Rings of Polynomials

Let R be a ring and let x be called an indeterminant (as opposed to a variable).

Def. A **polynomial** $f(x)$ with coefficients in R is any expression of the form:

$$\sum_{i=0}^{\infty} a_i x^i = a_0 + a_1 x + a_2 x^2 + \cdots + a_n x^n + \cdots$$

where $a_i \in R$ and $a_i = 0$ for all but a finite number of values of i. The a_i's are **coefficients** of $f(x)$. The largest i for which $a_i \neq 0$ is called the **degree of the polynomial**. If for all $i, a_i = 0$, then we say the degree of $f(x)$ is undefined.

Let $R[x] = \{$set of polynomials, $f(x)$, with coefficients in $R\}$.

Notice that $R[x]$ is also a ring where addition and multiplication is defined in the usual way:

$$f(x) = a_0 + a_1 x + a_2 x^2 + \cdots + a_n x^n + \cdots$$

$$g(x) = b_0 + b_1 x + b_2 x^2 + \cdots + b_n x^n + \cdots$$

Then, $f(x) + g(x) = c_0 + c_1 x + c_2 x^2 + \cdots + c_n x^n + \cdots$,

where $c_i = a_i + b_i$

and $f(x)g(x) = d_0 + d_1 x + d_2 x^2 + \cdots + d_n x^n + \cdots$

where $d_i = \sum_{j=0}^{i} a_j \, b_{(i-j)}$.

Notice that if R is not commutative then neither is $R[x]$. If R is commutative then so is $R[x]$.

The additive identity element for $R[x]$ is $f(x) = 0$ and the multiplicative identity element is $g(x) = 1$.

Showing that $R[x], +$ is an abelian group and that $R[x]$ satisfies multiplicative associativity and the distributive laws is messy but straight forward.

Ex. Let $\mathbb{Z}_2[x] = R[x]$. Calculate $(x+1)^2$ and $(x+1)+(x+1)$.

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

$$(x+1)+(x+1) = (1+1)x + (1+1) = 0x + 0 = 0.$$

Ex. Find the sum and product of $f(x) = 4x - 5$ and $g(x) = 2x^2 - 4x + 2$ in $\mathbb{Z}_8[x]$.

$$\begin{aligned} f(x)+g(x) &= (4x-5) + (2x^2 - 4x + 2) \\ &= 2x^2 + (4-4)x + (2-5) \\ &= 2x^2 - 3 \\ &= 2x^2 + 5 \text{ in } \mathbb{Z}_8[x]. \end{aligned}$$

$$f(x)g(x) = (4x-5)(2x^2-4x+2)$$

$$= (4\cdot 2)x^3 - (4\cdot 4)x^2 + (4\cdot 2)x - (5\cdot 2)x^2 + (5\cdot 4)x - (5\cdot 2)$$

$$= 0x^3 - 0x^2 + 0x - 2x^2 + 4x - 2$$

(since $10 \equiv 2 \ (mod\ 8)$ and $20 \equiv 4 \ (mod\ 8)$)

$$= -2x^2 + 4x - 2$$

$$= 6x^2 + 4x + 6.$$

We define $R[x_1, x_2, \dots, x_n]$ the ring of polynomials in n indeterminants with coefficients in R in the usual way.

Ex. What are the units of $\mathbb{Z}_5[x]$?

So given an element $f(x) = a_0 + a_1x + a_2x^2 + \cdots + a_nx^n$

when is there a $g(x) = b_0 + b_1x + b_2x^2 + \cdots + b_mx^m$

such that $(f(x))(g(x))$ =1 in $\mathbb{Z}_5[x]$?

Notice that $\mathbb{Z}_5 \subseteq \mathbb{Z}_5[x]$, and $\mathbb{Z}_5$ is a field (but $\mathbb{Z}_5[x]$ isn't a field).

Thus, any non-zero element in $\mathbb{Z}_5$ has an inverse. So the polynomials $f(x) = 1,\ f(x) = 2,\ f(x) = 3,$ and $f(x) = 4$ are units in $\mathbb{Z}_5[x]$.

