \) and \( rx \in N \).

c) For all \( x, y \in N \) and \( r, s \in R \) one has: \( rx + sy \in N \).

4) Let \( M_1, M_2 \) be \( R \)-modules, and consider \( M := M_1 \times M_2 \) viewed as an abelian group w.r.t. the component wise addition. Prove/answer the following:

a) Via the outer multiplication \( r(x_1, x_2) := (rx_1, rx_2) \), \( M \) becomes an \( R \)-module.

b) Let \( N_i \subseteq M_i, \ i = 1, 2, \) be subsets, and set \( N := N_1 \times N_2 \) viewed as subset of \( M = M_1 \times N_2 \). Then \( N \subset M \) is an \( R \)-submodule iff \( N_1 \subseteq M_1 \) and \( N_2 \subseteq M_2 \) are so.

c) Is the same correspondingly true, for \( n \) modules \( M_1, \ldots, M_n \) and their product \( M = M_1 \times \ldots \times M_n \) endowed with the component wise addition?

5) Answer the following:

a) Let \( V \) be an \( F \)-vector space. Show that for all \( \alpha \in F \) and \( v \in V \) one has: \( \alpha v = 0 \iff \alpha = 0 \text{ or } v = 0 \).

b) Is the same true for all rings \( R \) with \( 1_R \neq 0_R \) and all \( R \)-modules \( M \)?

6) Let \( \mathcal{P}ol(\mathbb{R}) \subset \mathcal{F}(\mathbb{R}, \mathbb{R}) \) be the set of all the polynomial functions. Prove or disprove:

a) The set \( V_0 = \{ f \in \mathcal{P}ol(\mathbb{R}) \mid f(0) = 0 \} \) is an \( \mathbb{R} \)-vector space, which is not finitely generated.

b) Is the same is true for the set \( V_1 = \{ f \in \mathcal{P}ol(\mathbb{R}) \mid f(1) = 1 \} ? \)
7) Answer the following:
   a) Let $V = \mathbb{Q}^2$ be viewed as a $\mathbb{Q}$-vector space. Describe all the $\mathbb{Q}$-subspaces of $V$.
   b) Let $M = \mathbb{Z}^2$ be viewed as a $\mathbb{Z}$-module. Describe all the $\mathbb{Z}$-submodules of $V$.

8) Prove or disprove the following:
   a) $(\mathbb{Q}, +)$ is not a finitely generated $\mathbb{Z}$-module.
   b) $(\mathbb{R}, +)$ is not a finitely generated $\mathbb{Q}$-vector space.
   c) $(\mathbb{C}, +)$ is not a finitely generated $\mathbb{R}$-vector space.