MAT 312/AMS 351: Applied Algebra
Solutions to Problem Set 9 (20pts)

4.4 2; 3pts *Let X be a set and $F(X)$ be the set of all maps from X to itself. Show that $f \in F(X)$ is a surjection if and only if $gf = hf$ implies $g = h$ for all $g, h \in F(X)$.*

Suppose $f \in F(X)$ is a surjection and $g, h \in F(X)$ are distinct, i.e. with $g(x) \neq h(x)$ for some $x \in X$. Since f is a surjection, $x = f(y)$ for some $y \in X$. Along with $g(x) \neq h(x)$, this implies that $g(f(y)) \neq h(f(y))$ and so $gf \neq hf$. Thus, $gf = hf$ implies $g = h$ if f is a surjection.

Suppose $f \in F(X)$ is not a surjection, i.e. there exists $x \in X$ such that $x \neq f(y)$ for any $y \in X$. Define

$$g, h \colon X \longrightarrow X, \qquad g(y) = y \quad \forall\, y \in X, \qquad h(y) = \begin{cases} y, & \text{if } y \neq x; \\ f(x), & \text{if } y = x. \end{cases}$$

In particular, $gf = hf$ because both compositions send y to $f(y)$. However, $g \neq h$ because $x \neq f(x)$. Thus, $gf = hf$ implies $g = h$ for all $g, h \in F(X)$ only if f is a surjection.

4.4 5; 2pts *Suppose R is a ring with no zero divisors. Let $a, b, c \in R$ be such that $ac = bc$ and $c \neq 0$. Show that $a = b$.*

Since $ac - bc = 0$, the distributive law gives $(a-b)c = 0$. Since R has no zero divisors, it follows that either $a - b = 0$ or $c = 0$. Since the latter is not the case by assumption, $a - b = 0$ and so $a = b$.

4.4 11; 3pts *Let F be a field with additive identity 0 and multiplicative identity 1. The characteristic $\chi(F)$ of F is the smallest $n \in \mathbb{Z}^+$ such that*

$$n \cdot 1 \equiv \underbrace{1+1+\ldots+1}_{n}$$

is 0; if such an $n \in \mathbb{Z}^+$ does not exist, then $\chi(F) \equiv 0$. Suppose $\chi(F) \neq 0$. Show that $\chi(F)$ is a prime number.

First, $\chi(F) \neq 1$ because $1 \neq 0$ in a field. Suppose $\chi(F) = mn$ with $m, n \in \mathbb{Z}^+$ and $m, n \geq 2$. Since $m, n < \chi(F)$, the elements

$$m \cdot 1 \equiv \underbrace{1+1+\ldots+1}_{m} \qquad \text{and} \qquad n \cdot 1 \equiv \underbrace{1+1+\ldots+1}_{n}$$

of F are not zero, but their product $mn = \chi(F)$ is zero; thus, m and n are zero divisors in F. Since a field F has no zero divisors, this is a contradiction. Thus, $\chi(F)$ is either 0 or a prime number.

Problem E (12pts)

Let $(R,+,\cdot)$ be a commutative ring with additive identity 0 and multiplicative identity 1. An element $u\in R$ is called a unit *if it has a multiplicative inverse (thus, 0 is not a unit, and every nonzero element of a field is a unit).*

(a) Show that the sets of powers series and polynomials with coefficients in R,

$$R[[x]] \equiv \left\{\sum_{n=0}^{\infty} a_n x^n : a_0, a_1, \ldots \in R\right\} \qquad \text{and}$$
$$R[x] \equiv \left\{\sum_{n=0}^{\infty} a_n x^n \in R[[x]] : \exists\, d\in\mathbb{Z}^{\ge 0} \text{ s.t. } a_n=0\ \forall\, n>d\right\},$$

have natural commutative ring structures. Specify the addition and product operations, additive identity $\mathbf{0}$, and multiplicative identity $\mathbf{1}$. Verify the required properties.

(b) Show that $a(x)\equiv 1+x$ is not a unit in $R[x]$.

(c) Show that $a(x)\equiv\sum_{n=0}^{\infty} a_n x^n$ is a unit in $R[[x]]$ if and only if a_0 is a unit in R.

(a; **6pts**) The addition and multiplication on $R[[x]]$ are given by

$$\sum_{n=0}^{\infty} a_n x^n + \sum_{n=0}^{\infty} b_n x^n = \sum_{n=0}^{\infty} (a_n+b_n) x^n \quad \text{and} \quad \left(\sum_{n=0}^{\infty} a_n x^n\right)\cdot\left(\sum_{n=0}^{\infty} b_n x^n\right) = \sum_{n=0}^{\infty}\Bigg(\sum_{\substack{i,j\in\mathbb{Z}^{\ge 0}\\ i+j=n}} a_i b_j\Bigg) x^n,$$

respectively. The latter is well-defined because each of the inner sums is finite and the addition in R is associative.