Suppose $f(x) = a_0 + a_1x + a_2x^2 + \cdots + a_nx^n$ has an inverse $g(x) = b_0 + b_1x + b_2x^2 + \cdots + b_mx^m$ in $\mathbb{Z}_5[x]$.

Let's assume $a_n \neq 0$ for some $n > 0$ i.e. $f(x)$ is not a constant function,

then $f(x)g(x) = c_0 + c_1x + c_2x^2 + \cdots + c_{n+m}x^{(n+m)}$
where the highest power of $f(x)g(x)$ is a_nb_m where a_n is the coefficient of the highest power of $f(x)$ (with a non-zero coefficient) and b_m is the coefficient of the highest power of $g(x)$ (with a non-zero coefficient).

Since $a_n \neq 0$, $a_nb_mx^{n+m}$, does not have $n + m = 0$.

But In order for $f(x)g(x) = 1$, all coefficients $c_1, c_2, \dots, c_{n+m}$ must be 0.

But that would mean $a_nb_m = 0$ and that can't happen because $\mathbb{Z}_5$ is a field and has no 0 divisors. Thus, the only units of $\mathbb{Z}_5[x]$ are the constant functions $f(x) = 1,\ f(x) = 2,\ f(x) = 3,$ and $f(x) = 4$.

If D is an integral domain then so is $D[x]$. The argument is similar to the one used in the previous example. If

$$f(x) = a_0 + a_1x + a_2x^2 + \cdots + a_nx^n$$
$$g(x) = b_0 + b_1x + b_2x^2 + \cdots + b_mx^m$$

then the only way for $f(x)g(x) = 0$ (that is, the product is the 0 polynomial) is for all coefficients of the product $f(x)g(x)$ to be 0.

The coefficient of the highest power of $f(x)g(x)$ is a_nb_m, where $a_n \neq 0$, $b_m \neq 0$. Thus the only way for $a_nb_m = 0$ is for there to be 0 divisors in D. But D is an integral domain so that can't happen.

If F is a field (and hence an integral domain) $F[x]$ is an integral domain but not a field since x is not a unit (i.e. there is no $f(x) \in F[x]$ with $xf(x) = 1$) However, we can form the field of rational functions from the integral domain $F[x]$ (as we did earlier) by creating the field of quotients for $F[x]$.

Theorem:

Let F be a subfield of a field E.

Let $\alpha \in E$, and let x be an indeterminant.

The map $\phi_\alpha: F[x] \to E$ is defined by:

$$\phi_\alpha(a_0 + a_1x + a_2x^2 + \cdots + a_nx^n) = a_0 + a_1(\alpha) + a_2\alpha^2 + \cdots + a_n\alpha^n$$

is a homomorphism of $F[x]$ into E.

In particular, $\phi_\alpha(x) = \alpha$, for all $\alpha \in F$, maps F isomorphically into E. The homomorphism ϕ_α is called the **evaluation homomorphism** at α.

Proof: The fact that ϕ_α is a homomorphism comes from the definition of addition and multiplication in $F[x]$.

If $f(x) = a_0 + a_1x + \cdots + a_nx^n$,

$g(x) = b_0 + b_1x + \cdots + b_mx^m$

$h(x) = f(x) + g(x) = c_0 + c_1x + \cdots + c_nx^n$, where $n \geq m$, then

$$\phi_\alpha\big(f(x) + g(x)\big) = \phi_\alpha\big(h(x)\big) = c_0 + c_1\alpha + \cdots + c_n\alpha^n$$

$$\phi_\alpha\big(f(x)\big) + \phi_\alpha\big(g(x)\big) = a_0 + a_1\alpha + \cdots + a_n\alpha^n + b_0 + b_1\alpha + \cdots + b_m\alpha^m$$

By the definition of addition in $F[x]$, $c_i = a_i + b_i$, so

$$\phi_\alpha\big(f(x) + g(x)\big) = \phi_\alpha\big(f(x)\big) + \phi_\alpha\big(g(x)\big).$$

