MA-638 Rings and Fields
Homework for Section 7.2, Jan. 20
Adam Frank

Problem 1. Define $R[[x]]$ of *formal power series* in the indeterminate x with coefficients from the commutative ring R to be all formal infinite sums

$$\sum_{n=0}^{\infty} a_n x^n$$

Define addition and multiplication in the usual way. Prove that $R[[x]]$ is a commutative ring with $\mathbb{1}$.

Let

$$\sum_{n=0}^{\infty} a_n x^n, \sum_{n=0}^{\infty} b_n x^n, \sum_{n=0}^{\infty} c_n x^n \in R[[x]]$$

We start by showing that $R[[x]]$ is a commutative group under addition. We begin by observing that R is a ring and hence addition in R is associative and commutative. Hence

$$\sum_{n=0}^{\infty} a_n x^n + \sum_{n=0}^{\infty} b_n x^n = \sum_{n=0}^{\infty} (a_n + b_n) x^n = \sum_{n=0}^{\infty} (b_n + a_n) x^n = \sum_{n=0}^{\infty} b_n x^n + \sum_{n=0}^{\infty} a_n x^n,$$

$$\sum_{n=0}^{\infty} a_n x^n + \left(\sum_{n=0}^{\infty} b_n x^n + \sum_{n=0}^{\infty} c_n x^n \right) = \sum_{n=0}^{\infty} (a_n + (b_n + c_n)) x^n$$

$$= \sum_{n=0}^{\infty} ((a_n + b_n) + c_n) x^n$$

$$= \left(\sum_{n=0}^{\infty} a_n x^n + \sum_{n=0}^{\infty} b_n x^n \right) + \sum_{n=0}^{\infty} c_n x^n.$$

1

This shows that addition is commutative and associative in $R[[x]]$. Since R is a ring then $0 \in R$, and the below shows that the power series of all zero coefficients is a zero of $R[[x]]$.

$$\sum_{n=0}^{\infty} a_n x^n + \sum_{n=0}^{\infty} 0 x^n = \sum_{n=0}^{\infty} (a_n + 0) x^n = \sum_{n=0}^{\infty} a_n x^n.$$

Similarly the set is closed under additive inverses.

$$\sum_{n=0}^{\infty} a_n x^n + \sum_{n=0}^{\infty} (-a_n) x^n = \sum_{n=0}^{\infty} (a_n - a_n) x^n$$

$$= \sum_{n=0}^{\infty} 0 x^n = 0$$

Finally to show closure, we note that for any $a_n, b_n \in R$ we have that $a_n + b_n \in R$. Hence $\sum_{n=0}^{\infty} a_n + \sum_{n=0}^{\infty} b_n = \sum_{n=0}^{\infty} (a_n + b_n)$ is in $R[[x]]$. With this we have shown that $R[[x]]$ is a commutative group under addition.

Next we show that multiplication associates, and in particular consider any nth coefficient of $\left(\sum_{n=0}^{\infty} a_n x^n \right) \left(\left[\sum_{n=0}^{\infty} b_n x^n \right] \cdot \left[\sum_{n=0}^{\infty} c_n x^n \right] \right)$. First define d_k to be the kth coefficient of $\left[\sum_{n=0}^{\infty} b_n x^n \right] \left[\sum_{n=0}^{\infty} c_n x^n \right]$. Therefore

$$d_k = \sum_{i=0}^{k} b_i c_{k-i}.$$

Before establishing the associativity of multiplication, I want to establish a lemma, which is that $\sum_{n=0}^{m} a_n b_{m-n} = \sum_{i+j=m} a_i b_j$ where $0 \leq i, j \leq m$. In fact I will prove this by showing that the indexed set of terms of the left sum is equal to the indexed set of terms of the right. For any term in the left sum, $a_n b_{m-n}$, clearly the indices sum to m. Hence the terms of $\sum_{n=0}^{m} a_n b_{m-n}$ are a subset of the terms of $\sum_{i+j=m} a_i b_j$. Now select any $0 \leq i, j \leq m$ such that $i + j = m$. Then $a_i b_j = a_i b_{m-i}$. Since $0 \leq i \leq m$ this implies $a_i b_{m-i}$ is a term of $\sum_{n=0}^{m} a_n b_{m-n}$. So

we have that every term of $\displaystyle\sum_{i+j=m} a_i b_j$ is a term of $\displaystyle\sum_{n=0}^{m} a_n b_{m-n}$, and the lemma is proved.

