Math 350, Spring 2025 Professor Rob Benedetto

Multiplication of Polynomials is Associative

Let R be a ring. As noted without proof at the bottom of page 193 of Saracino's book, the set $R[X]$ of polynomials $a_0 + a_1X + \cdots + a_nX^n$ with coefficients $a_0, \ldots, a_n \in R$ forms a ring under the following operations. Writing $f, g \in R[X]$ as

$$f(X) = a_0 + a_1X + a_2X^2 + \cdots = \sum_{i\geq 0} a_iX^i \quad \text{and} \quad g(X) = b_0 + b_1X + b_2X^2 + \cdots = \sum_{i\geq 0} b_iX^i,$$

(where we understand each to actually be a finite sum, i.e., all but finitely many a_i and b_i are 0), then we define the $+$ and $\cdot$ operations on $R[X]$ by

$$(f+g)(X) = \sum_{i\geq 0}(a_i+b_i)X^i = (a_0+b_0) + (a_1+b_1)X + (a_2+b_2)X^2 + \cdots$$

and

$$(f\cdot g)(X) = \sum_{i\geq 0}\left(\sum_{j=0}^{i} a_jb_{i-j}\right)X^i = a_0b_0 + (a_0b_1 + a_1b_0)X + (a_0b_2 + a_1b_1 + a_2b_0)X^2 + \cdots .$$

Actually proving this claim — that $R[X]$ really is a ring with these two operations — is just a matter of proving each of the ring axioms (Properties 0–7 in a previous handout). But maybe I should have put "just" in quotes, since their proofs vary wildly in difficulty. In class I proved one of the distributive laws (which is of medium difficulty), and in this handout I'll prove two others: the associativity of addition (less difficult) and the associativity of multiplication (the most difficult).

But first, I'll also note (as Saracino does on page 194) that if R is commutative, then so is $R[X]$. Similarly, if R has unity 1, then so does $R[X]$ (and that unity element is 1, viewed as a polynomial of degree 0). However, even if R is a division ring or field, then $R[X]$ is definitely *not* a division ring or field, since the degree 1 polynomial X has no multiplicative inverse.

Addition in $R[X]$ is associative

Proof. Given $f, g, h \in R[X]$, write $f = \sum a_iX^i$, $g = \sum b_iX^i$, $h = \sum c_iX^i$, where each sum starts at $i = 0$, and $a_i, b_i, c_i \in R$ with all but finitely many equal to zero. Then

$$\begin{aligned}(f+g)+h &= \left(\sum_{i\geq 0}(a_i+b_i)X^i\right) + \sum_{i\geq 0} c_iX^i = \sum_{i\geq 0}\Big((a_i+b_i)+c_i\Big)X^i \\ &= \sum_{i\geq 0}\Big(a_i+(b_i+c_i)\Big)X^i = \sum_{i\geq 0} a_iX^i + \left(\sum_{i\geq 0}(b_i+c_i)X^i\right) = f+(g+h)\end{aligned}$$

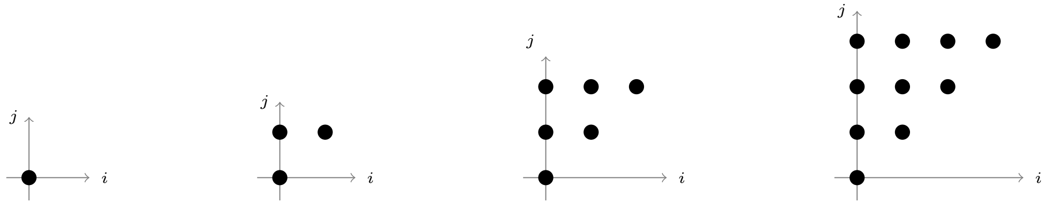
QED + is assoc

It turns out to be *much* harder to prove that multiplication is associative in $R[X]$, because rather than the coefficient of X^i being a simple expression like $(a_i + b_i) + c_i = a_i + (b_i + c_i)$ as in the proof above, instead a re-indexing of a double sum is required. In anticipation of this, we state and prove the following lemma not about rings, but about certain sets of pairs of integers:

