Exercises on Polynomial Rings

Zack M. Davis

15–20 February 2025

Abstract

Exercises from Dustin Ross and Emily Clader, *Beginning Algebraic Geometry*.

0.1.1. *Theorem.* Addition and multiplication of polynomials on $R[x_j]_{j=1}^n$ is a commutative ring with unity.

Proof. (Additive closure.) Addition is defined as $\sum_\alpha a_\alpha x^\alpha + \sum_\alpha b_\alpha x^\alpha = \sum_\alpha (a_\alpha + b_\alpha)x^\alpha$ (definition 0.4), but $a_\alpha, b_\alpha \in R$ (definition 0.2), so $a_\alpha + b_\alpha \in R$ (by the additive closure of the thing R). ✓

(Additive associativity.) $\sum_\alpha a_\alpha x^\alpha + (\sum_\alpha b_\alpha x^\alpha + \sum_\alpha c_\alpha x^\alpha) = \sum_\alpha a_\alpha x^\alpha + \sum_\alpha (b_\alpha + c_\alpha)x^\alpha = \sum_\alpha (a_\alpha + b_\alpha + c_\alpha)x^\alpha = \sum_\alpha (a_\alpha + b_\alpha)x^\alpha + \sum_\alpha c_\alpha x^\alpha = (\sum_\alpha a_\alpha x^\alpha + \sum_\alpha b_\alpha x^\alpha) + \sum_\alpha c_\alpha x^\alpha$ ✓

(Additive identity.) $\sum_\alpha a_\alpha x^\alpha + 0 = \sum_\alpha a_\alpha x^\alpha$ ✓

(Additive inverses.) $\sum_\alpha a_\alpha x^\alpha + \sum_\alpha -a_\alpha x^\alpha = \sum_\alpha (a_\alpha - a_\alpha)x^\alpha = \sum_\alpha 0x^\alpha = 0$ ✓

(Additive commutativity.) $\sum_\alpha a_\alpha x^\alpha + \sum_\alpha b_\alpha x^\alpha = \sum_\alpha (a_\alpha + b_\alpha)x^\alpha = \sum_\alpha (b_\alpha + a_\alpha)x^\alpha$ (by commutativity of addition in the ring R) and $\sum_\alpha (b_\alpha + a_\alpha)x^\alpha = \sum_\alpha b_\alpha x^\alpha + \sum_\alpha a_\alpha x^\alpha$ ✓

(Multiplicative closure.) $(\sum_\alpha a_\alpha x^\alpha)(\sum_\alpha b_\alpha x^\alpha) = \sum_\alpha \left(\sum_{\alpha_1+\alpha_2=\alpha} a_{\alpha_1} b_{\alpha_2}\right) x^\alpha$ and $\left(\sum_{\alpha_1+\alpha_2=\alpha} a_{\alpha_1} b_{\alpha_2}\right) \in R$ ✓

(Multiplicative associativity.) $(\sum_\alpha a_\alpha x^\alpha)((\sum_\alpha b_\alpha x^\alpha)(\sum_\alpha c_\alpha x^\alpha)) = (\sum_\alpha a_\alpha x^\alpha) \sum_\alpha \left(\sum_{\alpha_1+\alpha_2=\alpha} b_{\alpha_1} c_{\alpha_2}\right) x^\alpha = \sum_\alpha \left(\sum_{\alpha_1+\alpha_2=\alpha} a_{\alpha_1} \left(\sum_{\beta_1+\beta_2=\alpha_2} b_{\beta_1} c_{\beta_2}\right)\right) x^\alpha = \sum_\alpha \left(\sum_{\alpha_1+\beta_1+\beta_2=\alpha} a_{\alpha_1} b_{\beta_1} c_{\beta_2}\right) x^\alpha$

whereas $((\sum_\alpha a_\alpha x^\alpha)(\sum_\alpha b_\alpha x^\alpha))(\sum_\alpha c_\alpha x^\alpha) = \left(\sum_\alpha \left(\sum_{\alpha_1+\alpha_2=\alpha} a_{\alpha_1} b_{\alpha_2}\right) x^\alpha\right)(\sum_\alpha c_\alpha x^\alpha)$

$= \sum_\alpha \left(\sum_{\alpha_1+\alpha_2=\alpha} \left(\sum_{\beta_1+\beta_2=\alpha_1} a_{\beta_1} b_{\beta_2}\right) c_{\alpha_2}\right) x^\alpha = \sum_\alpha \left(\sum_{\beta_1+\beta_2+\alpha_2=\alpha} a_{\beta_1} b_{\beta_2} c_{\alpha_2}\right) x^\alpha.$

