MATH 100B: Homework #6

Due on Feb 22, 2024 at 12:00pm

Professor McKernan

Section A02 6:00PM - 6:50PM
Section Leader: Castellano-Macías

Source Consulted: Textbook, Lecture, Discussion, Office Hour

Ray Tsai

A16848188

Problem 1

Let M be an R-module and let $r \in R$. Show that the map

$$\phi : M \to M \quad \text{given by} \quad m \mapsto rm$$

is R-linear.

Proof. Let $m, n \in M$, and let $s \in R$. Since $\phi(m+n) = r(m+n) = rm + rn = \phi(m) + \phi(n)$, and $\phi(sm) = rsm = s\phi(m)$, ϕ is R-linear. $\square$

Problem 2

Prove that a subset N of an R-module is a submodule if and only if it is non-empty and closed under addition and scalar multiplication.

Proof. If N is a submodule, then N is an additive subgroup closed under scalar multiplication, by definition. Hence, it suffices to show the converse. Let $m, n \in N$ and $r, s \in R$. Since N is closed under scalar multiplication, $-1 \cdot m = -m \in N$. Since N is both closed under addition and taking inverses, N is an additive subgroup, and N is obviously abelian as it is a subset of an R-module. Since m, n are elements in an R-module, $1 \cdot m = m$, $(rs) \cdot m = r \cdot (s \cdot m)$, $(r + s) \cdot m = r \cdot m + s \cdot m$, and $r \cdot (m + n) = r \cdot m + r \cdot n$. However, N is closed under addition and scalar multiplication, so $r \cdot (s \cdot m), r \cdot m + s \cdot m, r \cdot m + r \cdot n \in N$. The result now follows. □

Problem 3

Let $\phi : M \to N$ be an R-linear map between two R-modules. Prove that the kernel of ϕ is a submodule of M.

Proof. Let K be the kernel of ϕ. Note that ϕ is a group homomorphism, so K is an additive subgroup. It suffices to check that K is closed under scalar multiplication. Let $m \in K$, and let $r \in R$. Since $\phi(rm) = r\phi(m) = r \cdot 0 = 0$, $rm \in K$, and we are done. $\square$

Problem 4

Let M be an R-module. Prove that the intersection of any set of submodules is a submodule.

Proof. Let S be a set of submodules of M, and let $N = \bigcap_{A \in S} A$. It suffices to check that N is nonempty, closed under addition and scalar multiplication. Let $m, n \in N$, and let $r \in R$. For all $A \in S$, $0, m+n, rm \in A$, and thus $0, m + n, rm \in N$. $\square$

Problem 5

Let M be an R-module and let X be any subset of M. Prove the existence of the submodule generated by X.

Proof. Let N be the intersection of all submodules of M that contains X. N contains X and any other submodules that contains X also contains N. The result now follows from N. $\square$

Problem 6

Let M be an R-module and let X be any set. Show how the set of all maps from X to M becomes an R-module.

Proof. Let S be the set of all maps $X \to M$. Since the map $e : X \to M$ which maps every element to 0 is in S, S is nonempty. Let $f, g \in S$. Since M is associative, commutative, and closed under addition, $f + g$ is still a mapping from X to M, and thus S is associative, commutative, closed under addition. Since $f + e = e + f = f$, e acts as the identity element in S. Let $-f$ be the map which sends x to $-f(x)$. Since $(f + (-f))(x) = ((-f) + f)(x) = 0$, $f + (-f) = (-f) + f = e$, so S is closed under taking additive inverses. Therefore, S is an abelian group under addition. Let $r, s \in R$. Since $r \cdot f(x) \in M$, there exists $X \to M$ that maps x to $r \cdot f(x)$, and thus S is closed under scalar multiplication. Since M is an R-module, $1 \cdot f(x) = f(x)$, $(rs) \cdot f(x) = r \cdot (s \cdot f(x))$, $(r+s) \cdot f(x) = r \cdot f(x) + s \cdot f(x)$, and $r \cdot (f+g)(x) = r \cdot (f(x)+g(x)) = r \cdot f(x) + r \cdot g(x)$. It follows that S meets all the rules to be a module over R. $\square$

Problem 7

Let M and N be any two R-modules. Denote by $\mathrm{Hom}_R(M, N)$ the set of all R-linear maps from M to N. Show that this set is naturally an R-module.

