

Last time:

$R$  is UFD  $\implies R[x]$  is UFD

$\vdots$   
 $\implies R[x_1, \dots, x_n]$  is UFD.

Today we will use this to study curves in the plane.



Idea: If  $\mathbb{F}$  is algebraically closed then an affine curve  $C \subseteq \mathbb{F}^2$  is determined by a unique "minimal polynomial"  $f(x, y) \in \mathbb{F}[x, y]$  with properties:

- $C = C_f : f(x, y) = 0$
- $C_f \subseteq C_g$  implies  $f \mid g$ .

In particular, if  $f, g$  are "square-free" polynomials (i.e., no repeated factors)

then  $C_f = C_g \iff f \sim g$ .


Remark: Algebraic closure is necessary. Consider  $F = x^2 + y^2$  and  $g = x$  with corresponding real curves  $C_F, C_g \in \mathbb{R}^2$ .

Then  $C_F = \{(0,0)\}$

$C_g = y\text{-axis}$ .

Hence  $C_F \subseteq C_g$ , but we clearly have  $x^2 + y^2 \not\equiv x$ . The problem is

that  $x^2 + y^2 = (x + iy)(x - iy)$ , so we should really think of  $C_F$  as a pair of "lines" in  $\mathbb{C}^2$ .

Thus  $C_F \not\subseteq C_g$ , which explains why  $F \not\equiv g$ . 

Sturdy's Lemma for Curves in the Affine plane (1889):

Let  $\mathbb{F}$  be algebraically closed.

Consider  $f, g \in \mathbb{F}[x, y]$ ,  $C_f, C_g \subseteq \mathbb{F}^2$ .

(a) If  $f$  is irreducible &  $f \nmid g$

then  $\#(C_f \cap C_g) < \infty$ . [ $\mathbb{F}$  arbitrary.]

(b) If  $f$  is irreducible &  $C_f \subseteq C_g$

then  $f \mid g$ .

(c) The same holds when  $\mathcal{F}$  is square-free. Get a bijection:

curves  $\subseteq \mathbb{F}^2 \iff$  square-free polynomials

(d) We say curve  $C \subseteq \mathbb{F}^2$  is irreducible if it cannot be a union of non-empty curves:  $C = C_1 \cup C_2$ .

Get a bijection:

irreducible curves  $\iff$  irreducible polynomials.  $\equiv$

Proof: Let  $f$  irreducible,  $f \nmid g$ .

Then  $f$  &  $g$  are coprime in  $\mathbb{F}[x, y]$ :

Smallest principal ideal containing

$$(f, g) := f\mathbb{F}[x, y] + g\mathbb{F}[x, y]$$

is the whole ring  $\mathbb{F}[x, y]$ . Now let

$\mathbb{F}(x) = \text{Frac}(\mathbb{F}[x])$  and consider

$$f, g \in \mathbb{F}[x, y] \subseteq \mathbb{F}(x)[y].$$

Claim:  $f$  &  $g$  are still coprime in the larger ring. Indeed, suppose

$p \mid f$  &  $p \mid g$  in  $\mathbb{F}(x)[y]$  for some

irreducible  $p \in \mathbb{F}(x)[y]$ . Since

$\mathbb{F}[x]$  is UFD (PID), it follows

from Gauss' Lemma that

$$p' \mid f' \text{ \& \ } p' \mid g' \text{ in } \mathbb{F}[x, y] = \mathbb{F}[x][y].$$

But this implies that  $p' \mid f$  &  $p' \mid g$ .

Contradiction.

Now since  $\mathbb{F}(x)$  is a field,  
 $\mathbb{F}(x)[y]$  is a PID, hence from  
Bézout's Identity,

$$fF + gG = 1$$

for some  $F, G \in \mathbb{F}(x)[y]$ . Let  
 $h(x) \in \mathbb{F}[x]$  be a common multiple  
of the denominators of the  $y$ -coeffs  
of  $F$  &  $G$ . Multiply by  $h(x)$  to get

$$f(x,y)\tilde{F}(x,y) + g(x,y)\tilde{G}(x,y) = h(x).$$

where  $\tilde{F}, \tilde{G} \in \mathbb{F}[x,y]$ . For any  
 $(a,b) \in C_f \cap C_g$ , we evaluate to get

$$f(a,b)\tilde{F}(a,b) + g(a,b)\tilde{G}(a,b) = h(a)$$

$$0 = h(a).$$

$\exists$  finitely many such  $a \in \mathbb{F}$ .

