# Ring of Polynomials

$R$ is a ring

$R[x] = \{$ Polynomials in $X$ w/ coefficient in $R\}$
with finite non-zero coefficient

Fact

Every polynomial $f(x) = R(x)$ determines a function

$f: R \to R$
$r \mapsto f(r)$

Two different polynomials can define the same functions

e.g. $x^p, x \in \mathbb{Z}_p[x]$ $p$ is a prime

but functions $\mathbb{Z}_p \to \mathbb{Z}_p$ are the same

b.c. $r^p = r$ $\forall r \in \mathbb{Z}_p$
by Fermat's Little Thm

Suppose $R$ is a subring of $S$

$f(x) \in R[x] \rightsquigarrow$ we can view $f$ as an element of $S[x]$, we can evaluate $f(s)$, $s \in S$

We need to be careful w/ Rings of Coefficients
(which rings we work with?)

Solving Polynomials

$f(x) \in R[x]$

$r \in R$ is called a <u>zero</u> or <u>root</u> of $f(x)$

if $f(r) = 0$

- $x^2+1$ has no root in $\mathbb{R}$, but has roots in $\mathbb{C}$

so roots are ring dependent

- $x^2-2$ has no root in $\mathbb{Q}$

but has roots in $\mathbb{R}$

<u>Rational Roots Theorem</u>

$f(x) = a_0 + a_1 x + \dots + a_n x^n \in \mathbb{Z}[x]$

If $f(\frac{p}{q}) = 0$, $\gcd(p, q) = 1$, $q \neq 0$

$\Rightarrow p \mid a_0$ and $q \mid a_n$

e.g. $f(x) = x^2 - 2$

$\Rightarrow p \mid 2$, $q \mid 1 \Rightarrow \frac{p}{q} = \pm 2, \pm 1$

$f(\pm 2) = 2$, $f(\pm 1) = -1$

$\Rightarrow$ no rational root

Pf

$f(\frac{p}{q}) = a_0 + a_1 \frac{p}{q} + \dots + a_n \frac{p^n}{q^n} = 0$

$a_0 q^n + a_1 p q^n + \dots + a_n p^n = 0$

$\Rightarrow p \mid a_0 q^n$ $\qquad\qquad$ $\Rightarrow q \mid a_n p^n$

since $\gcd(p,q)=1$

$\gcd(p,q^n)=1$ $\qquad\qquad$ $\gcd(p^n,q)=1$

$\Rightarrow p \mid a_0$ (Euclid's Lemma) $\qquad$ $\Rightarrow q \mid a_n$

$\blacksquare$

<u>Lemma</u> $R[x]$ is a Ring:

<u>pf</u>: $(a_0+a_1x+\dots)+(b_0+b_1x+\dots)=(a_0+b_0)+(a_1+b_1)x+\dots$

$(R,+)$ is abelian $\Rightarrow$ $(R[x],+)$ is abelian

$$\sum_{i\geq 0} a_i x^i + \sum_{j\geq 0} b_j x^j$$

$$= \sum_{ij} a_i b_j x^i x^j = \sum_{ij} a_i b_j x^{i+j} = \sum_{k\geq 0}\Big(\sum_{\substack{i+j=k\\ ij\geq 0}} a_i b_j\Big)x^k \; *$$

associativity

$$\Big(\big(\textstyle\sum a_i x^i\big)\big(\sum b_j x^j\big)\Big)\big(\sum c_k x^k\big) = \dots = \sum_{ijk} a_i b_j c_k x^{i+j+k}$$

$$\big(\textstyle\sum a_i x^i\big)\Big(\big(\sum b_i x^i\big)\big(\sum c_i x^i\big)\Big) = \dots = \; | \; | \; | \; | \; | \; | \; |$$

$*$ $x$ commutes w/ $r\in R$

<u>Observation</u> Fix $r \in R$

$$R[x] \longrightarrow R \quad \text{(evaluation map)}$$

$$f(x) \longmapsto f(r)$$

$$a_0 + a_1 x + \dots \longmapsto a_0 + a_1 r + \dots$$

not always a homomorphism unless R commutes

$$f(x) \to f(r)$$
$$g(x) \to g(r)$$

$$f+g \to f(r)+g(r) \quad \text{ok}$$
$$fg \to f(r)\,g(r) \quad \text{not ok}$$

$arbr \neq abr^2$ unless R is commutative

A factorization of $f(x) \in R[x]$
is $f(x) = P_1(x)\,P_2(x) \dots P_k(x)$ $\quad P_i(x) \in R[x]$

