Last time:

$$R \text{ is UFD} \implies R[x] \text{ is UFD}$$
$$\vdots$$
$$\implies R[x_1, \dots, x_n] \text{ is UFD}.$$

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 <u>real</u> curves $C_f, C_g \in \mathbb{R}^2$.

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

$C_g = y$-axis.

Hence $C_f \subseteq C_g$, but we clearly have $x^2 + y^2 \nmid x$. 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 $C_f \nsubseteq C_g$, which explains why $f \nmid g$. ///

Study'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 f is square-free. Get a bijection:

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

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

$$\text{irreducible curves} \longleftrightarrow \text{irreducible polynomials}.$$

///

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 $\mathbb{F}(x) = \mathrm{Frac}(\mathbb{F}[x])$ 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

$p' \mid f'$ & $p' \mid g'$ 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. ✓

(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 $\mathbb{F}$ $\lightning$

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

Let $f(x,y) = \sum c_k(x) y^k$. 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 nonzero, hence $\exists$ ∞ 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 ∞ many points, conclude from (a) that $f \mid g$.

(c) Let $f = g_1 \cdots g_k$ square-free and $C_f \subseteq C_g$. Then $C_{g_i} \subseteq C_f \subseteq C_g$
$\Longrightarrow$ $g_i \mid g$ for all i. Since $\mathbb{F}[x,y]$ is UFD this implies $f \mid g$.

Let $C = C_f$ for any polynomial $f = g_1^{e_1} \cdots g_k^{e_k}$ and define

$$\sqrt{f} = g_1 \cdots g_k.$$

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

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

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

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 $q \mid g_1$ is any prime factor then

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

part (b) $\Longrightarrow$ $q \mid f$. But $q \nmid f$ because g_2 is non-constant. Hence f is <u>reducible</u>.

$\square$

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 $a \in \mathbb{F}$.

$$\text{points} \longleftrightarrow \text{irreducible polynomials}.$$

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