("Commutative ring".) $(\sum_\alpha a_\alpha x^\alpha)(\sum_\alpha b_\alpha x^\alpha) = \sum_\alpha \left(\sum_{\alpha_1+\alpha_2=\alpha} a_{\alpha_1} b_{\alpha_2}\right) x^\alpha$

and $(\sum_\alpha b_\alpha x^\alpha)(\sum_\alpha a_\alpha x^\alpha) = \sum_\alpha \left(\sum_{\alpha_1+\alpha_2=\alpha} b_{\alpha_1} a_{\alpha_2}\right) x^\alpha$, but $a_{\alpha_1} b_{\alpha_2} = b_{\alpha_1} a_{\alpha_2}$ if the underlying ring R is commutative. ✓

("With unity".) $(1x^0)(\sum_\alpha a_\alpha x^\alpha) = \sum_\alpha \left(\sum_{\alpha_1+\alpha_2=\alpha} [\alpha_1 = 0] a_{\alpha_2}\right) x^\alpha = \sum_\alpha a_\alpha x^\alpha$ ✓

(Distributivity.) $(\sum_\alpha a_\alpha x^\alpha)(\sum_\alpha b_\alpha x^\alpha + \sum_\alpha c_\alpha x^\alpha) = (\sum_\alpha a_\alpha x^\alpha)(\sum_\alpha (b_\alpha + c_\alpha)x^\alpha) = \sum_\alpha \left(\sum_{\alpha_1+\alpha_2=\alpha} a_{\alpha_1}(b_{\alpha_2} + c_{\alpha_2})\right) x^\alpha$ $= \sum_\alpha \left(\sum_{\alpha_1+\alpha_2=\alpha} a_{\alpha_1} b_{\alpha_2} + a_{\alpha_1} c_{\alpha_2}\right) x^\alpha = \sum_\alpha \left(\sum_{\alpha_1+\alpha_2=\alpha} a_{\alpha_1} b_{\alpha_2}\right) + \sum_\alpha \left(\sum_{\alpha_1+\alpha_2=\alpha} a_{\alpha_1} c_{\alpha_2}\right) x^\alpha = \sum_\alpha a_\alpha b_\alpha x^\alpha + \sum_\alpha a_\alpha c_\alpha x^\alpha$ ✓

0.1.2. $f = xyz^2 + xyz + z^3 + x^2z^2 + yz^2 + z + x + 1 \in R[x, y, z]$
$f = z^3 + (xy + y + x^2)z^2 + (xy + 1)z + (x + 1) \in R[x, y][z]$
$f = (x + 1)yz^2 + xyz + z^3 + x^2z^2 + z + (x + 1) \in R[x][y, z]$
$f = z^2x^2 + (yz^2 + yz + 1)x + (z^3 + yz^2 + z + 1) \in R[y, z][x]$

0.1.3. *Theorem.* $\varphi(\sum_{\alpha\in\mathbb{N}^n} a_\alpha \prod_{j=1}^n x_j^{\alpha_j}) : R[x_j]_{j=1}^n \to R[x_j]_{j=1}^{n-1}[x_n] := \sum_{d\geq 0} \left(\sum_{\alpha\in\mathbb{N}^n, \alpha_n=d} a_\alpha \prod_{j=1}^{n-1} x^{\alpha_j}\right) x_n^d$ is a ring isomorphism.

Proof. (Addition.) $\varphi(\sum_{\alpha\in\mathbb{N}^n} a_\alpha \prod_{j=1}^n x_j^{\alpha_j} + \sum_{\alpha\in\mathbb{N}^n} b_\alpha \prod_{j=1}^n x_j^{\alpha_j}) = \varphi(\sum_{\alpha\in\mathbb{N}^n} (a_\alpha + b_\alpha) \prod_{j=1}^n x_j^{\alpha_j})$

$= \sum_{d\geq 0} \left(\sum_{\alpha\in\mathbb{N}^n, \alpha_n=d} (a_\alpha + b_\alpha) \prod_{j=1}^{n-1} x^{\alpha_j}\right) x_n^d$

$= \sum_{d\geq 0} \left(\sum_{\alpha\in\mathbb{N}^n, \alpha_n=d} a_\alpha \prod_{j=1}^{n-1} x^{\alpha_j}\right) x_n^d + \sum_{d\geq 0} \left(\sum_{\alpha\in\mathbb{N}^n, \alpha_n=d} b_\alpha \prod_{j=1}^{n-1} x^{\alpha_j}\right) x_n^d$ ✓

