Math 3032 Lecture 13 (4 March 2021)

No lecture next week.

Two HW sets, one of them optional, due in 2 weeks.

Last time: One of the most theorems in the course:

(0) If F is a field then $F[x]$ has long division. "Euclidean domain" ← uses that we have good control over "deg".

(1) If R is an integral domain w/ long division, then R is a principal ideal domain. ← every ideal is principal.

(2) If R is a PID, then R has unique factorization.

None of these are iff. E.g. $F[x,y]$ is a UFD but not PID.

$f(x) = x^4 + 2x^3 - 9x^2 + x + 2$

$g(x) = x^3 + 2x^2 - 3x - 6$.

$I = \langle f(x), g(x) \rangle$

So I contains all polys of the form

$r(x)f(x) + s(x)g(x)$.

Lemma: The set of polys of form $r(x)f(x) + s(x)g(x)$ is an ideal.

Pf: $(r_1 f + s_1 g) + (r_2 f + s_2 g) = (r_1 + r_2) f + (s_1 + s_2) g$

so this set is additive. and $\forall t \in \mathbb{R}[x]$

$t(x) \cdot (r(x)f(x) + s(x)g(x)) = (t \cdot r) f + (t \cdot s) g$.

So this set is an ideal.

So this is the ideal I.

Cor: Suppose $\alpha \in \mathbb{R}$ which is a common zero of f, g.

i.e. s.t. $f(\alpha) = g(\alpha) = 0$. If $p(x) = r(x)f(x) + s(x)g(x)$

then $p(\alpha) = r(\alpha) \cdot 0 + s(\alpha) \cdot 0 = 0$.

$f(x) = x^4 + 2x^3 - 9x^2 + x + 2$ $\quad I = \langle f(x), g(x) \rangle$

$g(x) = x^3 + 2x^2 - 3x - 6$. $\quad = \{ r(x)f(x) + s(x)g(x) \}$

Cor: Suppose $\alpha \in \mathbb{R}$ which is a common zero of f, g.
i.e. s.t. $f(\alpha) = g(\alpha) = 0$. If $p(x) = r(x)f(x) + s(x)g(x)$
is in $p(\alpha) = r(\alpha) \cdot 0 + s(\alpha) \cdot 0 = 0$.

i.e.: If $p(x) \in I$, then any common zero of $f(x)$ and $g(x)$ is also a zero of $p(x)$.

Also: If $I = \langle p(x) \rangle$ i.e. if we have found a gen as a principal ideal

then $f(x) \in I$ so $f = a(x) \cdot p(x)$ $\quad g = b(x) \cdot p(x)$

So any zero of p will be a zero of both f and g.

$f(x) = x^4 + 2x^3 - 9x^2 + x + 2$

$g(x) = x^3 + 2x^2 - 3x - 6.$

From last time: p will be the smallest-deg elt of I.

we want to find $p(x)$ s.t. $\langle p(x) \rangle = \langle f(x), g(x) \rangle$.

Let's just try to find small elts?

(0) maybe $g = p$?

$g \in \langle g \rangle$ ✓.

is $f \in \langle g \rangle$? i.e. is $f = z \cdot g$? No!

$f(x) - x \cdot g(x)$

$= -6x^2 + 7x + 2 =: r(x)$

Learned: • $\langle g \rangle \neq \langle f, g \rangle$.

• $r(x) \in \langle f, g \rangle$.

$f(x) = x \cdot g(x) + r(x)$.

Contrived example:

Let's work in $\mathbb{R}[x]$, and ask:

what is the smallest ideal I containing both

$$f(x) = x^4 + 2x^3 - 9x^2 + x + 2$$

and

$$g(x) = x^3 + 2x^2 - 3x - 6.$$

$I = \langle f(x), g(x) \rangle$ ← angle brackets notation for the smallest ideal containing both.

$f \in I$, $g \in I$.

for any $r(x) \in \mathbb{R}[x]$, $r(x) \cdot f(x) \in I$.

$s(x) \in \mathbb{R}[x]$ $s(x) \cdot g(x) \in I$

i.e. "understand" this ideal in more explicit terms.

in particular, "success" will mean to find $p(x)$ s.t.

