Math 3032: 25 March 2021

HW8 due Tuesday.

When can you promote a property of a ring R ("niceness") to $R[x]$?

i.e. for niceness properties is it true that property for R $\Rightarrow$ property for $R[x]$?

Examples

- integral domain
- UFD
- Noetherian

Non-examples

- field
- PID — $\mathbb{Z}[x]$, $\mathbb{F}[x,y]$ not PIDs.

Goal: If R is a UFD then $R[x]$ is a UFD.

Corollaries: $\mathbb{Z}[x]$ is a UFD. $\mathbb{C}[x,y]$ is a UFD
$\mathbb{Z}[x_1,\ldots,x_7]$ is a UFD.

in fact, we will supply "algorithm" for factorization.

Strategy: If R a UFD, certainly an integral domain.
Set $\mathbb{F} :=$ field of fractions of R.
$R \hookrightarrow \mathbb{F}$ (e.g. $R = \mathbb{Z}$, $\mathbb{F} = \mathbb{Q}$) and so $R[x] \hookrightarrow \mathbb{F}[x]$
(injection)
$\mathbb{F}$ a field $\Rightarrow \mathbb{F}[x]$ is a UFD.
Given $f(x) \in R[x]$, factor in $\mathbb{F}[x]$. Promote to a factorization over R. Study uniqueness.
Require: Compare irreducibility in $R[x]$ vs. $\mathbb{F}[x]$.

Defn: Given a set of elements $a_0, \ldots, a_n \in R$, a **greatest common divisor** g of the set is an elt of R s.t. $g \mid a_i \ \forall i$ and if $r \mid a_i \ \forall i$ then $r \mid g$. ← "universal property"

E.g.: $4, -6 \in \mathbb{Z}$ 2 and -2 are both gcds.

Lemma: Any two gcds are associate.

Pf: if g_1 and g_2 are gcds of same set, then $g_1 \mid g_2$ and $g_2 \mid g_1$.

Lemma: If R a UFD, then gcds exist.

Pf: Factor all the a_i and take "intersection" (product of) of their factors.

Defn: Given $f(x) = a_0 + a_1 x + a_2 x^2 + \dots + a_n \in R[x]$, define the content of f to be gcd(coeffs).

↳ defined up to association.

$f(x)$ is primitive if its content "is" 1. — i.e. content is invertible.

↙ up to association

Lemma: Any poly will factor uniquely as

$f(x) = \underbrace{(\text{content of } f)}\cdot(\text{primitive})$.

↑ $R \subseteq R[x]$ ← constant polynomials.

uses that any factorization of a constant is into const. factors.

by assumption, content of f does have a unique factorization.

In particular, if $f \in R[x]$ is nonconstant and irred, then it is primitive.

Lemma (Gauss): If $f(x)$ and $g(x)$ $\in R[x]$ are primitive then $(f\cdot g)(x)$ is primitive. (Assuming R is a UFD.)

N.B: If f or g is not primitive, then certainly $f\cdot g$ is not primitive.

Pf: Let $f(x) = a_0 + a_1 x + \dots + a_m$, $g(x) = b_0 + \dots + b_n x^n$.

$(f\cdot g)(x) = c_0 + \dots + c_{m+n} x^{m+n}$, $\quad c_k = \sum_{i+j=k} a_i b_j$

WTS: $\forall p$ irred, $p \nmid$ some c_k.

Since f, g is primitive, $\exists a_i, b_j$ s.t. $p \nmid a_i, b_j$. Set r, s = smallest i, j s.t. $p \nmid a_r$. $p \nmid b_s$.

$$c_{r+s} = \sum_{\substack{i=0 \\ \cancel{i+j=r+s}}}^{r+s} a_i b_j \quad (j = r+s-i) \quad = \sum_{i=0}^{r-1} a_i b_{r+s-i} + a_r b_s + \sum_{j=0}^{s-1} a_{r+s-j} b_j$$

(p divides all these; p does not divide $a_r b_s$; p divides these)

So p does not divide c_{r+s}. $\square$.

Prop: Suppose $f(x) \in R[x]$ is nonconstant and primitive. Then $f(x)$ is irred in $R[x]$ iff $f(x)$ is irred in $\mathbb{F}[x]$.

Pf: ($\Leftarrow$) If f factors in $R[x]$, then it factors into (primitive) nonconstants.
This would also provide a nontrivial factorization in $\mathbb{F}[x]$.

($\Rightarrow$) Suppose $f(x) = r(x) \cdot s(x)$ in $\mathbb{F}[x]$.

$$r(x) = \frac{a_1}{a_2} r_1(x), \quad \text{and} \quad s(x) = \frac{b_1}{b_2} s_1(x)$$

where $r_1(x), s_1(x) \in R[x]$ primitive
a_1/a_2 , $b_1/b_2 \in \mathbb{F}$.