A symmetric proof using  $\mathbb{F}(y)[x]$  shows  $\exists$  finitely many such  $b$ .  $\checkmark$

(b) Now let  $\mathbb{F}$  be alg. closed, hence  $\mathbb{F}$  is infinite. If not, consider

$$1 + \prod_{a \in \mathbb{F}} (x - a) \in \mathbb{F}[x].$$

which has no roots in  $\mathbb{F}$   $\Downarrow$

If  $f$  is non-constant, this implies that  $C_f \subseteq \mathbb{F}^2$  has  $\infty$  many points:

$$\text{Let } f(x, y) = \sum c_k(x) y^k. \text{ For}$$

infinitely many  $a \in \mathbb{F}$  I claim that

$f(a, y) \in \mathbb{F}[y]$  is non-constant.

Indeed, since  $\mathbb{F}$  is non-constant,

$\exists k \geq 1$  so  $c_k(x)$  is non zero,

hence  $\exists \infty$  many  $a \in \mathbb{F}$  so

$$c_k(a) \neq 0.$$

For each such  $a \in \mathbb{F}$ ,  $\exists$  at least one  $b \in \mathbb{F}$  such that  $f(a, b) = 0$ , because  $f(a, y) \in \mathbb{F}[y]$  must have a root.

So now let  $f$  irreducible,  $C_f \subseteq C_g$ .

Then since  $C_f \subseteq C_f \cap C_g$  has as many points, conclude from (a) that  $f \mid g$ .

(c) Let  $f = z_1 \cdots z_k$  square-free and  $C_f \subseteq C_g$ . Then  $C_{z_i} \subseteq C_f \subseteq C_g \Rightarrow z_i \mid g$  for all  $i$ . Since  $\mathbb{F}[x, y]$  is UFD this implies  $f \mid g$ .

Let  $C = C_f$  for any polynomial

$f = z_1^{e_1} \cdots z_k^{e_k}$  and define

$$\sqrt{f} = z_1 \cdots z_k.$$

Then  $C_f = C_{\sqrt{f}}$ .

(d) Say  $f = g_1 g_2$  is reducible, i.e.  
 $g_1$  &  $g_2$  non-constant. Then

$$C_f = C_{g_1} \cup C_{g_2}$$

where  $C_{g_1}$  &  $C_{g_2}$  are non-empty  
(in fact, infinite!).

Conversely, suppose  $C_f = C_1 \cup C_2$   
for  $C_1, C_2$  non-empty. This means  
 $C_1 = C_{g_1}$  &  $C_2 = C_{g_2}$  for non-constant  
 $g_1$  &  $g_2$ . If  $g \mid g_1$  is any prime  
factor then

$$C_g \subseteq C_{g_1} \subseteq C_f,$$

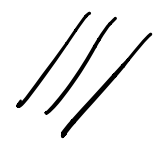
part (b)  $\Rightarrow g \mid f$ . But  $g \nmid f$   
because  $g_2$  is non-constant.

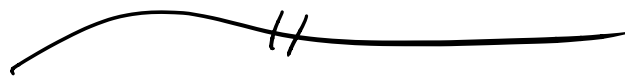
Hence  $f$  is reducible.



Corollary: Every curve  $C \subseteq \mathbb{F}^2$



has a unique decomposition into irreducible curves. 



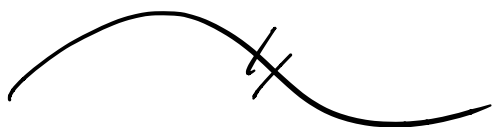
Compare to Descartes' Theorem:  
Given  $f(x) \in \mathbb{F}[x]$  &  $a \in \mathbb{F}$ ,

$$f(a) = 0 \iff (x-a) \mid f(x).$$

$$f \text{ vanishes on } \{a_1, \dots, a_n\} \iff (x-a_1) \cdots (x-a_n) \mid f(x)$$

If  $\mathbb{F}$  is algebraically closed,  
irreducible polynomials are just  
 $x-a$  for some  $a \in \mathbb{F}$ .

points  $\iff$  irreducible polynomials.



Remark: Study's Lemma parts  
(b, c, d) holds verbatim for  
hypersurfaces, but the proof is  
considerably more involved.