$f(x)g(x) = d_0 + d_1x + \cdots + d_sx^s$ and

$$\phi_\alpha\big(f(x)g(x)\big) = d_0 + d_1\alpha + \cdots + d_s\alpha^s$$

$$\big[\phi_\alpha\big(f(x)\big)\big]\big[\phi_\alpha\big(g(x)\big)\big] = (a_0 + a_1\alpha + \cdots + a_n\alpha^n)(b_0 + b_1\alpha + \cdots + b_m\alpha^m)$$

By the definition of multiplication in $F[x]$:

$$\phi_\alpha\big(f(x)g(x)\big) = \big[\phi_\alpha\big(f(x)\big)\big]\big[\phi_\alpha\big(g(x)\big)\big].$$

If $f(x) = a$ is a constant polynomial in $F[x]$, then $\phi_\alpha(a) = a$.

So ϕ_α maps the constant functions isomorphically onto $F \subseteq E$.

By the definition of ϕ_α, $\phi_\alpha(x) = \alpha$.

Ex. Let $F = \mathbb{Q}$, and $E = \mathbb{R}$. Consider $\phi_3: \mathbb{Q}[x] \to \mathbb{R}$.

$$\phi_3(a_0 + a_1x + \cdots + a_nx^n) = a_0 + a_1(3) + \cdots + a_n(3)^n.$$

Notice that $\phi_3(x^2 - x - 6) = 3^2 - 3 - 6 = 0$.

So $x^2 - x - 6$ is in the kernel of ϕ_3.

What is the kernel of ϕ_3?

$$\ker(\phi_3) = \{f(x) \in \mathbb{Q}[x] |\, f(3) = 0\}.$$

Ex. Let $F = \mathbb{Q}$, and $E = \mathbb{C}$ and consider:

$$\phi_{2i}(a_0 + a_1x + \cdots + a_nx^n) = a_0 + a_1(2i) + \cdots + a_n(2i)^n$$

where $i^2 = -1$.

Notice that $\phi_{2i}(x^2 + 4) = (2i)^2 + 4 = 0$.

So $x^2 + 4$ is in the $\ker(\phi_{2i}) = \{f(x) \in \mathbb{Q}[x] |\, f(2i) = 0\}$.

Def. Let F be a subfield of a field E, and let α be an element of E.

Let $f(x) = a_0 + a_1x + \cdots + a_nx^n \in F[x]$, and let $\phi_\alpha : F[x] \to E$ be the evaluation homomorphism.

Let $f(\alpha)$ denote $\phi_\alpha\left(f(x)\right) = a_0 + a_1\alpha + \cdots + a_n\alpha^n$.

If $f(\alpha) = 0$, then α is a **zero of** $f(x)$.

Ex. Find all of the zeros of $x^4 + 2x^2 + 2x$ in $\mathbb{Z}_7$.

Since $\mathbb{Z}_7$ only has 7 elements we can just evaluate the polynomial for each value and see where it's 0 in $\mathbb{Z}_7$.

$\boldsymbol{x}$	$\boldsymbol{x^4 + 2x^2 + 2x = x(x^3 + 2x + 2)}$
0	$0(0^3 + 2(0) + 2) \equiv 0 \ (mod\ 7)$
1	$1(1^3 + 2(1) + 2) \equiv 5 \not\equiv 0 \ (mod\ 7)$
2	$2(2^3 + 2(2) + 2) \equiv 2(8 + 4 + 2) \equiv 2(14) \equiv 0 \ (mod\ 7)$
3	$3(3^3 + 2(3) + 2) \equiv 3(27 + 6 + 2) \equiv 3(35) \equiv 0 \ (mod\ 7)$
4	$4(4^3 + 2(4) + 2) \equiv 4(64 + 8 + 2) \equiv 4(74) \not\equiv 0 \ (mod\ 7)$
5	$5(5^3 + 2(5) + 2) \equiv 5(125 + 10 + 2) \equiv 5(137) \not\equiv 0 \ (mod\ 7)$
6	$6(6^3 + 2(6) + 2) \equiv 6(216 + 12 + 2) \equiv 6(230) \not\equiv 0 \ (mod\ 7)$

So the zeros occur at $x = 0,\ x = 2,\ x = 3$.