Week 5

Phase II: Polynomial Rings

Goals/uses:

(1) Field theory

(2) Ideas about factorization and reducibility

↳ other types of rings: PIDs, UFDs, etc.

Q: Why polynomials?

Upgraded Q: what is the universal property of polynomials

To get there

Intuitive def: A relation in a ring R is any equality involving some of it's elements

Ex (1): In $\mathbb{Z}/7\mathbb{Z}$

"trivial relations" $2=2$ $2-2=0$ $2+3=3+2$ (ring axiom)

nontrivial: $3^2=2$ $5^6=1$

Are there elements in a ring R with "no nontrivial relations"?

Is there a "free element"

Side observation: If $\phi: R \to S$ is a ring homomorphism

then every relation in R gives a relation between the images in S

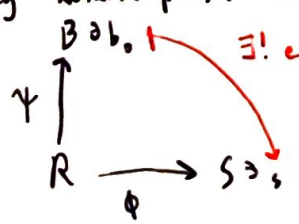
Ex: $a,b,c \in R$ satisfy $a^2-2ab+abc=0_R$

$\Rightarrow$ $\phi(a)^2-2\phi(a)\phi(b)+\phi(a)\phi(b)\phi(c)=0$

$\Rightarrow$ If $r \in R$ is not free, then you can't arbitrarily send it somewhere :)

More precise question: given a ring R, is there a "nearest" ring that contains a "free" element?

→ is there a ring B that contains a free element $b_0 \in B$ with a homomorphism from R to B, $\psi: R \to B$ such that if $\phi: R \to S$ is any ring homomorphism and $s \in S$ is any free element, then there is a unique map ev_s s.t. $\phi = ev_s \circ \psi$ and $ev_s(b_0)=s$



FACT: Such a ring does exist for any ring R

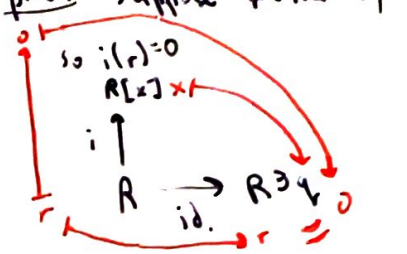
It's denoted $R[x]$ called "R adjoin x"

The free element is called $x \in R[x]$

Denote ring hom. $i: R \to R[x]$

Lemma 1: The hom i is injective

proof: Suppose $r \in \ker(i)$



so $r=0 \Rightarrow i$ injective

Claim: $R[x] = \{c_0 + c_1 x + c_2 x^2 + \dots + c_n x^n : c_0, \dots, c_n \in R,\ n \in \mathbb{Z}_{\geq 0}\}$

operations: familiar operations for polynomials,

Ex (3): $\mathbb{Z}_n\left(\mathbb{Z}/6\mathbb{Z}\right)[x]$ $\quad (1-2x+4x^2)(3-2x)$

$= 3 - 2x - 6x + 4x^2 + 12x^2 - 8x^3$

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

Also, the **degree** of a polynomial

$f(x) = c_0 + c_1 x + \dots + c_n x^n \qquad c_n \neq 0$

then $\deg(f(x)) = n$

degree of zero polynomial

degree 0?

we define

$\boxed{\deg(0) = -\infty}$

Lemma 2: Suppose you're in an integral domain

then for any 2 polynomials $f(x), g(x) \in R[x]$

$\deg(f(x)g(x)) = \deg(f(x)) + \deg(g(x))$

proof: $(c_0 + c_1 x + \dots + c_n x^n)(d_0 + d_1 x + \dots + d_m x^m)$

$= c_0 d_0 + (c_0 d_1 + c_1 d_0)x + \dots + d_m c_n x^{n+m}$

c_n and d_m are non-zero so $c_n d_m \neq 0$ (domain)

so $\deg(fg) = \deg(f) + \deg(g)$

Corollary: If R is an integral domain, then so is $R[x]$

Ex 4: $\mathbb{Q}$ is a field, but $\mathbb{Q}[x]$ is not a field

Q: what are the units in a polynomial ring?, in $R[x]$

Q: Given an ideal $I \subseteq R$

a) What is $(I)_{R[x]}$, the ideal generated by I in the bigger ring? $(I[x])$

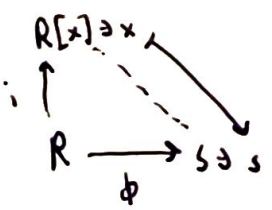
b) $(R/I)[x]$ vs. $\frac{R[x]}{(I)_{R[x]}}$

Back to polynomials:

For any commutative ring R,

$R[x]$, polynomial ring over R

- $p(x) = c_0 + c_1 x + \dots + c_n x^n \quad c_i \in R$
- injective hom. $i: R \to R[x]$
  $r \longmapsto r = p(x)$
- degree function $\deg: R[x] \to \mathbb{Z}_{\geq 0} \cup \{-\infty\}$
- universal property: For any hom. $\phi: R \to S$ and $s \in S$