Suppose R is commutative $\Rightarrow$

$P_i(r) = 0$ for some $i$ $\Rightarrow$
$f(r) = 0$

If R is integral domain

$\Rightarrow$ If $f(r) = 0 \Rightarrow P_i(r) = 0$ for some $i$

# Heirarchy of Rings

Easy: Field

$2^{nd}$ Easiest: $F[x]$ where $F$ is a field

Long division of polynomials:

Thm $F$ field, $f, g \in F[x]$, $g \neq 0$

$\Rightarrow$ we can write $f = qg + r$ $q \in F[x]$

where $\deg(r) < \deg(g)$ or $r = 0$

pf:

Let $I$ be the set of all $r(x)$ s.t. $r(x) = f(x) - g(x)q(x)$ for all possible $q(x)$

If $0 \in I$ then $r(x)$ is $0$ and we're done.

If not, let $r(x)$ be the polynomial with the smallest possible degree.

Claim $\deg r(x) < \deg g(x)$

Argue by contradiction, suppose

$r(x) = b_0 + \ldots + b_k x^k$ $b_k \neq 0$

$g(x) = a_0 + \ldots + a_n x^n$ $a_n \neq 0$

and $k > n$

$r(x) = f(x) - q(x) g(x)$

Consider $\hat{r}(x) = r(x) - g(x) \cdot x^{k-n} \frac{b_k}{a_n}$

$$\hat{r}(x) = f(x) - g(x)\left[q(x) + x^{k-n}\frac{b_k}{a_n}\right]$$

has degree less than $k$, contradiction

Uniqueness of $r(x)$ and $q(x)$?

Let's argue by contradiction,

suppose $f(x) = g(x)q(x) + r(x) = g(x)\hat{q}(x) + \hat{r}(x)$

$$\deg r, \deg \hat{r} < \deg g$$

$$\underbrace{g(x)\left[q(x) - \hat{q}(x)\right]}_{\deg \geq 0} = \underbrace{\hat{r}(x) - r(x)}_{\deg < \deg g}$$

Contradiction, The only possibility is that $r(x) = \hat{r}(x)$

in which case $q(x) = \hat{q}(x)$ as well

b.c. $F[x]$ is an integral domain

Useful Fact

$f(x) \in F(x)$, $F$ is a field

$\alpha \in F$ is a root of $f(x)$

$\iff f(x) = (x-\alpha)g(x)$

Pf $f(x) = (x-\alpha)g(x)$

$\Rightarrow f(\alpha) = (\alpha-\alpha)g(x) = 0$

Now suppose $f(\alpha)=0$

Long Divide:

$$f(x)=(x-\alpha)\,g(x)+r(x)$$

Either $r(x)=0$ and then we have factorization

or $\deg r < \deg(x-\alpha)=1$

$\Rightarrow \deg r(x)=0$

$\Rightarrow r(x)=r$ is a constant polynomial

$f(x)=(x-\alpha)\,g(x)+r \quad r\in F$

$f(\alpha)=(\alpha-\alpha)\,g(\alpha)+r \quad \Rightarrow r=f(\alpha)$

but $f(\alpha)=0 \Rightarrow r=0$

$\Rightarrow f(x)=f(x-\alpha)\,g(x)$ ∎

<u>Fact</u> $f(x)\in F[x]$, $f$ is a field

$\deg f=n \Rightarrow f(x)$ has most $n$ different roots in $F$.

<u>Pf</u> Suppose $\alpha_1,\alpha_2,\dots,\alpha_k$ are different roots of $f(x)$

$\Rightarrow f(x)=(x-\alpha_1)\,g(x)$

$0=f(\alpha_i)=(\alpha_i-\alpha_i)\,g(\alpha_i)$

$\Rightarrow g(x)$ has roots $\alpha_2,\dots,\alpha_k$

$\deg g=\deg f-1=n-1$

Anyway, by induction on degree,

$n-1 \geq k-1$ (roots $\alpha_2, \dots \alpha_n$)

$\Rightarrow n \geq k$. ∎

We can continue w/ factorization & get that

$f(x) = (x-\alpha_1)(x-\alpha_2)\cdots(x-\alpha_k)h(x)$

<u>def</u> $f(x) \in F[x]$, $F$ is a field

$f(x)$ is irreducible if there is no factorization $f(x) = g(x)h(x)$

$\deg g, h < \deg f$

If $f(x)$ has a root $\alpha \in F$

then $f(x)$ is reducible unless $\deg f(x) = 1$

or $f = 0$

If $f(x)$ is reducible then $f(x)$ has a root

if $\deg f(x) = 2$ or $3$

[in this case one of the factors will have degree $1 \Leftrightarrow f(x)$ has a root]