The commutativity and associativity of the addition on $R[[x]]$ and the commutativity of the multiplication on $R[[x]]$ defined above follow immediately from the commutativity and associativity of the addition on R and the commutativity of the multiplication on R. The distributive law for R implies the distributive law for $R[[x]]$. The associativity of the multiplication on $R[[x]]$ follows from the associativity of the multiplication on R via

$$\left(\left(\sum_{n=0}^{\infty} a_n x^n\right)\cdot\left(\sum_{n=0}^{\infty} b_n x^n\right)\right)\cdot\left(\sum_{n=0}^{\infty} c_n x^n\right) = \sum_{n=0}^{\infty}\Bigg(\sum_{\substack{i,j,k\in\mathbb{Z}^{\ge 0}\\ i+j+k=n}} (a_i b_j) c_k\Bigg) x^n = \sum_{n=0}^{\infty}\Bigg(\sum_{\substack{i,j,k\in\mathbb{Z}^{\ge 0}\\ i+j+k=n}} a_i (b_j c_k)\Bigg) x^n$$
$$= \left(\sum_{n=0}^{\infty} a_n x^n\right)\cdot\left(\left(\sum_{n=0}^{\infty} b_n x^n\right)\cdot\left(\sum_{n=0}^{\infty} c_n x^n\right)\right).$$

The zero power series and the constant power series with value 1,

$$\mathbf{0} \equiv \sum_{n=0}^{\infty} 0x^n \qquad \text{and} \qquad \mathbf{1} \equiv 1x^0 + \sum_{n=1}^{\infty} 0x^n\,,$$

are the additive identity in $R[[x]]$ and the multiplicative identity in $R[[x]]$, respectively. Thus, $R[[x]]$ is a commutative ring with additive identity $\mathbf{0}$ and multiplicative identity $\mathbf{1}$.

Since the addition and multiplication operations on $R[[x]]$ send a pair of polynomials, i.e. elements of $R[x]\subset R[[x]]$, to polynomials, these operations restrict to addition and multiplication operations on $R[x]$. Since the operations on $R[[x]]$ are commutative and associative and satisfy the distributive law, the same applies to their restrictions to $R[x]$. Since $\mathbf{0},\mathbf{1}\in R[x]$, we conclude that $R[x]$ is also a commutative ring with additive identity $\mathbf{0}$ and multiplicative identity $\mathbf{1}$.

(b; **2pts**) Suppose

$$\mathbf{1} = (1+x)\cdot\bigg(\sum_{n=0}^{\infty} b_n x^n\bigg) \equiv b_0+\sum_{n=1}^{\infty}\big(b_n+b_{n-1}\big)x^n.$$

This implies that $b_0=1$ and $b_n+b_{n-1}=0$ for all $n\in\mathbb{Z}^+$. Thus, $b_n=(-1)^n$ and so

$$(1+x)^{-1} = \sum_{n=0}^{\infty}(-1)^n x^n \in R[[x]]-R[x].$$

We conclude that $1+x$ is a unit (has a multiplicative inverse) in $R[[x]]$, but not in $R[x]$.

(c; **4pts**) Suppose

$$\mathbf{1} = \bigg(\sum_{n=0}^{\infty} a_n x^n\bigg)\cdot\bigg(\sum_{n=0}^{\infty} b_n x^n\bigg) = a_0 b_0 + \sum_{n=1}^{\infty}\bigg(\sum_{\substack{i,j\in\mathbb{Z}^{\ge 0}\\ i+j=n}} a_i b_j\bigg)x^n.$$

This implies that $a_0 b_0=1$, i.e. $a_0\in R$ is a unit (has a multiplicative inverse).

Suppose $a_0\in R$ is a unit with multiplicative inverse $a_0^{-1}\in R$. Thus,

$$\begin{aligned} b(x) \equiv \bigg(a_0\bigg(1+a_0^{-1}\sum_{n=1}^{\infty}a_n x^n\bigg)\bigg)^{-1} &\equiv a_0^{-1}\bigg(1+\sum_{m=1}^{\infty}\bigg(-a_0^{-1}\sum_{n=1}^{\infty}a_n x^n\bigg)^m\bigg) \\ &\equiv a_0^{-1}\bigg(1+\sum_{m=1}^{\infty}\bigg(\sum_{n=1}^{\infty}a_n x^{n-1}\bigg)^m\big(-a_0^{-1}\big)^m x^m\bigg) \end{aligned}$$

is well-defined element of $R[[x]]$; the last expression becomes a power series in x after applying the multinomial theorem and collecting coefficients of the same powers of x because only finitely many terms contribute to each power of x. By a direct check, $a(x)b(x)=\mathbf{1}$ and so $a(x)$ has a multiplicative inverse in $R[[x]]$, i.e. $a(x)$ is a unit in $R[[x]]$.