(Note that although the proof above establishes the equality of the set of terms, this may not establish the equality of the sums if any terms are repeated. However, indices uniquely determine terms in these sums. Therefore every indexed term appears precisely once in each set, and the equality of the sums therefore follows from the proof above.)

Next I want to establish a second lemma which is that $\displaystyle\sum_{m+n=a} \left(\sum_{i+j=n}^{d} x_{m,i,j} \right) = \sum_{m+i+j=a} x_{m,i,j}$ where $x_{m,i,j}$ is any term which is a function of m, i, j. Of course we take $m, n, i, j \in \mathbb{N}$. Again we show that the two sums have the same terms, and of course if $x_{m,i,j}$ is a term such that $m + n = a$ and $i + j = n$, then it follows immediately that $m + i + j = a$ and therefore $x_{m,i,j}$ is a term of the right hand series. Conversely if $x_{m,i,j}$ is any term where $m + i + j = a$, then define $n = a - m$. It then follows that $0 \leq i + j = n$ and so $x_{m,i,j}$ is a term of the left hand sum.

Now we can begin the proof. The nth coefficient of $\displaystyle\left(\sum_{n=0}^{\infty} a_n x^n \right) \left(\left[\sum_{n=0}^{\infty} b_n x^n \right] \cdot \left[\sum_{n=0}^{\infty} c_n x^n \right] \right)$ is given by

$$\sum_{k=0}^{n} a_k d_k = \sum_{i+j=n} a_i d_j = \sum_{i+j=n} \left(a_i \sum_{m=0}^{j} b_m c_{j-m} \right)$$

$$= \sum_{i+j=n} \left(a_i \sum_{k+m=j} b_k c_m \right)$$

$$= \sum_{i+j=n} \left(\sum_{k+m=j} a_i b_k c_m \right)$$

$$= \sum_{i+k+m=n} a_i b_k c_m.$$

We then see that the same is true for $\displaystyle\left(\left[\sum_{n=0}^{\infty} a_n x^n \right] \left[\sum_{n=0}^{\infty} b_n x^n \right] \right) \left(\sum_{n=0}^{\infty} c_n x^n \right)$.
If we call $\displaystyle e_k = \sum_{n=0}^{k} a_n b_{k-n}$ the kth term of $\displaystyle\left[\sum_{n=0}^{\infty} a_n x^n \right] \left[\sum_{n=0}^{\infty} b_n x^n \right]$, then the nth

term of $\left(\left[\sum_{n=0}^{\infty} a_n x^n \right] \left[\sum_{n=0}^{\infty} b_n x^n \right] \right) \left(\sum_{n=0}^{\infty} c_n x^n \right)$ is given by

$$\sum_{k=0}^{n} e_k c_{n-k} = \sum_{i+j=n} e_i c_j = \sum_{i+j=n} \left(\sum_{m=0}^{i} a_m b_{j-m} \right) c_j$$

$$= \sum_{i+j=n} \left(\sum_{k+m=i} a_k b_m c_j \right)$$

$$= \sum_{k+m+j=n} a_k b_m c_j$$

Of course the names of the variables are irrelevant and this shows that the two sums are equal. Hence multiplication is associative.

Now we show that multiplication distributes.

$$\left(\sum_{n=0}^{\infty} a_n x^n \right) \left(\sum_{n=0}^{\infty} b_n x^n + \sum_{n=0}^{\infty} c_n x^n \right) = \left(\sum_{n=0}^{\infty} a_n x^n \right) \left(\sum_{n=0}^{\infty} (b_n + c_n) x^n \right)$$

$$= \sum_{n=0}^{\infty} \left(\sum_{m=0}^{n} a_m (b_{n-m} + c_{n-m}) \right) x^n$$

$$= \sum_{n=0}^{\infty} \left(\sum_{m=0}^{n} a_m b_{n-m} + \sum_{m=0}^{n} a_m c_{n-m} \right) x^n$$

$$= \sum_{n=0}^{\infty} \left(\sum_{m=0}^{n} a_m b_{n-m} \right) x^n + \sum_{n=0}^{\infty} \left(\sum_{m=0}^{n} a_m c_{n-m} \right) x^n$$

$$= \left(\sum_{n=0}^{\infty} a_n x^n \right) \left(\sum_{n=0}^{\infty} b_n x^n \right) + \left(\sum_{n=0}^{\infty} a_n x^n \right) \left(\sum_{n=0}^{\infty} c_n x^n \right)$$

If R is commutative then multiplication is commutative, demonstrated below.