$I = \langle p(x) \rangle$

So I contains all polys of the form

$r(x)f(x) + s(x)g(x)$.

$f(x) = x^4 + 2x^3 - 9x^2 + x + 2$

$6g(x) = 6x^3 + 12x^2 - 18x - 36.$

$r(x) = -6x^2 + 7x + 2$

$f(x) = x \cdot g(x) + r(x).$

Learned: • $\langle g \rangle \neq \langle f, g \rangle$.

• $r(x) \in \langle f, g \rangle$.

$g \in I$ iff $6g \in I$.

$f \in \langle g, r \rangle$ because $\langle 6g, r \rangle$ ↰

Conclusion: $\langle f, g \rangle = \langle g, r \rangle$.

Let's write $6g = q \cdot r + s$. Then $\langle g, r \rangle = \langle r, s \rangle$.

Keep going.

$6g(x) = -x \cdot r(x) + \underbrace{19x^2 - 16x - 36}_{s}.$

$I = \langle -6x^2 + 7x + 2,\ 19x^2 - 16x - 36 \rangle.$

$f(x) = x^4 + 2x^3 - 9x^2 + x + 2$

$6g(x) = 6x^3 + 12x^2 - 18x - 36.$

$r(x) = -6x^2 + 7x + 2$

$I = \langle -6x^2 + 7x + 2,\ 19x^2 - 16x - 36 \rangle.$

$= \langle r' = 19 \cdot (-6)x^2 + 133x + 38,\ 5r' = 19 \cdot 6\, x^2 - 96 - 216 \rangle$

$= \langle r' = \text{gcd},\ 5+r' = 37x - 78 \rangle$

Eventually you must end w/ no remainder

$\therefore\ I = \langle p(x),\ 0 \rangle = \langle p(x) \rangle.$

if $p \mid f, g$, then $f, g \in \langle p \rangle$ so $I \subseteq \langle p \rangle$.

$I = \langle f, g \rangle$

Euclid's algorithm.

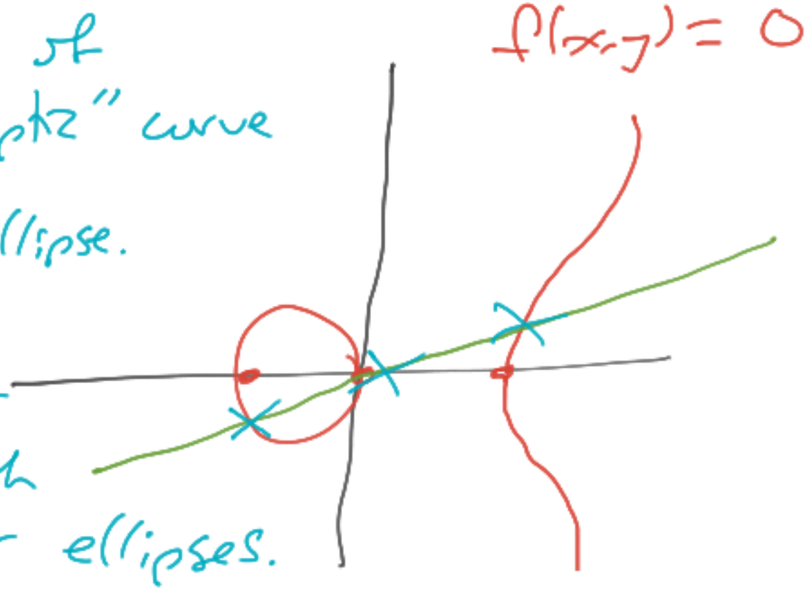
Generator p of $\langle f, g \rangle$ is the gcd of f and g.

In algebraic geometry, what you're interested in are understanding the common solutions to some set of polynomials (in multiple variables).

$$f(x,y) = y^2 - (x^3 - x)$$

$$g(x,y) = 2y - x$$

three common zeros



↙ example of an "elliptic" curve

not an ellipse.

rather it's related to the arclength problem for ellipses.

Sets of zeros of polys $\subseteq$ "algebraic varieties".

$V(f,g) :=$ common zeros of $f, g. \subseteq \mathbb{R}^2$ or $\mathbb{C}^2$.