$c_0 + c_1 x + c_2 x^2 + \dots + c_n x^n$

$\downarrow$

$\phi(c_0) + \phi(c_1) s + \dots + \phi(c_n) s^n$

Assume R is a domain)

Claim: The units in $R[x]$ are just the units from R (considered const. polynomials)

$(R[x])^\times = R^\times$

units in:

$\mathbb{Z}[x]$: $p(x) = \pm 1$

$\mathbb{Q}[x]$: $p(x) = c \quad c \in \mathbb{Q} - \{0\}$

$(\mathbb{Z}/6\mathbb{Z})[x]$: $p(x) = 1, 5$

proof: Suppose $p(x) = c_0 + c_1 x + \dots + c_n x^n \in R[x]$

and $p(x) q(x) = 1$ for some $q(x) \in R[x]$

$\deg(p(x)) + \deg(q(x)) = \deg(1) = 0$

so $\deg(p(x)) = \deg(q(x)) = 0$

$\Rightarrow p(x) = c_0, \quad q(x) = d_0$

If R is not a domain

$\deg(1) = \deg(p(x)q(x)) \leq \deg(p(x)) + \deg(q(x))$ is it true?!

Ideals in $R[x]$

Suppose $I \subseteq R$ is an ideal

then $(I)_{R[x]} = \{c_0 + c_1 x + \dots + c_n x^n : c_i \in I\}$

new notation $= I[x]$

Ex: (2) $(2) \subseteq \mathbb{Z}$

then $(2)_{\mathbb{Z}[x]} = \{c_0 + c_1 x + \dots + c_n x^n : c_i \in (2)\}$

$= \{c_0 + c_1 x + \dots + c_n x^n : c_i \text{ even}\}$

$= 2\mathbb{Z}[x]$

Proof: Suppose $\tilde{J} \subseteq R[x]$ is an ideal that contains I

Then: $\tilde{J}$ is closed under scaling, so for any $c \in I \subseteq \tilde{J}$ and $x^n \in R[x]$ we must have $cx^n \in \tilde{J}$

then $\tilde{J}$ is closed under + $\Rightarrow \{c_0 + c_1 x + \dots + c_n x^n : c_i \in I\} \subseteq \tilde{J}$

↑ this is an ideal in $R[x]$

Warning: Not all ideals in $R[x]$ are of the form $I[x]$ for some ideal in R

Ex: (3) $(x) \subseteq \mathbb{Z}[x]$

then $(x) = \{x f(x) : f(x) \in \mathbb{Z}[x]\} = \{c_1 x + \dots + c_n x^n : c_i \in \mathbb{Z}\}$

this not $I[x]$ for any $I \subseteq \mathbb{Z}$

Claim: If $I \subseteq R$ is an ideal, then there is an isomorphism

$$\frac{R[x]}{I[x]} \simeq \left(\frac{R}{I}\right)[x]$$

Ex: (4) $I = (2) = 2\mathbb{Z}$

in $\frac{\mathbb{Z}[x]}{2\mathbb{Z}[x]}$: some elements $\underbrace{1 - 2x + 3x^2 + 2\mathbb{Z}[x]}_{p}$ $\underbrace{5 - 4x + x^2 + 2\mathbb{Z}[x]}_{q}$))

$p(x) - q(x) = -4 + 2x + 2x^2 \in 2\mathbb{Z}$

so $p(x) + 2\mathbb{Z}[x] = q(x) + 2\mathbb{Z}[x]$

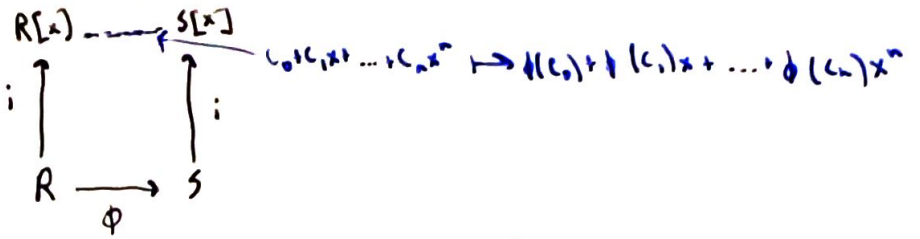
$p(x) = 1 - 2x + 3x^2 \in \left(\frac{\mathbb{Z}}{2\mathbb{Z}}\right)[x]$

$q(x) = 5 - 4x + 1x^2 \in \left(\frac{\mathbb{Z}}{2\mathbb{Z}}\right)[x] \Rightarrow p(x) = q(x)$

proof: we'll find a hom. $R[x] \to (R/I)[x]$

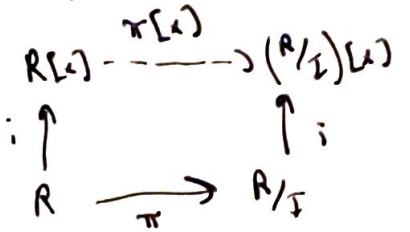
side lemma: If $\phi: R \to S$ is a hom. then

there is a unique hom.



we have the natural proj. $\pi: R \to R/I$

$\Rightarrow$ have



units in $R[x]$

$f(x) = c_0 + c_1x + \dots + c_nx^n$

c_0: unit in R; $c_1, \dots, c_n$: nilpotents in R

in $\mathbb{Z}_4[x]$

$c_0 = 1, 3$, $c_i = 0, 2$, $\forall i \geq 1$

Today: Division!

