Let k be a field, maybe $k = \mathbb{R}$.

Let $f \in k[x]$, $\deg \geq 1$

so $\langle f \rangle \subsetneq k[x]$

if f is reducible then $k[x]/\langle f \rangle$ has 0-divisors

if f is irreducible then $k[x]/\langle f \rangle$ is a field.

[Compare: Let $n \in \mathbb{Z}$ $n \neq 1, -1, 0$

if n is not prime then $\mathbb{Z}_n = \mathbb{Z}/\langle n \rangle$ has 0-dvs.

if n is prime then $\mathbb{Z}_n$ is a field.

Pf: if $f = g \cdot h$ where $\deg g, \deg h \geq 1$

then $\bar{g}, \bar{h}$ are not zero in $k[x]/\langle f \rangle$

because $g, h \notin \langle f \rangle$ for deg. reasons,

BUT, $\bar{g} \cdot \bar{h} = \bar{f} = \bar{0}$ in $k[x]/\langle f \rangle$.

(Example: $\overline{(x-5)(x-6)} = 0$ in $\mathbb{Q}[x]/\langle x^2 - 11x + 30 \rangle$)

if f is irreducible

take any $\bar{g} \in k[x]/\langle f \rangle$.

if $\bar{g} \neq \bar{0}$ then $g \notin \langle f \rangle$

so $f \nmid g$.

bec. f is irred

$\gcd(f, g) = 1$

so we can write $1 = f \cdot h + g \cdot k$

for some $h, k \in k[x]$

then $\bar{g} \cdot \bar{k} = \bar{1}$ in $k[x]/\langle f \rangle$

so $\bar{g}$ is a unit. ∎

Examples: on worksheet 5 you proved that $\mathbb{Z}_2[x]/\langle x^3+x+1\rangle$ was a field

$\bar{x}$, $\bar{x}^2$, $\bar{x}^3 = \bar{x}+1$, $\bar{x}^4 = \bar{x}^2+\bar{x}$

$\bar{x}^5 = \bar{x}^3+\bar{x}^2 = \bar{x}^2+\bar{x}+1$

$\bar{x}^6 = \bar{x}^3+\bar{x}^2+\bar{x} = \bar{x}^2+1$

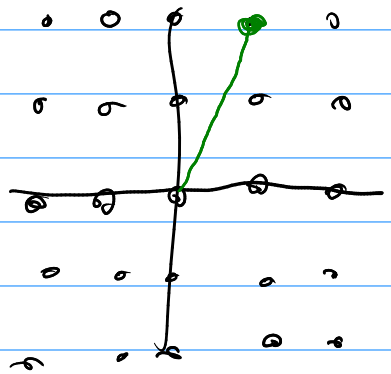
$\bar{x}^7 = 1$

so $\bar{x}^{-1} = \bar{x}^6$ $\bar{x}^{-2} = \bar{x}^5$ etc.

Upcoming HW features $\mathbb{Z}_2[x]/\langle x^2+x+1\rangle$

Gaussian Integers

$\mathbb{Z}[i] = \{a+bi \mid a,b \in \mathbb{Z}\}$



like $\mathbb{Z}$, and $F[x]$, it has a division algorithm.

if $z = a+bi$ then $|z|^2 = a^2+b^2$

$|z| = \sqrt{a^2+b^2}$

Thm: given $z, w \in \mathbb{Z}[i]$ with $w \neq 0$

$\exists\, q, r \in \mathbb{Z}[i]$ s.t. $z = qw + r$

and $|r|^2 < |w|^2$

think: $\frac{z}{w}$ is q, with remainder r

Example: $z = 8+5i$ $\quad w = 5+6i$

take $\frac{z}{w} = \frac{8+5i}{5+6i} \cdot \frac{(5-6i)}{(5-6i)} = \frac{70-23i}{25+36=51}$

$$= \frac{70}{51} - \frac{23}{51}i$$

round it to get $q = 1+0i$

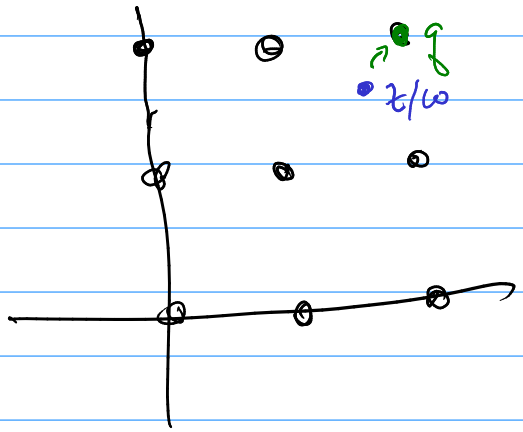
want $z = qw + r$

so $r = z - qw = (8+5i) - 1(5+6i)$

$$r = 3 - i$$

In general:

- Take $\frac{z}{w}$, write as $x+iy$ where $x, y \in \mathbb{Q}$
- Round x and y to get q.
- Take $r = z - qw$.



Why does it work?

Claim: $\left|\frac{z}{w} - q\right| < 1$

Pf: $\frac{z}{w} = x+iy$

$q = a+bi$ where $|x-a| \le \frac{1}{2}$ and $|y-b| \le \frac{1}{2}$

so $\left|\frac{z}{w} - q\right| = |(x-a)+(y-b)i|$

$$= \sqrt{(x-a)^2 + (y-b)^2} \le \sqrt{\frac{1}{4}+\frac{1}{4}} = \sqrt{\frac{1}{2}} = \frac{\sqrt{2}}{2} < 1$$

($(x-a)^2 \le 1/4$, $(y-b)^2 \le 1/4$)

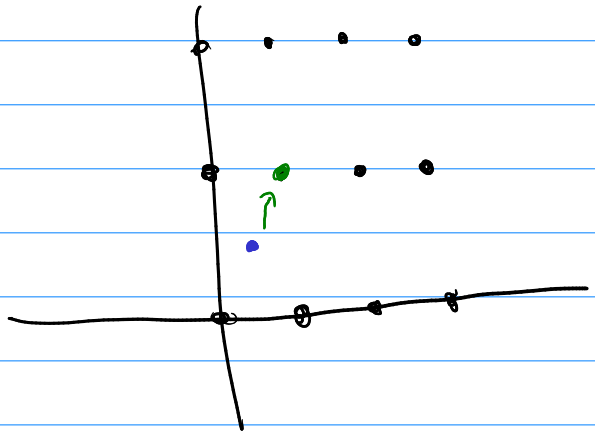
If we put $r = z - qw = \left(\frac{z}{w} - q\right) \cdot w$

then $|r| = \left|\frac{z}{w} - q\right| \cdot |w| < 1 \cdot |w|$

which is what we wanted.

=

same idea fails in $\mathbb{Z}[\sqrt{-5}]$



$\bullet = \frac{1}{2} + \frac{\sqrt{5}}{2} i$

$\omega = 1 + \sqrt{5}\, i$

distance is $\sqrt{\left(\frac{1}{2}\right)^2 + \left(\frac{\sqrt{5}}{2}\right)^2}$

$= \sqrt{\frac{1}{4} + \frac{5}{4}} = \sqrt{\frac{6}{4}} > 1$

In fact there can't be any div. alg. in $\mathbb{Z}[\sqrt{-5}]$

because 3 is irreducible and not prime there

and the ideal $\langle 2, 1+\sqrt{-5} \rangle$ is not principal.