Polynomials are like Integers (cont'd).

Last time: F a field

$f, g \in F[x]$ not both zero

Consider $S = \{$ all $F[x]$-linear combos of f and $g \}$

$= \{ fs + gt \mid s, t \in F[x] \}$

thm: $\exists\, d \in S$ such that

$S = \{$ all multiples of $d \}$

$= \{ du \mid u \in F[x] \}$

proof: let d be a non-zero element of S of minimal degree

($d \in S$, $d \neq 0$, $\forall e \in S$ have $\deg d \leq \deg e$)

① every multiple of d is in S

write $d = fs + gt$ for some $s, t \in F[x]$

then $du = fsu + gtu$ so $du \in S$

② f is a multiple of d:

otherwise, divide f by d and write

$f = qd + r$ where $r = 0$ or $\deg r < \deg d$

if $r=0$ then $d \mid f$

if $r \neq 0$ then $r = f - qd$

$$= f - q(fs + gt)$$

$$= f(1 - qs) + g(-t)$$

So $r \in S$, contradicting our choice of d as a non-zero element of min. deg.

(3) Similarly $d \mid g$

(4) So d divides every element of S:

if $f = d \cdot a$ and $g = d \cdot b$

then an arbitrary element of S:

$$fs + gt = das + dbt = d(as + bt)$$ $\boxtimes$

Comment: the statement is almost always false in $R[x]$ if R is not a field.

e.g. $R = \mathbb{Z}$ and $f = x$, $g = 2$ in $\mathbb{Z}[x]$

e.g. $R = F[y]$ and $f = x$, $g = y$ in $R[x] = F[x,y]$

another project idea!

As with integers, the Euclidean alg finds such an element of min. deg. and we call it $\gcd(f,g)$

could have found gcd by factoring, but that's harder:

from worksheet

$f = x^3 - 1 = (x-1)(x^2+x+1)$ in $\mathbb{Q}[x]$

$g = x^4 + x^3 - x^2 - 2x - 2 = (x^2-2)(x^2+x+1)$

$\gcd = x^2 + x + 1$ but factoring is hard!

you found $\gcd = -x^2 - x - 1$ via Eucl. alg.

notice: $\{fs + gt\}$

$= \{$all multiples of $x^2+x+1\}$

$= \{$all multiples of $-x^2-x-1\}$

similarly, with

$f = x^2 + (1-\sqrt{2})x - \sqrt{2} \quad \in \mathbb{R}[x]$

$= (x+1)(x-\sqrt{2})$

$g = x^2 - 2$

$= (x+\sqrt{2})(x-\sqrt{2})$

$\gcd = x - \sqrt{2}$ you found $(1+\sqrt{2})x + (2-\sqrt{2})$

mine = yours $\cdot (1+\sqrt{2})$

yours = mine $\cdot (-1-\sqrt{2})$

the point: $1+\sqrt{2}$ is a unit in $\mathbb{R}[x]$

---

next thing we did in $\mathbb{Z}$: primes + unique factorization

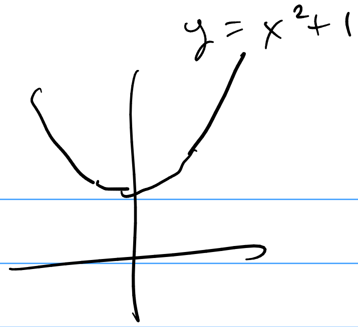
Def let F be a field

a poly. $f \in F[x]$ is irreducible

if it can't be factored as

$f = g \cdot h$

where $\deg g \geq 1$ and $\deg h \geq 1$



Example: in $\mathbb{R}[x]$, take $f = x^2+1$

can write $f = 1 \cdot (x^2+1)$

$= -1 \cdot (-x^2-1)$

$= \frac{1}{2} \cdot (2x^2+2)$

but that's silly.

analogy in $\mathbb{Z}$:

$5 = 1 \cdot 5$

$= (-1) \cdot 5$

but that's silly

can't write $f = (x+a)(x+b)$
bec. it has no roots in $\mathbb{R}$

OTOH, $x^2-1 = (x+1)(x-1)$ is reducible

$6 = 2 \cdot 3$

it matters what coefficient field you take:

in $\mathbb{C}[x]$, $x^2+1 = (x+i)(x-i)$

$5 = (2+i)(2-i)$

in $\mathbb{Z}[i]$

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

Prop. (Euclid's lemma):

if f is irred and $f \mid gh$
then $f \mid g$ or $f \mid h$.

Proof: on worksheet.