(Multiplication.) $\varphi\left(\left(\sum_{\alpha\in\mathbb{N}^n} a_\alpha \prod_{j=1}^n x_j^{\alpha_j}\right)\left(\sum_{\alpha\in\mathbb{N}^n} b_\alpha \prod_{j=1}^n x_j^{\alpha_j}\right)\right) = \varphi\left(\sum_\alpha \left(\sum_{\alpha_1+\alpha_2=\alpha} a_{\alpha_1} b_{\alpha_2}\right) x^\alpha\right)$

$$= \sum_{d\geq 0} \left(\sum_{\alpha\in\mathbb{N}^n, \alpha_n=d} \left(\sum_{\alpha_1+\alpha_2=\alpha} a_{\alpha_1} b_{\alpha_2}\right) \prod_{j=1}^{n-1} x^{\alpha_j}\right) x_n^d \quad (1)$$

whereas

$\left(\sum_{d\geq 0}\left(\sum_{\alpha\in\mathbb{N}^n,\alpha_n=d} a_\alpha \prod_{j=1}^{n-1} x^{\alpha_j}\right) x_n^d\right)\left(\sum_{d\geq 0}\left(\sum_{\alpha\in\mathbb{N}^n,\alpha_n=d} b_\alpha \prod_{j=1}^{n-1} x^{\alpha_j}\right) x_n^d\right)$ ... um, this is where it gets tricky: we can't trivially mechanically apply our formal definition of multiplication using multiïndex notation to a product not written in multiïndex form. But $R[x_j]_{j=1}^{n-1}[x_n]$ is a space of single-variable polynomials (albeit with funny-looking coëfficients); this shouldn't actually be hard. It's $\left(\sum_k a_k x^k\right)\left(\sum_k b_k x^k\right) = \sum_j \left(\sum_{k_1+k_2=j} a_{k_1} b_{k_2}\right) x^j$. In this case, that's

$$\sum_j \left(\sum_{k_1+k_2=j}\left(\sum_{\alpha\in\mathbb{N}^n,\alpha_n=k_1} a_\alpha \prod_{j=1}^{n-1} x^{\alpha_j}\right)\left(\sum_{\alpha\in\mathbb{N}^n,\alpha_n=k_2} b_\alpha \prod_{j=1}^{n-1} x^{\alpha_j}\right)\right) x^j \tag{2}$$

which is *plausibly* the same thing as (1), but the last few steps of showing the equivalency are not entirely trivial. I don't think you can "just factor out" the $\prod_{j=1}^{n-1} x^{\alpha_j}$ from both inner factors, because the product over $\alpha \in \mathbb{N}^n$ such that $\alpha_n = k_1$ is not obviously the same as the one over $\alpha \in \mathbb{N}^n$ such that $\alpha_n = k_2$ ... or is it?

In (1), we're looping through $\alpha \in \mathbb{N}^n$ filtered for $\alpha_n = d$ (the power for the last variable being d), and inside that, looping through all ways two n-tuples α_1 and α_2 can add up to α, and inside that, taking the product of the coëfficients $a_{\alpha_1} b_{\alpha_2}$ times the product of the first $n-1$ variable powers.

In (2), we're looping through all ways k_1 and k_2 can add up to d, and inside that ... um, I don't think verbal restatement is helping here.

ChatGPT o3-mini-high is suggesting that we can rewrite the multiïndex to split off the last coördinate ... [TODO: finish]

(Unity.) $\varphi(1x^0) = 1x^0$ ✓

(Injectivity.) [TODO]

(Surjectivity.) [TODO]

0.1.6. *Proposition.* If R is not an integral domain, then neither is $R[x_j]_j$.

Proof. If $ab = 0$ for nonzero a, $b \in R$, then $ab = 0$ also in the constant subring of $R[x_j]_j$.

Proposition. If R is not an integral domain, then $\deg(fg) = \deg(f) + \deg(g)$ need not hold.

Proof. Suppose $a, b \in R$ are such that $ab = 0$. Then $\underbrace{(ax+c)}_{\deg(f)=1}\underbrace{(bx+c)}_{\deg(g)=1} = \underbrace{\cancelto{0}{abx^2} + (a+b)cx + c^2}_{\deg(f+g)=1\neq 1+1}$.

0.1.8. *Theorem.* $\deg(f+g) \leq \max(\deg(f),\ \deg(g))$

Proof. Suppose not: $\deg(f+g) > \max(\deg(f),\ \deg(g))$. Where would the highest-order term come from??

0.2.1. *Theorem.* $R* \subseteq R$ is a group under multiplication.

Proof. (Identity.) $1 \in R*$ because 1 is a unit: $1 \cdot 1 = 1$. ✓

(Inverses.) Units are defined as elements that have a multiplicative inverse! ✓

(Closure.) Suppose $u_1 u_2 \in R*$, and let $w := u_1 u_2$. Then $u_1^{-1} w = u_2$ and then $u_2^{-1} u_1^{-1} w = 1$. But then $u_2^{-1} u_1^{-1}$ is an inverse for w. So w is a unit. ✓

0.2.4. *Theorem.* $f \in K[x]$ being a polynomial of degree 2 or 3, f is irreducible iff there does not exist $a \in K$ such that $f(a) = 0$.