Lemma. Let $k \geq 0$ be an integer. Then
$\big\{(i,j)\in\mathbb{Z}\times\mathbb{Z}\,\big|\,0\leq j\leq k \text{ and } 0\leq i\leq j\big\} = \big\{(i,j)\in\mathbb{Z}\times\mathbb{Z}\,\big|\,0\leq i\leq k \text{ and } i\leq j\leq k\big\}.$

Proof of Lemma. Given $k \geq 0$, call the first set A_k and the second set B_k.
Given $(i,j) \in \mathbb{Z}\times\mathbb{Z}$, we have $(i,j) \in A_k \iff 0 \leq i \leq j \leq k \iff (i,j) \in B_k$. QED Lemma

The reason for the Lemma is that, as we'll see in the proof below, we will need to show that we'll want to switch the two sum signs in sum of the form $\sum_{j=0}^{k}\sum_{i=0}^{j}$ to get $\sum_{i=0}^{k}\sum_{j=i}^{k}$. (And we'll need *more* reindexing from there, but that's the start.) Of course, what's going on here, as noted in the proof of the Lemma, is that both sums are over the set of i, j with $0 \le i \le j \le k$. Intuitively, this is what that set looks like for some small values of k:



$k = 0$ $\quad$ $k = 1$ $\quad$ $k = 2$ $\quad$ $k = 3$

So switching the order of summation is very similar to switching the order of the integral signs in a double integral. With that preface, we are now ready to prove the desired result (which is also exercise 19.11(b) in Saracino's book).

Multiplication in $R[X]$ is associative

Proof. Given $f, g, h \in R[X]$, write $f = \sum a_i X^i$, $g = \sum b_i X^i$, $h = \sum c_i X^i$, where each sum starts at $i = 0$, and $a_i, b_i, c_i \in R$ with all but finitely many equal to zero.
We make the following claim about certain sums in the ring R:

Claim: For any $k \ge 0$, we have $\displaystyle\sum_{j=0}^{k}\left(\left(\sum_{i=0}^{j} a_i b_{j-i}\right) c_{k-j}\right) = \sum_{i=0}^{k}\left(a_i\left(\sum_{m=0}^{k-i} b_m c_{k-m-i}\right)\right)$.

Proof of Claim: Given $k \ge 0$, by the distributive law, the left side is $\displaystyle\sum_{j=0}^{k}\sum_{i=0}^{j}(a_i b_{j-i})c_{k-j}$.

By the Lemma, this expression equals $\displaystyle\sum_{i=0}^{k}\sum_{j=i}^{k}(a_i b_{j-i})c_{k-j}$. Since $(a_i b_{j-i})c_{k-j} = a_i(b_{j-i}c_{k-j})$, the expression is $\displaystyle\sum_{i=0}^{k}\left(a_i\sum_{j=i}^{k}(b_{j-i}c_{k-j})\right)$, by the distributive law.

Finally, re-indexing via $m = j - i$ in the second sum changes that inner sum from $\displaystyle\sum_{j=i}^{k}(b_{j-i}c_{k-j})$ to $\displaystyle\sum_{m=0}^{k-i}(b_m c_{k-m-i})$. That is, the full expression equals $\displaystyle\sum_{i=0}^{k}\left(a_i\left(\sum_{m=0}^{k-i} b_m c_{k-m-i}\right)\right)$, which is the desired right side. QED Claim

Thus,

$$(f \cdot g) \cdot h = \left(\sum_{j\ge 0}\left(\sum_{i=0}^{j} a_i b_{j-i}\right)X^j\right)\left(\sum_{i\ge 0} c_i X^i\right) = \sum_{k\ge 0}\left(\sum_{j=0}^{k}\left(\sum_{i=0}^{j} a_i b_{j-i}\right)c_{k-j}\right)X^k$$

$$= \sum_{k\ge 0}\left(\sum_{i=0}^{k} a_i\left(\sum_{m=0}^{k-i} b_m c_{k-m-i}\right)\right)X^k = \left(\sum_{i\ge 0} a_i X^i\right)\left(\sum_{j\ge 0}\left(\sum_{m=0}^{j} b_m c_{j-m}\right)X^j\right) = f \cdot (g \cdot h)$$

where the third equality is by the Claim. QED $\cdot$ is assoc