Clearing denominators:

$$(a_2 \cdot b_2) \cdot f(x) = a_1 \cdot b_1 \, r_1(x) \, s_1(x).$$

Compare contents. Since $f(x)$ primitive,

content(LHS) $= a_2 \cdot b_2$ content(RHS) $= a_1 \cdot b_1$

So $a_2 b_2 \sim a_1 b_1$

So $f(x) = u \cdot r_1(x) \, s_1(x)$. □

We showed: If f primitive factors over $\mathbb{F}$, then it factors over R with factors of <u>same degree</u>.

Thm: If R is a UFD, then $R[x]$ is.

Pf: Given $f(x) \in R[x]$, saw that factorization $f(x) = \underbrace{\text{content}} \times \text{primitive}$ is unique (up to $\sim$).
↪ factors uniquely in R.

So suffices to show that factorization of primitives is unique. So assume $f(x)$ primitive.

Pick factorization $f(x) = p_1(x) \cdots p_n(x)$ with as many factors as possible. (cannot be more than $\deg(f)$ factors, so a maximum does exist.)
Automatically: all $p_i(x)$ are irred.

So $\exists$ factorization into irreds.

We're left only with showing factorization is unique.

Suppose $f(x) = p_1(x) \cdots p_m(x) = q_1(x) \cdots q_n(x)$

are factorizations in $R[x]$ into irreds.

Since f assumed primitive, p_i's and q_j's are primitive,

so these are factorizations into irreducibles

in $\mathbb{F}[x]$. That means that up to reordering

$p_i(x) \underset{\mathbb{F}}{\sim} q_i(x)$ are associate over $\mathbb{F}$.

unit in R.

i.e. $q_i(x) = \frac{a_i}{b_i} \cdot p_i(x)$.

$b_i q_i(x) = a_i p_i(x)$.

Compare content. $a_i \sim b_i$ associate in R.

$\square$

Thm (Hilbert basis thm):

If R is noetherian then $R[x]$ is noetherian.

↳ any ascending chain of ideals stabilizes.

↳ any ideal has a finite basis.

Pf: Let $I \subseteq R[x]$ be an ideal. Want to find a finite basis.

If $I = \{0\} =: I_0$ done. Else:

Set $f_1(x)$ to be an elt of $I \setminus I_0$ of minimal degree.

If $I = \langle f_1 \rangle =: I_1$ done.

Recall: in $\mathbb{F}[x]$, we showed PID. principal generator of I is any elt of I of minimal degree.

Else, pick $f_2(x) \in I \setminus I_1$ of minimal degree.

Set $I_2 := \langle f_1(x), f_2(x) \rangle$. If $I = I_2$ done.

Otherwise continue.

End up with a sequence

$$f_1(x), f_2(x), \ldots$$

possibly finite, possibly infinite. WTS it's finite.

Set $r_i :=$ leading coef of $f_i(x)$.

$$f_i(x) = a_{i0} + a_{i1}x + \ldots + \underbrace{a_{in}}_{\overset{!!}{r_i}} x^n.$$

r_i are a sequence in R.

Look at chain of ideals

$\langle r_1 \rangle \subseteq \langle r_1, r_2 \rangle \subseteq \ldots$ in R.

R noeth, this seq will stabilize.

Eventually, $\langle r_1, \ldots, r_{m+1} \rangle = \langle r_1, \ldots, r_m \rangle$.

i.e. $r_{m+1} \in \langle r_1, \ldots, r_m \rangle$ i.e. $\exists$ coefs (not unique)

$c_i \in R$ s.t. $r_{m+1} = \sum_{i=1}^{m} c_i r_i$

Now inspect $g(x) := \sum_{i=1}^{m} c_i f_i(x) \cdot x^{\overbrace{\deg f_{m+1} - \deg f_i}^{\geq 0}}$

$g(x)$: $\sum c_i r_i x^{\deg f_{m+1}}$ + ...

$c_i f_i(x) = (c_i r_i x^{\deg f_i} + \text{l.o.})$

$\deg f_j \leq \deg f_{j+1}$

$c_i \in R$ s.t. $r_{m+1} = \sum_{i=1}^{m} c_i r_i$

Now inspect $g(x) := \sum_{i=1}^{m} c_i f_i(x) \cdot x^{\deg f_{m+1} - \deg f_i}$ (exponent ≥ 0)

$g(x) = \sum c_i r_i x^{\deg f_{m+1}} + \dots$, where $c_i f_i(x) = (c_i r_i x^{\deg f_i} + \text{l.o.})$

$\sum_{i=1}^{m} c_i f_i(x) \cdot x^{\deg f_{m+1} - \deg f_i} \in I_m = \langle f_1(x), \dots, f_m(x) \rangle$

$f_{m+1}(x)$, if it exists is in I, but not in I_m, and of minimal degree w/ this property.