If $\vec{\alpha} \in V(f,g)$ and $p \in \langle f, g \rangle$ then $p(\vec{\alpha}) = 0$.

So $V(f,g)$ only depends on $\langle f,g \rangle = I$.

i.e. given ideal $I \subseteq \mathbb{R}[x_1, \ldots, x_n] = "\mathbb{R}[\vec{x}]"$

[or use $\mathbb{C}$]

get an alg variety $V(I) \subseteq \mathbb{R}^n$ "vanishing locus of I"

$=$

$\vec{\alpha} \in \mathbb{R}^n$ s.t. $p(\vec{\alpha}) = 0$ for all $p(\vec{x}) \in I$.

$=$

vanishing locus of any generating set for $I := \langle f_1(\vec{x}), \ldots, f_k(\vec{x}) \rangle$

Asides:

- Hilbert showed: every ideal in $\mathbb{R}[x_1, \ldots, x_n]$ is finitely generated.
- A basis for I is any generating set like $\uparrow$.

Warn: no "linear independence" requirement.

Ideals in $\mathbb{R}[x_1, \ldots, x_n]$ $\longrightarrow$ subsets of $\mathbb{R}^n$

I $\longmapsto$ $V(I)$.

ideals in $\mathbb{R}[x_1, \ldots, x_n]$ $\longleftarrow$ subsets of $\mathbb{R}^n$

$\{ f(\vec{x}) \in \mathbb{R}[\vec{x}]$ $\longleftarrow|$ $A \subseteq \mathbb{R}^n$

s.t. $f(\vec{\alpha}) = 0$ for all $\vec{\alpha} \in A \} =: \mathcal{I}(A)$

$\mathcal{I}$ obviously an ideal because $0+0=0$

$0 \cdot \text{anything} = 0$.

These $\rightleftarrows$ not inverse functions in any sense.

If $I \subseteq J$, then $V(I) \supseteq V(J)$

and if $A \subseteq B$, then $\mathcal{I}_A \supseteq \mathcal{I}_B$.

So $V \rightleftarrows \mathcal{I}$ are a "Galois correspondence":

↑ they reverse order of inclusion.

$$\mathcal{I}(V(I)) \supseteq I.$$

$$V(\mathcal{I}(A)) \supseteq A.$$

$V, \mathcal{I}$ are "adjoint".

Back to one variable.

$\mathbb{C}[x]$.

FTA: every poly has solns in $\mathbb{C}$.

$\Rightarrow$ only irred polys are linear terms.

