Polynomial rings

Let R be a ring. The sum

$$f = a_n x^n + a_{n-1} x^{n-1} + \dots + a_1 x + a_0 \quad (\text{w/ } n \geq 0)$$

is called a polynomial in x, with coefficients a_i in R. If $a_n \neq 0$, the degree of f is n, and the leading coefficient is a_n.

If R contains 1, f is monic if $a_n = 1$.

Def: The set of all such polynomials is called the ring of polynomials in one variable over R. It's denoted $R[x]$. That is

$$R[x] := \{ a_n x^n + \dots + a_0 \mid n \geq 0,\ a_i \in R \}.$$

The operations are the familiar operations from a high school algebra class:

$$(a_0 + a_1 x + \dots) + (b_0 + b_1 x + \dots) = (a_0 + b_0) + (a_1 + b_1) x + \dots$$

To multiply, we first define $(a x^i)(b x^j) = ab\, x^{i+j}$. Then

$$(a_0 + a_1 x + \dots)(b_0 + b_1 x + \dots) = a_0 b_0 + (a_0 b_1 + a_1 b_0) x + (a_0 b_2 + a_1 b_1 + a_2 b_0) x^2 + \dots$$

In general, the coefficient of x^k in the product is $\sum_{i=0}^{k} a_i b_{k-i}$.

With these definitions, it's easy to check $R[x]$ is in fact a ring.

Remark: Usually the case we'll care about will be when R

has 1, and is commutative. In this case, $R[x]$ is also commutative with 1.

Note that $R \subseteq R[x]$. In fact, since R is already a ring, it's a subring of $R[x]$.

Ex: Let $R = \mathbb{Z}/2\mathbb{Z}$. Then all coefficients in $R[x]$ can be written as 0 or 1. So

$$(x+1)^2 = x^2 + 2x + 1 = x^2 + 1.$$

i.e. in $(\mathbb{Z}/2\mathbb{Z})[x]$ x^2+1 is a perfect square, even though it's not a perfect square in $\mathbb{Z}[x]$.

However, if $f(x) = x^n + \text{lower deg terms}$, $g(x) = x^m + \text{lower degree terms}$, then $fg(x) = x^{n+m} + \text{lower degree terms}$. i.e. in $\mathbb{Z}/2\mathbb{Z}[x]$, $\deg(fg) = \deg f + \deg g$. In fact, this is true over any integral domain:

Thm: Let R be an integral domain and $p(x), q(x) \in R[x]$, nonzero. Then

1.) degree $p(x)q(x)$ = degree $p(x)$ + degree $q(x)$

2.) units of $R[x]$ = units of R.

3.) $R[x]$ is an integral domain.

Pf: We can write $p(x) = a x^n + \text{lower terms}$, $q(x) = b x^m + \text{lower terms}$ where $a \neq 0$, $b \neq 0$. Then $\deg p = n$, $\deg q = m$.

$p(x)q(x) = ab\,x^{n+m} + \text{lower deg terms}$. Since R is an integral domain, $ab \neq 0$, so $\deg(pq) = m+n$, and $p(x)q(x) \neq 0$, which proves 1.) and 3.)

2.) If $a \in R$ is a unit in R, then it's a unit in $R[x]$, so $R^\times \subset R[x]^\times$.

If $b \in R[x]$ is a unit, then $\exists\ c \in R[x]$ s.t. $bc = 1$.

Thus $\deg(bc) = 0$, so b, c both have deg 0. Thus, $b, c \in R$.

So $b \in R^\times$.

Ex: If $S \subseteq R$ is a subring, then $S[x] \subseteq R[x]$ is a subring.

Ex: Let $R[x^2]$ be the set of polynomials where only even powers of x appear. Then $R[x^2]$ is a subring of $R[x]$.

We'll discuss more about polynomial rings later.