Division algorithm: in $\mathbb{Z}$:

For any $a, b \in \mathbb{Z}$ there are integers $q, r \in \mathbb{Z}$

with

① $a = qb + r$

② either $r = 0$ or $|r| < |b|$

in $F[x]$ where F is a field

For any $f(x), g(x) \in F[x]$ where $g(x) \neq 0$

there are $q(x), r(x) \in F[x]$ with

① $f(x) = q(x)g(x) + r(x)$

② either $r(x) = 0$ or $\deg(r(x)) < \deg(g(x))$

Ex ① $f(x) = x^5 + 3x^3 + 5x^2 + 2x + 5$

$g(x) = 2x^3 + x^2 + 2x + 1$ in $\mathbb{Z}_7[x]$

divide $f(x)$ by $g(x)$

$$2x^3+x^2+2x+1 \;\overline{)\; x^5+0x^4+3x^3+5x^2+2x+5 \;}\; = 2x^2+4x+4 = q_1(x)$$

$$\begin{array}{r} x^5+4x^4+x^3+4x^2 \\ \hline 3x^4+2x^3+x^2+2x+5 \\ -3x^4+5x^3+3x^2+5x \\ \hline 0+4x^3+5x^2+4x+5 \\ 4x^3+2x^2+4x+2 \\ \hline 0+3x^2+0x+3 = 3x^2+3 = r_1(x) \end{array}$$

observe the first equation is easy to satisfy, the hard part is making $r<b$

In general, for an integral domain, a Euclidian function on R is a function $f: R\setminus\{0\} \to \mathbb{Z}_{\geq 0}$ such that $\forall a,b \in R$ with $b\neq 0$ there are elements $q,r \in R$ with

1) $a = qb+r$
2) either $r=0$ or $f(r)<f(b)$

① On $\mathbb{Z}$: $|\cdot|$ absolute value
② on $F[x]$, F a field: $\deg(\cdot)$ degree
③ F a field: $f: F\setminus\{0\} \to \mathbb{Z}_{\geq 0}$

$f(r)=1$ for all $r\neq 0$

An integral domain that can be endowed a Euclidean function, is called a Euclidean domain

For a general comm. ring, we can talk about "divisors"

A divisor of an element $a\in R$ is an element $d\in R$ such that $a=qd$ for some $q\in R$

we can write $d|a$ ("d divides a")

A common divisor of a and b is a divisor of a and b

$d|a$ and $d|b$

↳ can consider the set of common divisors

want to say "greatest common divisor" → but what does "greatest" mean?

Def: A greatest common divisor of 2 elements of $a,b\in R$ is a common divisor such that every other common divisor $d'\in R$ divides d i.e.

1) $d|a$ & $d|b$
2) if $d'|a$ and $d'|b$ then $d'|d$

Week 2 pt 2 #

Issues

1) Greatest common divisors might not be unique
2) Greatest common divisors might not exist

FACT: In a Euclidean domain

- greatest common divisors always exist (can be computed with division algorithm
- they are unique "up to unit"

If d and d' are gcd's for some elements,
then $d = ud'$ for some unit $u \in R$

In $\mathbb{Z}$, units: ± 1

then we can just choose the positive one
$\Rightarrow$ the gcd (a,b)

In $F[x]$ units: $f(x) = c_0$ $c_0 \in F \setminus \{0\}$

→ choose the gcd so the top-deg coeff is 1

$d(x) = x^n + c_{n-1}x^{n-1} + \dots + c_0$ "monic polynomial

Back to ex: 1

$f(x) = x^5 + 3x^3 + 5x^2 + 2x + 5$ $\quad g(x) = 2x^3 + x^2 + 2x + 1$

$f(x) = q_1(x)g(x) + \underbrace{3x^2 + 3}_{r_1(x)}$

$\Rightarrow \gcd(f,g) = \gcd(g, r_1)$

then divide g by r_1

$$
\begin{array}{r|l}
 & 3x + 5 \quad (q_2) \\
\hline
3x^2 + 0x + 3 & 2x^3 + x^2 + 2x + 1 \\
 & 2x^3 + 0 + 2x \\
\hline
 & x^2 + 1 \\
 & x^2 + 1 \\
\hline
 & 0 \quad (r_2)
\end{array}
$$

so $\Rightarrow$ a gcd of f, g is

$r_1(x) = 3x^2 + 3$

$\Rightarrow$ the $\gcd(f,g) = x^2 + 1$

$f(x) = x^5 + 3x^3 + 5x^2 + 2x + 5 = (x^2+1)(x+2)^2(x+3)$

$g(x) = 2x^3 + x^2 + 2x + 1 = (2x+1)(x^2+1)$