$$\left(\sum_{n=0}^{\infty} a_n x^n\right)\left(\sum_{n=0}^{\infty} b_n x^n\right) = \sum_{n=0}^{\infty}\left(\sum_{m=0}^{n} a_m b_{n-m}\right) x^n$$

$$= \sum_{n=0}^{\infty}\left(\sum_{m=0}^{n} b_m a_{n-m}\right) x^n$$

$$= \left(\sum_{n=0}^{\infty} b_n x^n\right)\left(\sum_{n=0}^{\infty} a_n x^n\right)$$

And finally if $\mathbb{1} \in R$ then this is also $\mathbb{1} \in R[[x]]$. That is to say the series with $a_0 = \mathbb{1}$ and all other $a_n = 0$ if $n \geq 1$, is the unitary element of $R[[x]]$. To see this, consider any nth term of $\mathbb{1} \cdot \sum_{n=0}^{\infty} a_n$. If we call b_m the mth coefficient of $\mathbb{1}$ then $a_n b_{n-m} = 0$ whenever $m < n$, and when $m = n$ we have $a_n b_{n-m} = a_n \cdot \mathbb{1} = a_n$. Hence the nth term of $\mathbb{1} \cdot \sum_{n=0}^{\infty} a_n$ is

$$\sum_{m=0}^{n} a_n b_{n-m} = a_n.$$

This shows that $\mathbb{1} \cdot \sum_{n=0}^{\infty} a_n = \sum_{n=0}^{\infty} a_n$ and so $\mathbb{1}$ is the unitary element.

Problem 2. Let S be any ring and let $n \geq 2$ be an integer. Prove that if A is any strict upper triangular matrix in $M_n(S)$ then $A^n = 0$.

Define the ith right-diagonal to be the tuple of matrix coordinates $(A_{0,i}, A_{1,i+1}, \ldots, A_{i,n})$. The assumption that A is a strict upper-triangular matrix then implies that the 0th right-diagonal is the tuple $(0, 0, \ldots, 0)$ of length n. We say that a coordinate $A_{r,c}$ is "strictly below" the ith diagonal if there is are $s, d \in \mathbb{N}$ such that $A_{r-s,c+d}$ is on the ith diagonal. Hence every cooridnate of A below the 0th diagonal is 0. We will prove that if the $(i-1)$th right-diagonal of A^i is a tuple of only zeroes and every coordinate below the $(i-1)$th right-diagonal is 0, then the ith right-diagonal of A^{i+1} will be a tuple of only zeroes and every coordinate below its ith diagonal will be 0, for $1 \leq i \leq n$.

Now suppose that the $(i-1)$th right-diagonal of A^i is a tuple of only zeroes, and every coordinate below its $(i-1)$th diagonal is zero. Consider $(A^{i+1})_{m,i+m}$ to be the mth coordinate on the ith right-diagonal of A^{i+1} (in particular $0 \leq m \leq n-i$). By definition of the matrix product, $(A^{i+1})_{m,i+m} = \sum_{k=1}^{n} (A^i)_{m,k} A_{k,i+m}$. We are guaranteed that for each $k < i+m$ we have that $(A^i)_{m,k} = 0$ since these coordinates are strictly below the ith right-diagonal. Moreover notice that if $k \geq i+m$ then $A_{k,i+m}$ is on or below the main diagonal of A and hence $A_{k,i+m} = 0$. Thus $(A^{i+1})_{m,i+m} = 0$ for each m. Therefore $\sum_{k=1}^{n} (A^i)_{m,k} A_{k,i+m} = 0$ which proves that the ith diagonal of A^{i+1} is a tuple of zeroes.

It then only remains for us to show that every coordinate below the ith right-diagonal of A^{i+1} is zero. We already have that the coordinates below the main diagonal are zero because we know that upper triangular matrices are closed under products. We can then repeat the above argument, for any jth right-diagonal of A^{i+1}, with $0 \leq j \leq i$. Its mth coordinate will again be $\sum_{k=1}^{n} (A^i)_{m,k} A_{k,j+m}$. For each $k < j+m$ we have $(A^i)_{m,k} = 0$ and for each $k \geq j+m$ we have $A_{k,j+m0}$. Hence $\sum_{k=1}^{n} (A^i)_{m,k} A_{k,j+m} = 0$.

The above is then a proof by induction that the nth right-diagonal of A^n is equal to zero and every coordinate below this diagonal is zero. But this exhausts every coordinate of A^n and therefore A^n is the zero matrix.