Proof. Let $H = \mathrm{Hom}_R(M, N)$. Since H is a subset of S, the set of all maps $M \to N$, it suffices to show that H nonempty, closed under addition, and closed under scalar multiplication, by Problem 6. Since H contains the maps $M \to N$ that sends m to rm for some $r \in R$, H is non empty. Let $f, g \in H$, $x, y \in M$, and $r \in R$. Since

$$(f+g)(x+y) = f(x+y) + g(x+y) = f(x) + g(x) + f(y) + g(y) = (f+g)(x) + (f+g)(y),$$

and

$$(f+g)(rx) = f(rx) + g(rx) = r \cdot f(x) + r \cdot g(x) = r \cdot (f+g)(x),$$

$f + g$ is a linear map, and so H is closed under addition. Define $r \cdot f$ to be the mapping $M \to N$ that sends m to $r \cdot f(m)$. Since

$$(r \cdot f)(x+y) = r \cdot f(x+y) = r \cdot f(x) + r \cdot f(y) = (r \cdot f)(x) + (r \cdot f)(y),$$

and

$$(r \cdot f)(sx) = r \cdot sf(x) = s \cdot (r \cdot f(x)) = s \cdot (r \cdot f)(x),$$

for some $s \in R$, H is closed under scalar multiplication, and the result follows. ☐

Problem 8

Let M be an R-module and let X be a subset of M. The annihilator I of X, is the subset of all elements r of R, such that $rm = 0$, for all elements m of X. Show that I is an ideal of R. Prove also that the annihilator of X is equal to the annihilator of the submodule generated by X.

Proof. We first note that I is nonempty, as $0 \in I$. Let $r, s \in I$, and let $m \in M$. Since $(r+s)m = rm+sm = 0$ and $(-r)m = -1 \cdot (rm) = 0$, I is closed under addition and taking additive inverse, and thus I is an additive subgroup. Let $k \in R$. Since $(kr)m = k(rm) = 0$, $k \in I$, and thus I is an ideal.

Let N be the submodule generated by X, and let $n \in N$. Since $n = r_1x_1 + r_2x_2 + \cdots + r_kx_k$, for some $r_1, r_2, \ldots, r_k \in R$ and $x_1, x_2, \ldots, x_k \in X$, we get $rn = r(r_1x_1 + r_2x_2 + \cdots + r_kx_k) = r_1(rx_1) + r_2(rx_2) + \cdots + r_k(rx_k) = 0$, and the result follows. $\square$

Problem 9

The next few results refer to the power series ring which is defined as follows. Let R be a commutative ring and let x be an indeterminate. The power series ring in R, denoted $R[\![x]\!]$, consists of all (possibly infinite) formal sums,

$$\sum_{n\geq 0} a_n x^n,$$

where $a_n \in R$. Thus if $R = \mathbb{Q}$, then both

$$x - \frac{x^3}{3!} + \frac{x^5}{5!} + \dots,$$

and

$$1 + 2!x + 3!x^2 + 4!x^3 + \dots,$$

are elements of $\mathbb{Q}[\![x]\!]$, even though the second, considered as a power series in the sense of analysis, does not converge for any $x \neq 0$. Addition and multiplication of elements of $R[\![x]\!]$ are defined as for polynomials.

The degree of a power series is equal to the smallest n, so that the coefficient of a_n is non-zero. Even for a polynomial, in what follows the degree always refers to the degree as a power series.

(i) Show that $R[\![x]\!]$ is a ring.

Proof. We first note that $0, 1 \in R \subset R[\![x]\!]$ are obviously the zero and unit of $R[\![x]\!]$. Let $f(x), g(x), h(x) \in R[\![x]\!]$, say $f(x) = \sum_{n\geq 0} f_n x^n$, $g(x) = \sum_{n\geq 0} g_n x^n$, and $h(x) = \sum_{n\geq 0} h_n x^n$. Then, $(f+g)(x) = \sum_{n\geq 0}(f_n + g_n)x^n$ and $(fg)(x) = \sum_{n\geq 0} k_n x^n$, where $k_n = \sum_{i\geq 0}^{n} f_i g_{n-i}$, and so $R[\![x]\!]$ is closed under addition and multiplication. Since R is associative under addition, $R[\![x]\!]$ is associative under addition and multiplication. Since $-f(x) = \sum_{n\geq 0} -f_n x^n \in R[\![x]\!]$ such that $f(x)+(-f(x)) = (-f(x))+f(x) = 0$, $R[\![x]\!]$ is closed under taking additive inverse. Since $f(g+h)(x) = \sum_{n\geq 0} l_n x^n = (fg)(x)+(gh)(x)$, where $l_n = \sum_{i\geq 0} f_i(g_{n-i} + h_{n-i}) = \sum_{i\geq 0} f_i g_{n-i} + f_i h_{n-i}$, $R[\![x]\!]$ is distributive. Hence, $R[\![x]\!]$ is a ring. □

(ii) Show that $f(x) \in R[\![x]\!]$ is invertible if and only if the degree of $f(x)$ is zero and the constant term is invertible. What is the inverse of $1 - x$?

Proof. Suppose that $f(x) = \sum_{n\geq 0} f_n x^n$ is invertible, with $g(x) = \sum_{n\geq 0} g_n x^n$ as its inverse. We know $fg(x) = gf(x) = \sum_{n\geq 0} k_n x^n = 1$, where $k_n = \sum_{i\geq 0} f_i g_{n-i}$. But then $f_0 g_0 = g_0 f_0 = 1$, so f_0 is nonzero and invertible.