Eisenstein Theorem

$f(x) = a_0 + a_1 x^1 + \dots + a_n x^n \in \mathbb{Z}[x]$

fix a prime $p$,

Suppose $p \nmid a_n$

$p \mid a_i \quad i < n$

$p^2 \nmid a_0$

$\Rightarrow f(x)$ is irreducible as a polynomial in $\mathbb{Q}[x]$

eg:

$P(x) = x^5 + 3x - 6$

Take $\underline{p=3}$

$3 \nmid 1$

$3 \mid 3, -6$

$9 \nmid -6$

$\Rightarrow f(x)$ is an irreducible polynomial in $\mathbb{Q}[x]$

Fix $p$ a prime

$$\frac{x^p - 1}{x-1} = x^{p-1} + x^{p-2} + \dots + 1 = \varphi_p(x)$$

Cyclotonic Polynomial

Claim $\varphi_p(x)$ is irreducible in $\mathbb{Q}[x]$

Let's try Eisentein Thm.

$\varphi_p(x)$ is reducible iff shifting the polynomial is reducible.

$\varphi_p(x+1)$ is reducible

$$\varphi_p(x+1) = \frac{(x+1)^p - 1}{(x+1)-1} = \frac{(x+1)^p - 1}{x}$$

$$= \frac{1 + \sum_{i=1}^{p-1} \binom{p}{i} x^i + x^p - 1}{x}$$

$$= \sum_{i=1}^{p-1} \binom{p}{i} x^{i-1} + x^{p-1}$$

$$= \binom{p}{1} x^0 + \sum_{i=2}^{p-1} \binom{p}{i} x^{i-1} + x^{p-1}$$

Use eisenstein w/ $p$

$p \nmid 1$

$p \mid p$ but $p^2 \nmid p$

Claim $p \mid \binom{p}{i}$ $2 \leq i \leq p-1$

$$p \mid \frac{p(p-1)\cdots(p-i+1)}{i!} \ ?$$

$p$ divides the numerator but not denominator

$\Rightarrow p$ divides $\binom{p}{i}$

**Theorem** $\mathbb{Z}_p^*$ is a cyclic group

**Pf** $\mathbb{Z}_p^*$ is an abelian group of order $p-1$

**Claim:** If $\mathbb{Z}_p^*$ is not cyclic, then

$$\exists k < p-1 \quad \forall x : \mathbb{Z}_p^* \quad x^k = 1$$

Given the Claim, suppose $\mathbb{Z}_p^*$ is not cyclic
By the claim, $x^k - 1 \ \forall x \in \mathbb{Z}_p^*$

$$x^k - 1 = 0$$

$x^k - 1 \in \underset{\substack{\uparrow \\ \text{field}}}{\mathbb{Z}_p}[x]$ can't have $p-1$ roots since $k < p-1$

**Lemma:** Let $G$ be an abelian group of order $n$
if $G$ is noncyclic $\Rightarrow \exists k < n$
(also divisor of $n$)
s.t. $x^k = 1 \ \forall x \in G$
(here we write the group multiplicatively)

**Pf:** By classification thm,

$$G \cong C_1 \times C_2 \times \ldots \times C_r$$

Cyclic groups of order:
$n_1, n_2, \ldots n_r$

$$n = n_1 \times n_2 \times \ldots \times n_r$$

$x \in G \qquad x = (x_1, \dots, x_r)$

$x_i \in C_i$

$\text{ord}(x_i)$ divides $n_i$

$$\text{ord}(x) = \underset{i=1\dots r}{\text{lcm}}(\text{ord}(x_i))$$

$\text{ord}(x)$ divides $\underset{i=1\dots r}{\text{lcm}}(n_i) = k$

If $k < n \Rightarrow x^k = 1 \quad \forall x \in G$

we are done.

$k = \text{lcm}(n_i) = n = n_1 \times \dots \times n_r$

$\Updownarrow$

$n_1, n_2, \dots, n_r$ are coprime

$\Rightarrow C_1 \times C_2 \times \dots \times C_r$ is a cyclic group

(orders are coprime)

which is illegal

$\blacksquare$