So $f_{m+1}(x) - g(x)$ is in $I \setminus I_m$.

Leading coefs of f_{m+1} and g agree.

So $\deg(f_{m+1}(x) - g(x)) < \deg f_{m+1}$. contradiction. ∎

What do these say in algebraic geometry?

Given set of polys in $\mathbb{C}[\underbrace{x_1, \dots, x_n}_{\text{e.g. } x,\, y}]$,

alg. geo wants to study common zeros of the set.

sets of com zeros "alg. varieties"

$\equiv$ common zeros of ideal generated by that set.

<u>HBT</u>: That ideal is $\langle \underbrace{f_1(\vec{x}), \dots, f_n(\vec{x})}_{\text{finite.}} \rangle$

i.e. $\exists$ finite set of polys s.t.

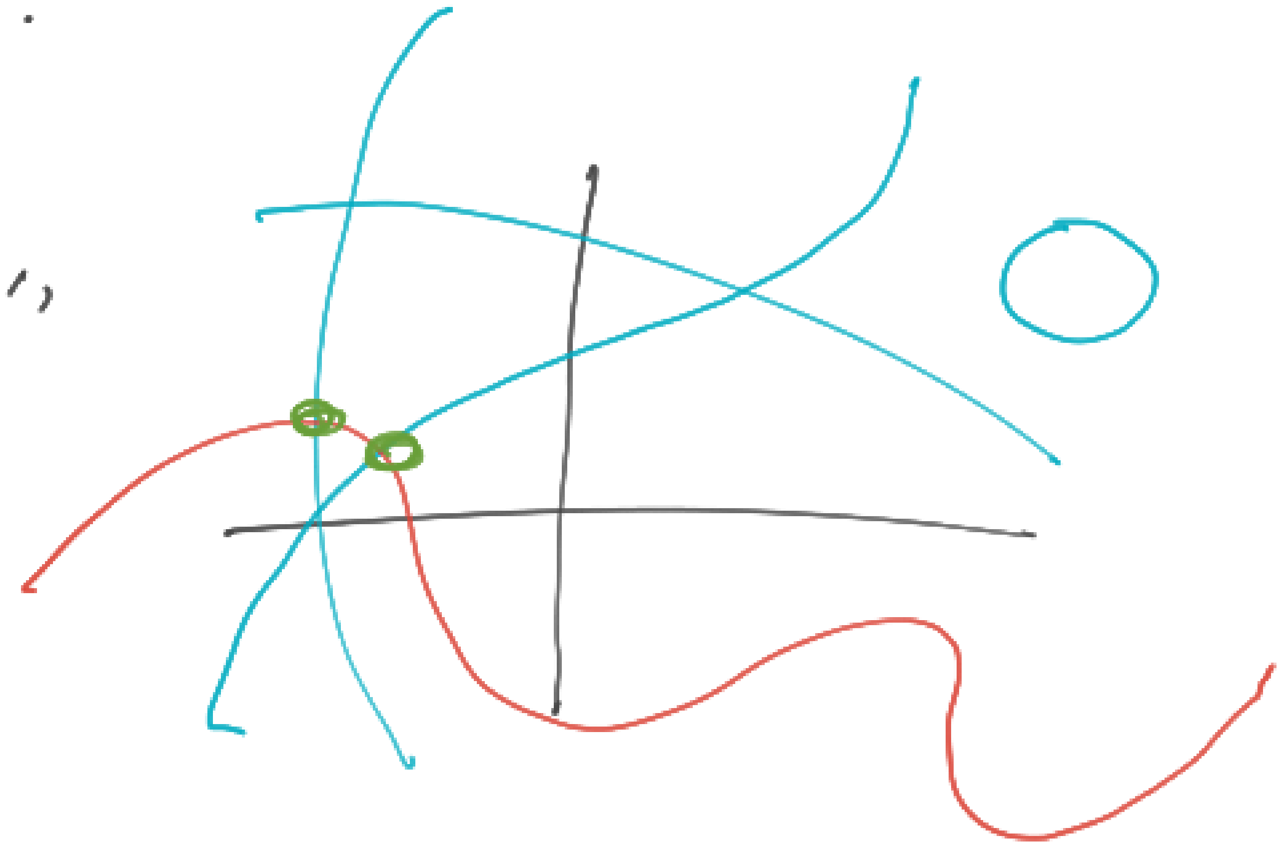
Your variety $=$ common solns to $f_1(\vec{x}) = 0$
and $f_2(\vec{x}) = 0$
and $\dots$ $f_n(\vec{x}) = 0$.