We now assume the converse. Since f_0 is invertible, we may assume that $f(x) = 1 + a_1 x + a_2 x^2 + \dots$. Let $y = 1 - f(x)$. We show that $g(x) = 1 + y + y^2 + \dots$ is in $R[\![x]\!]$ and act as the inverse of $f(x)$. Notice that $1 - f(x)$ is of degree at least 1, so

$$g(x) = 1 + y + y^2 + \dots = 1 + (1 - f(x)) + (1 - f(x))^2 + \dots = 1 + x f_1(x) + x^2 f_2(x) + \dots,$$

where $f_i(x) = a_{i,0} + a_{i,1}x + a_{i,2}x^2 + \dots$, and $a_{i,k}$ is the kth coefficient of $(1 - f(x))^i$. In particular, $a_{i,k} \in R$ as $1 - f(x) \in R[\![x]\!]$, and thus the kth coefficients of $g(x)$ is $\sum_{i=1}^{k} a_{i,k-i} \in R$. Then,

$$\begin{aligned}(fg)(x) = (gf)(x) &= (1-y)(1 + y + y^2 + \dots) \\ &= (1 + y + y^2 + \dots) - (y + y^2 + y^3 + \dots) \\ &= 1,\end{aligned}$$

and the result follows.

The inverse of $1-x$ is obviously $1+x+x^2+\cdots \in R[\![x]\!]$, as

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

□

(iii) Show that if R is an integral domain then the degree of a product is the sum of the degrees.

Proof. Suppose that $f(x)$ has degree m and $g(x)$ has degree n. If a is the leading coefficient of $f(x)$ and b is the leading coefficient of $g(x)$, then $f(x) = ax^m + \dots$, $g(x) = bx^n + \dots$, where $\dots$ indicate higher degree terms. Then, $(fg)(x) = (ax^m + \dots)(bx^n + \dots) = abx^{m+n} + \dots$. However, R is an integral domain, so $ac \neq 0$, which means $(fg)(x) \neq 0$ and is of degree $m+n$. □

(iv) Show that if R is an integral domain then so is $R[\![x]\!]$.

Proof. Let $f(x), g(x) \in R[\![x]\!]$ such that $f(x)g(x) = 0$. Then $\deg(fg)(x) = 0$, by (iii). This means that $\deg f(x) = \deg g(x) = 0$, so $f(x) = a, g(x) = b$, for some $a, b \in R$. But then $ab = 0$, so either a or b is 0. The result then follows from either $f(x)$ or $g(x)$ is 0. □

(v) If F is a field then prove that $F[\![x]\!]$ is a Euclidean domain.

Proof. Define $d : F[\![x]\!] - \{0\} \to \mathbb{N} \cup \{0\}$ by sending $f(x)$ to its degree. Suppose that we are given $f(x), g(x) \in R[\![x]\!]$. By (iii), $d(f(x)) \leq d(fg(x))$. It remains to show that we can find $q(x), r(x)$ such that $g(x) = q(x)f(x) + r(x)$, where $d(r(x))$ is either 0 or less than $d(f(x))$. We attempt to divide $f(x)$ into $g(x)$. If $\deg g(x) < \deg f(x)$, we take $q(x) = 0, r(x) = g(x)$ are we are done. Hence, we may assume $\deg g(x) \geq \deg f(x)$, say $f(x) = ax^m + \dots$, $g(x) = bx^n + \dots$, where $n > m$, $a, b \neq 0$, and $\dots$ indicate the higher degree terms. Notice that $f(x) = (a+\dots)x^m$ and $g(x) = (b+\dots)x^n$. By (ii), $(a+\dots)$ and $(b+\dots)$ are invertible as F is a field, so there exists $h = (a+\dots)^{-1}, k = (b+\dots)^{-1} \in F[\![x]\!]$. Take $q(x) = khx^{n-m}$ and $r(x) = 0$. It follows that $g(x) = q(x)f(x) + r(x)$, and this completes the proof. □

(vi) Show that if F' is a field then $F'[\![x]\!]$ is a UFD.

Proof. It follows from (vi) and Lemma 7.7 that $F[\![x]\!]$ is an Euclidean domain and thus a UFD. □

Problem 10

(i) Prove that if R is Noetherian then so is $R[\![x]\!]$

Proof. idk bro. $\square$

(ii) Prove that if R is Noetherian then so is $R[\![x_1, x_2, \ldots, x_n]\!]$, where the last term is defined appropriately.

Proof. We proceed by induction on n. By (i), $R[\![x_1]\!]$ is Noetherian. Suppose $n > 1$. We treat $R[\![x_1, x_2, \ldots, x_n]\!]$ like polynomial rings. Then, by the universal property of polynomial rings,

$$R[\![x_1, x_2, \ldots, x_n]\!] \simeq R[\![x_1, x_2, \ldots, x_{n-1}]\!][\![x_n]\!].$$

By induction, $R[\![x_1, x_2, \ldots, x_{n-1}]\!]$ is Noetherian, and the result now follows from (i). $\square$