Proof. ($\Leftarrow$) Suppose for the contraposition that f is reducible (not irreducible). Then $f = gh$ for $g, h \in K[x] \backslash K*$.

Suppose $\deg(f) = 2$. Then $\deg(g) + \deg(h) = 2$.

Suppose that $\deg(g) = 2$ (without loss of generality, $\deg(h)$). Then $\deg(h) = 0$. But then $h \in K*$. Contradiction!

Suppose that $\deg(g) = 1$ (without loss of generality, $\deg(h)$). Then g will take the form $k_1 x + k_2 = 0$ for some $k_1, k_2 \in R$. But then $x = \frac{-k_2}{k_1}$. So then $a := x$ is an a such that $g(a) = 0$ and thus that $f(a) = 0$.

Suppose that $\deg(g) = 0$ (without loss of generality, $\deg(h)$). Then $g \in K*$. Contradiction!

Now suppose that $\deg(f) = 3$. Then $\deg(g) + \deg(h) = 2$.

Suppose that $\deg(g) = 3$ (without loss of generality, *&c.*). Then $\deg(h) = 0$. But then $h \in K*$. Contradiction!

Suppose that $\deg(g) = 2$ (without loss of ... *&c.*). Then $\deg(h) = 1$. Then h will take the form $k_1 x + k_2 = 0$ ... *&c.* as above.

Suppose that $\deg(g) = 1$ (without loss ...). Then g will take the form $k_1 x + k_2 = 0$ ... *&c.* as above.

Suppose that $\deg(g) = 0$ (without ...). Then $g \in K*$. Contradiction!

($\Rightarrow$) Suppose for the contraposition that there exists $a \in K$ such that $f(a) = 0$. [TODO: finish this direction; we obviously know that $(x - a)$ is going to be a factor for polynomials in $\mathbb{R}$, but we need to prove it for the generic ring over a field $K[x]]$

0.2.5. $x^4 + 2x^2 + 1 = (x^2 + 1)(x^2 + 1) \in \mathbb{R}[x]$ has no zeros.

0.2.8. **a**. The units in $\mathbb{Z}[x]$ are the units in $\mathbb{Z}$, ± 1.
b. *Proposition.* For $n \in \mathbb{Z}$, $nx \in \mathbb{Z}[x]$ is reducible.
Proof. $nx = n \cdot x$, but $n, x \notin \{-1, 1\} = \mathbb{Z}*$

0.2.9. *Theorem.* Every field is a UFD.
Proof. Suppose nonunit $x \in K$ had two factorizations, $x = \prod_{i=1}^{m} p_i = \prod_{j=1}^{n} q_j$. Then $\prod_{i=1}^{m} p_i \prod_{j=n}^{1} q_j^{-1} = 1$. But then $x = \prod_{i=1}^{m} p_i$ would have a (right) inverse, and be a unit. Contradiction!

0.3.2. *Proposition.* Ideals contain 0.
Proof. Ideals are closed under subtraction. So for ideal I, if $a \in I$, then $a - a = 0 \in I$.

Proposition. Ideals are closed under addition.
Proof. Suppose $x, y \in I$ for ideal I. Then $-1 = -y \in I$ by multiplication absorption. Then $x - -y = x + y \in I$.

0.3.3. *Proposition.* The only ideals of a field K are $\{0\}$ and K.
Proof. $\{0\}$ is an ideal of K: $0 - 0 = 0 \in \{0\}$ and for all $k \in K$, $k0 = 0 \in \{0\}$.
K is an ideal of K because closed under subtraction and multiplication. (Closure amounts to absorption when considering a set as an ideal of itself.)
Suppose some nonzero $k \in K$ is in ideal I. Consider some other element $h \in K$. By multiplication absorption, $\frac{h}{k}k = h \in I$, so $I = K$.

0.3.4. Let $A \subseteq R$.
a. *Proposition.* $\langle A \rangle$ is an ideal of R.
Proof. We recall that $\langle A \rangle := \{\sum_{i=1}^{n} r_i a_i : n \in \mathbb{N},\ r_i \in R,\ a_i \in A\}$.
(Subtraction closure.) For r_i, $s_i \in R$, $a_i\, b_i \in A$, $\sum_{i=1}^{m} r_i a_i - \sum_{i=1}^{n} s_i b_i$ we can for j from 1 to n rename $r_{i+j} := -s_j$ and $a_{i+j} := b_j$ and get $\sum_{i=1}^{m+n} r_i a_i$, which when written that way more obviously belongs to A. ✓
(Multiplication absorption.) $s \sum_{i=1}^{n} r_i a_i = \sum_{i=1}^{n} s r_i a_i \in \langle A \rangle$ ✓