Last time:

R = comm. ring

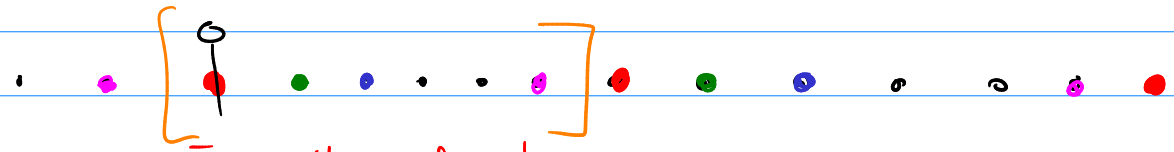
$I \subset R$ an ideal

$a \equiv b \pmod{I}$ means $a - b \in I$

$\bar{a} = \{ b \in R \mid a \equiv b \pmod{I} \}$ (depends on I!)

quotient ring $R/I = \{ \bar{a} \mid a \in R \}$

$R = \mathbb{Z}$ $I = \langle 6 \rangle$



$\bar{0}$ is the red set

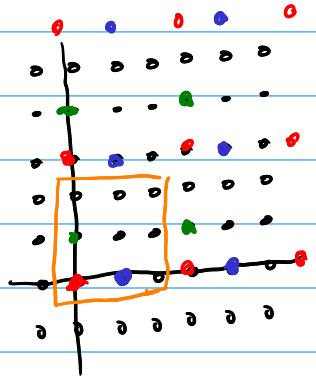
$\bar{1}$, $\bar{2}$ $\bar{-1} = \bar{5}$

$R/I = \mathbb{Z}_6$

in $\mathbb{Z}/\langle 6 \rangle$ aka $\mathbb{Z}_6$

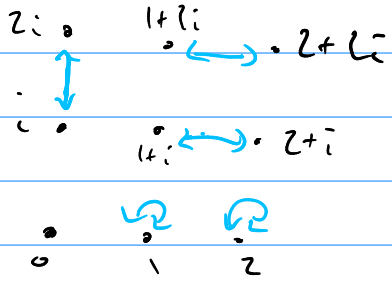
$\bar{3} \cdot \bar{5} = \overline{15} = \bar{3}$

$R = \mathbb{Z}[i]$ $I = \langle 3 \rangle$



$\bar{0} = \langle 3 \rangle$

$\bar{1}$ $\bar{i}$



$2 \cdot 2 = 4 \equiv 1 \pmod{3}$

$i \cdot 2i = -2 \equiv 1 \pmod{3}$

$(1+i)(2+i) = 2 + 3i - 1 = 1 + 3i$

$\equiv 1 \pmod{3}$

$(1+2i)(2+2i) = 2 + 6i - 4 = -2 + 6i \equiv 1 \pmod{3}$

R/I is a field with 9 elements.

quots of polynomial rings:

① $R = \mathbb{R}[x]$ $\quad I = \langle x^2+1 \rangle$

in the ring R/I, we have things like

$\overline{1}$, $\overline{2x+3}$, $\overline{4x-7}$, ...

$\overline{x^2+1} = \overline{0}$ $\qquad x^2+1 \equiv 0 \pmod{x^2+1}$

$\overline{x^2} = \overline{-1}$ $\qquad x^2 \equiv -1 \pmod{x^2+1}$

$$\overline{x^2+5x+6} = \overline{x^2} + \overline{5x+6} = \overline{-1} + \overline{5x+6} = \overline{5x+5}$$

given any polynomial $f = a_n x^n + a_{n-1}x^{n-1} + \cdots a_2 x^2 + a_1 x + a_0$

can divide by x^2+1 to get a quotient q and remainder r

$f = (x^2+1)q + r$ $\qquad \deg r < 2$

so $f \equiv r \pmod{x^2+1}$

every equiv. class has a unique elt. of deg < 2

find it by dividing by x^2+1 and taking remainder.

why??

how do we work in R/I?

take $\overline{3x+1}, \overline{2x-3} \in R/I$ "R mod I"

multiply: $\overline{6x^2-7x-3}$

divide by x^2+1 and get a remainder:

$$\begin{array}{r} 6 \\ x^2+1 \;\overline{)\,6x^2-7x-3} \\ 6x^2 \quad +6 \\ \hline -7x-9 \end{array}$$

$$\overline{6x^2-7x-3} = \overline{-7x-4}$$

$$6x^2-7x-3 \equiv -7x-9 \pmod{x^2+1}$$

easier: every time I see $\bar{x}^2$, turn it into -1

$$\overline{6x^2-7x-3} = \overline{-6-7x-3} = \overline{-7x-9}$$

uniqueness: if $f, g \in \mathbb{R}[x]$ with $\deg f < 2$ and $\deg g < 2$

then $f \equiv g \pmod{x^2+1}$ iff $f = g$.

Pf: $\deg(f-g) < 2$

So if x^2+1 divides $f-g$

then we must have

$f - g = 0 \cdot (x^2+1)$

$3x+1 \in R = \mathbb{R}[x]$

$2x-3 \in R$ as well.

So can talk about $\overline{3x+1} \in R/I$

by def, $\overline{3x+1} =$

$\{ g \in R \mid g \equiv 3x+1 \pmod{x^2+1} \}$

R/I looks a lot like $\mathbb{C}$

$3x+1 \longleftrightarrow 3i+1$

$2x-3 \longleftrightarrow 2i-3$

$\bar{x}^2 = \overline{-1}$ $\qquad$ $i^2 = -1$

---

another example: $R = \mathbb{R}[x]$ $\qquad$ $I = \langle x^2+x+1 \rangle$

now $\overline{x^2+x+1} = \bar{0}$ $\qquad$ so $\bar{x}^2 = \overline{-x-1}$

$$\overline{3x+1} \cdot \overline{2x-3} = \overline{6x^2-7x-3}$$

$$= \overline{6x^2} - \overline{7x} - \overline{3}$$

$$= \overline{-6x-6} - \overline{7x} - \overline{3}$$

$$= \overline{-13x-9}$$

Worksheet: practice in R/I

where $R = \mathbb{Z}_2[x]$ $\qquad$ $I = \langle x^3+x+1 \rangle$