Polynomials are like Integers (cont’d).

Last time: \( F \) a field

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

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

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

then \( f \in S \) such that

\[ S = \{ \text{all multiples of } d \} \]

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

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

\( \deg S, d \neq 0, d \in S \) 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 $d | f$

if $r \neq 0$ then $r = f \cdot q + d = f - q_1 = f - q_1 (f_1 + q_2 t) = f (1 - q_1) + q_2 t$

so $r \in S$, contradicting our choice of $d$ as a non-zero element of $M_n$. 

3. Similarly $d | g$

4. so $d$ divides every element of $S$:

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

then an arbitrary element of $S$:

$$f + g t = d a s + d b t = d (a s + b t)$$

$$\text{Comment: the statement is false in } R[x, y]$$

if $R$ is not a field.

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

eg. $R = E[y]$ and $f = x$, $g = y$ in $R[x] = E[x, y]$

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:

\[
f = x^2 - 1 = (x - 1)(x^2 + x + 1) \quad \in \mathbb{Q}[x]
\]
\[
g = x^4 + x^3 - x^2 - 2x - 2 = (x^2 - 2)(x^2 + x + 1)
\]
\[
\gcd = x^2 + x + 1 \quad \text{but factoring is hard!}
\]
you found \( \gcd = -x^2 - x - 1 \) \( \nu \mathbb{Q} \) Eucl. alg.

\[
\text{not:} \quad \{ f + g \mathbb{Z}[x] \}
\]
\[
= \{ \text{all multiples of } x^2 + x + 1 \}
\]
\[
\Rightarrow \{ \text{all multiples of } -x^2 - x - 1 \}
Similarly, with

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

\[ g = x^2 - 2 \]
\[ = (x + \sqrt{2})(x - \sqrt{2}) \]

\[ \text{gcd} = x - \sqrt{2} \quad \text{you found} \quad (1 + \sqrt{2})x + (2 - \sqrt{2}) \]

\[ \text{mine} = \text{yours} \cdot (1 + \sqrt{2}) \]

\[ \text{yours} = \text{mine} \cdot (-1 - \sqrt{2}) \]

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

\[ \text{---} \]

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 \( f = x^2 + 1 \)

\[ f = 1 \cdot (x^2 + 1) \]

\[ = -1 \cdot (-x^2 - 1) \]

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

Can write \( f \) but that's silly.

\[ \text{Analogy in } \mathbb{Z}^*: \]

\[ 5 = 1 \cdot 5 \]

\[ = (-1) \cdot 5 \]

But that's silly.

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

\[ \text{Otoh, } x^2 - 1 = (x+1)(x-1) \text{ is reducible} \]

\[ 6 = 2 \cdot 3 \]

It matters what coefficient field you take:

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

\[ 5 = (2+i)(2-i) \]

\[ \text{in } \mathbb{Q}(i) \]

\[ \big\{ a + bi \mid a, b \in \mathbb{Q} \big\} \]

Prop. (Euclid's lemma):

if \( f \) is irreducible in \( \mathbb{F}[x] \) then \( f|g \) or \( f|h \).

Proof: on worksheet.