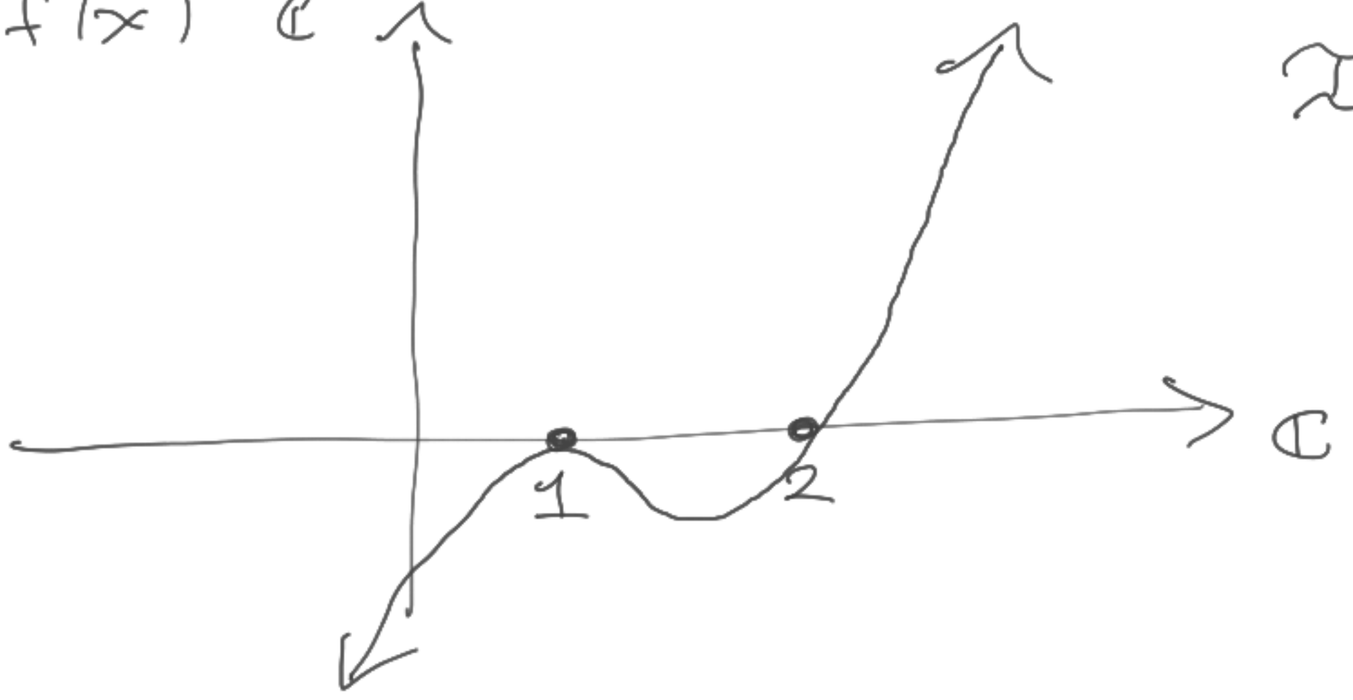
$f(x) = (x-1)^2 \cdot (x-2)$

$V(f) = \{1, 2\}$.

$\mathcal{I}_{\{1,2\}} = \langle (x-1)\cdot(x-2) \rangle$

graph:

$y = f(x)$ $\mathbb{C}$



$\mathbb{C}[x]$ is very similar to $\mathbb{Z}$.

e.g. both have long division.

In $\mathbb{C}[x]$, irreds = linear functions = points in $\mathbb{C}$.

irreds: up to rescaling = maximal ideals

linear functions: up to rescaling

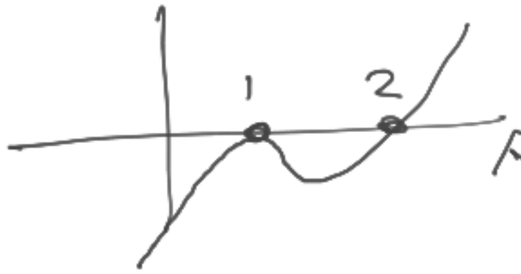
$(x-\alpha) \longleftrightarrow \alpha \in \mathbb{C}$.

In $\mathbb{Z}$, irreds up to rescaling = positive prime numbers $= \{2, 3, 5, \dots\}$.

$\langle -2 \rangle = \langle 2 \rangle$

Thought of

$(x-1)^2(x-2)$



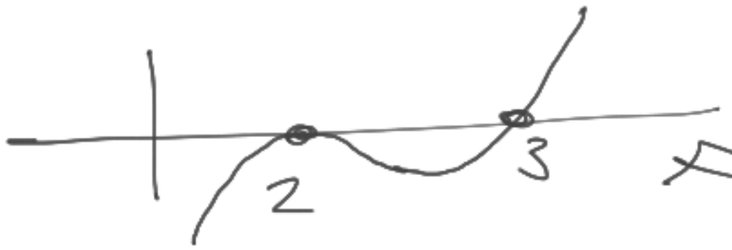
$\subset$ x-axis $= \mathbb{C}$

y-axis $= \mathbb{C}$

by analogy, I want to invite you to think about integers as "functions".

$12 = 2^2 \cdot 3$

"graph of 12"



$\subset$ x-axis is set of prime numbers 2, 3, 5, 7, 11, ...

y-axis ??

$12(p)$ = residue of 12 mod p.

So at $p \in$ x-axis, y-axis is $\mathbb{Z}_p$.

A com. unital ring R is Noetherian if every ideal is finitely generated. E.g. field trivially Noeth. only ideals are $(0), (1)$.

Abstract version of Hilbert's basis thm is:

if R is Noetherian then $R[x]$ is.