date: thursday, february 29, 2024

Polynomial Rings

Assumption: R is a commutative ring with 1_R.

Elements of the form

$$a_n x^n + a_{n-1} x^{n-1} + \cdots + a_1 x + a_0 \quad \text{with } a_n \neq 0,\ a_0, \ldots, a_n \in R$$

is called a polynomial over R with indeterminate X.

- $a_0, \ldots, a_n$ are coefficients
- a_n is the leading coefficient
- $p(x)$ is a monic polynomial if $a_n = 1$
- $\deg p(x) = n$ if $p(x) \neq 0$ or $\deg p(x) = -\infty$ if $p(x) = 0$

Def$^{\underline{n}}$: $R[x] = \{$all polynomials with coefficients in $R\}$

Note: $p(x) = a_n x^n + \cdots + a_0$ and $q(x) = b_m x^m + \cdots + b_0$, then $p(x) = q(x)$ iff $n = m$ and $a_i = b_i$ for all i.

Theorem: $R[x]$ is a commutative ring with identity 1 with the operations

$$(a_n x^n + a_{n-1} x^{n-1} + \cdots + a_0) + (b_n x^n + b_{n-1} x^{n-1} + \cdots b_0) = (a_n + b_n) x^n + (a_{n-1} + b_{n-1}) x^{n-1} + \cdots + (a_0 + b_0)$$

$$(a_n x^n + a_{n-1} x^{n-1} + \cdots + a_0)(b_n x^n + b_{n-1} x^{n-1} + \cdots b_0) = a_n b_m x^{n+m} + (a_{n-1} b_m + a_n b_{m-1}) x^{n+m-1} + \cdots + a_0 b_0$$

eg. $R = \mathbb{Z}_3$. Count the number of polynomials of degree 2.

$$\underset{\substack{\uparrow \\ 2 \\ \uparrow \\ \{1,2\}}}{a_2} x^2 + \underset{\substack{\uparrow \\ 3}}{a_1} x + \underset{\substack{\uparrow \\ 3}}{a_0} \quad \leftarrow \text{arbitrary polynomial of degree 2}$$

$\{0,1,2\}$

$\boxed{18 \text{ solutions}}$

Q: If R has property P, does $R[x]$ have property P?

A: It depends.

Theorem: If R is an integral domain, then $R[x]$ is also an integral domain.

__Proof__

Suppose $p(x) = a_n x^n + \cdots + a_0$ and $q(x) = b_m x^m + \cdots + b_0$. Then,

$$p(x)q(x) = a_n b_m x^{m+n} + \cdots$$

Since $a_n \neq 0$ and $b_m \neq 0$, and since R is an integral domain, $a_n b_m \neq 0$. So $p(x)q(x) \neq 0$. Thus, $R[x]$ is an integral domain.

$\square$

Corollary: If R is an integral domain and $p(x)q(x) \in R[x]$, then

$$\deg p(x)q(x) = \deg p(x) + \deg q(x).$$

eg. If $R = \mathbb{Z}_4$, and if $p(x) = 2x^{100} + 1$ and $q(x) = 2x^{2024} + 1$, then
$p(x)q(x) = 4x^{2124} + 2x^{100} + 2x^{2024} + 1 = 2x^{2024} + 2x^{100} + 1.$

eg. If F is a field, is $F[x]$ a field?
No, the element x has no inverse.
Suppose $q(x)x = 1$. Then $\deg q(x) + \deg x = 0$. This implies $\deg q(x) < 0$ which can't happen.

There are many maps $R[x]$ to R.

Theorem: Let $\alpha \in R$. Then the map $\varphi_\alpha : R[x] \to R$ given by

$$p(x) = a_n x^n + \cdots + a_0 \mapsto p(\alpha) = a_n \alpha^n + \cdots + a_0$$

is a homomorphism (called evaluation homomorphism at α).

Note: $R[x]$ is a commutative ring with identity 1. We can use this ring of coefficients to make a new polynomial ring.

$$(R[x])[y] = \{\text{all polynomials over } R[x] \text{ with indeterminate } y\}$$

$$g \in R[x][y] \Rightarrow g = f_n(x)y^n + f_{n-1}(x)y^{n-1} + \cdots + f_0(x)$$

usually write $R[x,y]$.
In general, can make $R[x_1, \ldots, x_n]$.

Division Algorithm in $F[x]$

High school stuff: polynomial division

$$
\begin{array}{r l}
 & \quad\quad\quad\quad\quad\;\; 2x + 7 \\
3x^2+2x+1 & \overline{)\,6x^3+25x^2+16x+17} \\
 & \underline{-6x^3+4x^2+2x} \;\downarrow \\
 & \quad\quad\;\; 21x^2+14x+17 \\
 & \quad\;\; \underline{-21x^2+14x+7} \\
 & \quad\quad\quad\quad\quad\quad\;\; 10
\end{array}
$$

$$6x^3+25x^2+16x+17=(3x^2+2x+1)(2x+7)+10$$

Can always do this if we assume our ring of coefficients is a field.

Theorem: (Division Algorithm for $F[x]$) If F is a field, and $a(x), b(x) \in F[x]$ and $b(x) \neq 0$, then there exists unique polynomials $q(x)$ and $r(x)$ such that

$$a(x)=b(x)q(x)+r(x) \quad \text{with } r(x)=0 \text{ or } \deg r(x) < \deg b(x).$$

eg. $R=\mathbb{Z}$, $a(x)=2x^2+1$, $b(x)=3x+1$

$(2x^2+1)=(3x+1)(ax+b)+c$

To make this work, $a=\frac{2}{3} \notin \mathbb{Z}$.

So we need the field property.

Proof: Next class issue

Recall: α is a root of $f(x)$ if $f(\alpha)=0$

Corollary: Let F be a field. Then α is a root of $f(x) \in F[x]$ iff $f(x)=(x-\alpha)q(x)$.

Proof

"$\Leftarrow$" If $f(x)=(x-\alpha)q(x)$, then $f(\alpha)=(\alpha-\alpha)q(\alpha)=0$.

"$\Rightarrow$" Apply the division algorithm to $f(x)$ and $(x-\alpha)$.

So $f(x)=q(x)(x-\alpha)+r(x)$ with $r(x)=0$ or $\deg(r(x))<1$. Then,

$$0=f(\alpha)=q(\alpha)(\alpha-\alpha)+r(\alpha)=r(\alpha).$$

But $r(x)$ is a constant, so $r(\alpha)=0$.

$\square$