E.g. $\mathbb{R}[x,y] = \underbrace{\mathbb{R}[x]}_{UFD}[y]$ $\quad$ $f_2(x,y)=0$

a single equation $f_1(x,y)=0$.

$\updownarrow$

some "curve"



$$f_1(x,y) = p_1(x,y)\cdot p_2(x,y)$$

$$\{f_1(x,y)=0\} = \{p_1(x,y)=0\} \sqcup \{p_2(x,y)=0\}$$

products $\leftrightarrow$ unions

multiple basis elts $\leftrightarrow$ intersections.

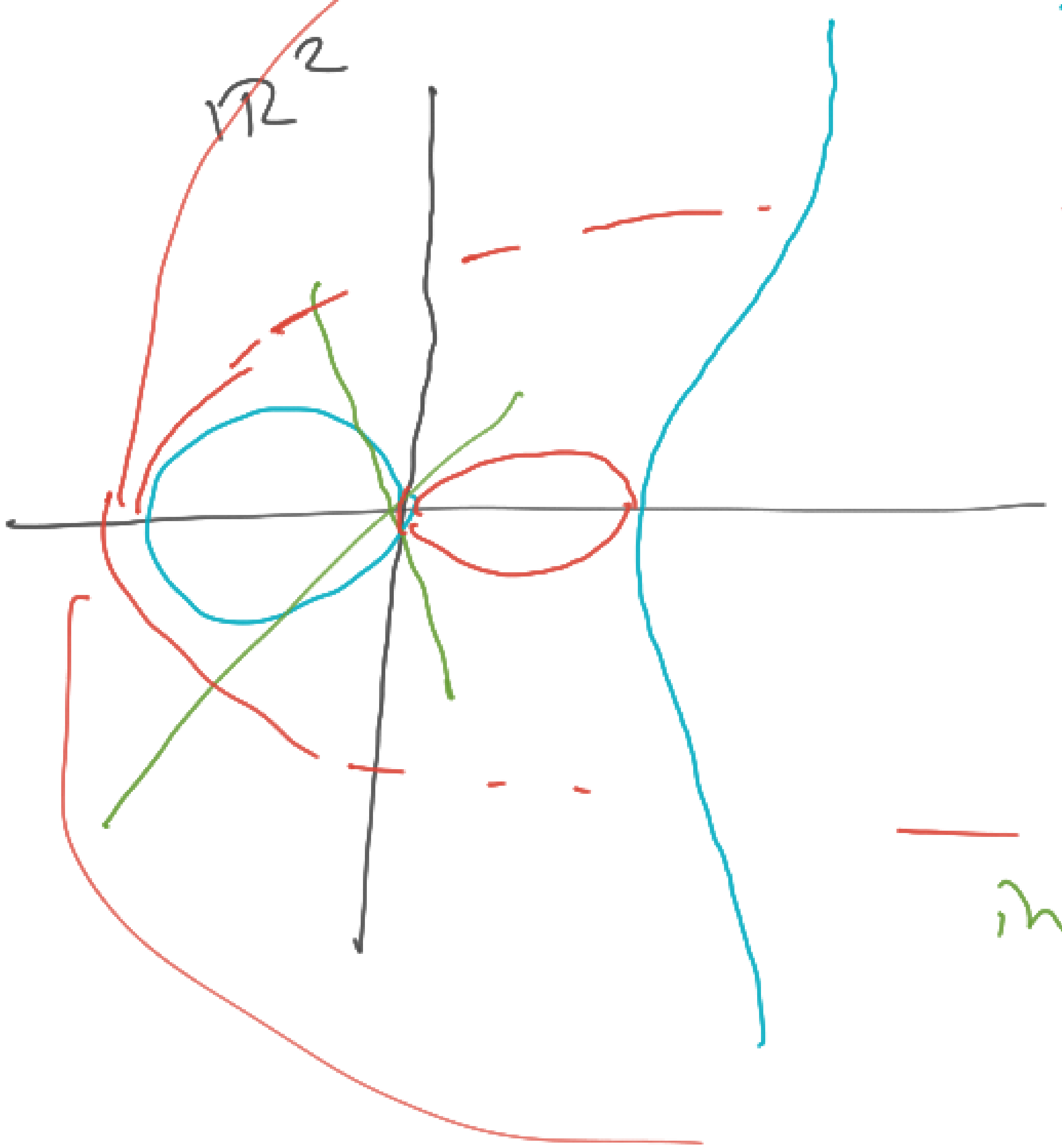
UFD geometrically:

Any single poly will have soln set which canonically is union of irred pieces. (smoother)

E.g.

$$y^2 - (x^3 - x) = 0$$

← irred.



So there do not exist polys whose solutions are just one pieces.

in $\mathbb{C}^2$ ← 4d.