Polynomial rings

Throughout, R is a commutative ring with identity.

Def. A polynomial over R with indeterminate x is an expression of the form

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

where the coefficients $a_0, a_1, \ldots, a_n$ is in R, and $a_n \neq 0$. We also consider $0 \in R$ to be the zero polynomial over R. We call a_n the leading coefficient and say that $p(x)$ is monic if $a_n = 1$. If $p(x) \neq 0$, then the degree of $p(x)$ is $\deg p(x) := n$. We also define $\deg 0 := -\infty$.

The set of all polynomials over R with indeterminate x is denoted $R[x]$.

$R[x]$ inherits binary operations from R via the usual addition and multiplication of polynomials.

Ex. Consider $p(x) = 6 + 3x^3$ and, $q(x) = 4 + 8x^2 + 4x^4$ in $\mathbb{Z}_{12}[x]$. $p(x) + q(x) = 10 + 8x^2 + 3x^3 + 4x^4$.

$$p(x)q(x) = 24 + 48x^2 + 24x^4 + 12x^3 + 24x^5 + 12x^7$$
$$= 0$$

So $\mathbb{Z}_{12}[x]$ has zero divisors!

Prop. Let R be a commutative ring with unity. Then $R[x]$ is a commutative ring with unity.

(Proof.) Exercise

1. Additive inverse is obtained by replacing each coefficient w/ its additive inverse.

2. Check associativity, distributivity, & commutativity of the product by expanding polynomial products. ∎

Prop. Let R be an integral domain. Then $R[x]$ is an I.D. and

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

$\forall\ p(x), q(x) \in R[x]$.

(Proof.) Let's write

$$p(x) = a_0 + a_1 x + \cdots + a_m x^m \ \ \&\ \ q(x) = b_0 + b_1 x + \cdots + b_n x^n,$$

with $a_m \neq 0$ & $b_n \neq 0$. Then $\deg p(x) = m$ & $\deg q(x) = n$. B/c R is an I.D., $a_m b_n \neq 0$, so the leading coefficient of $p(x)q(x)$ is $a_m b_n$. $\therefore$ $p(x)q(x) \neq 0$, and $\deg(p(x)q(x)) = m+n = \deg p(x) + \deg q(x)$. ∎

Def. Let R be a comm. ring with unity. Then the ring

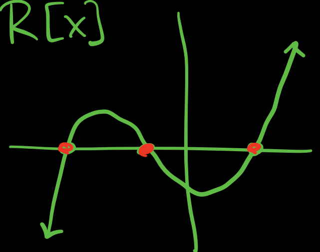
$$R[x,y] := (R[x])[y]$$

is called the ring of polynomials in two indeterminates over R.

In general, the ring of polynomials in n indeterminates over R is $R[x_1, \dots, x_n] := (R[x_1, \dots, x_{n-1}])[x_n]$.

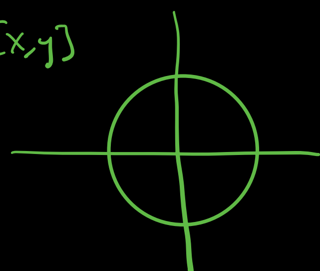
Aside:

$R[x]$



$p(x) = (x+4)(x+1)(x-2)$

$R[x,y]$



$p(x,y) = x^2 + y^2 - 1$

Prop. Let R be a commutative ring with unity and fix $\alpha \in R$. Then the map

$$\phi_\alpha : R[x] \longrightarrow R$$
$$p(x) \longmapsto p(\alpha) := a_0 + a_1\alpha + a_2\alpha^2 + \dots + a_n\alpha^n,$$

where $p(x) = a_0 + a_1 x + a_2 x^2 + \dots + a_n x^n$, is a homomorphism.

(Proof.) Exercise. ⊠

Def. We call ϕ_α the evaluation homomorphism at α.

Thm (The division algorithm)

Let F be a field and take $f(x), g(x) \in F[x]$, with $g(x) \neq 0$.

Then there exist unique polynomials $q(x), r(x) \in F[x]$ s.t.

$$f(x) = g(x)\,q(x) + r(x),$$

with $\deg r(x) < \deg g(x)$.

(Proof.)

Step ① Existence of $q(x)$ & $r(x)$.

First, if $f(x) = 0$, we can take $q(x) = r(x) = 0$.

(Note: $\deg r(x) = -\infty < \deg g(x)$.)

Now suppose $f(x) \neq 0$ and define

$$n := \deg f(x) \quad \& \quad m := \deg g(x).$$

If $m > n$, $q(x) = 0$ & $r(x) = f(x)$ works.

So assume $n \leq m$ and we'll apply induction on n.

Let's write

$$f(x) = a_0 + a_1 x + a_2 x^2 + \cdots + a_n x^n$$
$$g(x) = b_0 + b_1 x + b_2 x^2 + \cdots + b_m x^m.$$

Non-zero

Define

$$h(x) = f(x) - \frac{a_n}{b_m} x^{n-m} g(x).$$

Okay b/c base ring is a field

Highest-degree term of $-\frac{a_n}{b_m}x^{n-m}g(x)$ is

$$\left(-\frac{a_n}{b_m}x^{n-m}\right)\left(b_m x^m\right) = -a_n x^n,$$

which cancels highest-degree term of $f(x)$.

$\therefore$ $\deg h(x) < n$. By inductive hypothesis,

$$h(x) = g(x)\,q_h(x) + r(x),$$

for some $q_h(x), r(x) \in F[X]$ with $\deg r(x) < \deg g(x)$.

Finally,

$$q(x) := q_h(x) + \frac{a_n}{b_m}x^{n-m}$$

allows us to write $f(x) = g(x)\,q(x) + r(x)$.

Step 2 Uniqueness of $q(x)$ & $r(x)$.

Suppose $g(x)\,q_0(x) + r_0(x) = f(x) = g(x)\,q_1(x) + r_1(x)$,

with $\deg r_0(x), \deg r_1(x) < \deg g(x)$.

Then
$$\begin{aligned} r_1(x) - r_0(x) &= g(x)\,q_0(x) - g(x)\,q_1(x) \\ &= g(x)\left(q_0(x) - q_1(x)\right). \end{aligned}$$

If $q_0(x) - q_1(x) \neq 0$, then

$$\deg\left(r_1(x) - r_0(x)\right) = \deg g(x) + \deg\left(q_0(x) - q_1(x)\right)$$

$\geq \deg g(x)$.

But both $r_0(x)$ and $r_1(x)$ have degree less than $\deg g(x)$, so this is a contradiction.

$\therefore\ q_0(x) - q_1(x) = 0$.

$\therefore\ r_1(x) - r_0(x) = g(x)\big(q_0(x) - q_1(x)\big) = 0$. ∎

__Def.__ Let R be a commutative ring with unity and fix $\alpha \in R$ and $p(x) \in R[x]$. Then α is a zero or root of $p(x)$ if $p(x) \in \operatorname{Ker} \phi_\alpha$, where $\phi_\alpha : R[x] \to R$ is the evaluation homom. at α.

__Cor__ Let F be a field. Then $\alpha \in F$ is a zero of $p(x) \in F[x]$ iff $x - \alpha \in F[x]$ is a factor of $p(x)$ in $F[x]$.

__Cor__ If F is a field, then a polynomial in $F[x]$ of degree n has at most n distinct roots in F.