New Chapter: More Algebra.
Background for HW2.
Goal: Nullstellensatz in dim 2, extension to any dimension.

GCDs in a UFD: Given elements $a_1, a_2, \ldots, a_n \in R$ in a UFD, there exists a unique smallest principal ideal dR containing the ideal

$$a_1 R + a_2 R + \cdots + a_n R.$$

[We proved it last time.] Any generator of dR is called a gcd of $a_1, \ldots, a_n$. We say

$$\gcd(a_1, \ldots, a_n) \sim d,$$

unique up to multiplication by units.

GCDs in a PID. If R is PID and if $\gcd(a_1, \ldots, a_n) \sim d$, then there exist $b_1, \ldots, b_n \in R$ with

$$a_1 b_1 + \cdots + a_n b_n = d.$$

"Bézout's Identity."

Proof: In this case, $a_1 R + \cdots + a_n R$ is principal, so equals dR.

Gauss' Lemma:

Let R be UFD, $\mathbb{F} = \mathrm{Frac}(R)$.
For any $f(x) \in R[x]$ let $c(f)$ be the gcd of the coeffs, so $f = c(f) f'$ where $c(f') = 1$ (we say $f'(x)$ is a "primitive" polynomial).

(a) For all $f, g \in R[x]$,

$$c(f) = c(g) = 1 \Rightarrow c(fg) = 1.$$

(b) For all $f \in \mathbb{F}[x]$ there is a unique expression $f(x) = \alpha f'(x)$ where $\alpha \in \mathbb{F} \setminus 0$ & $f'(x) \in R[x]$ is primitive.

(c) If $f(x) = \prod g_i(x)$ in $\mathbb{F}[x]$ then $f'(x) = \prod g_i(x)$ in $R[x]$.

[Remark: Gauss proved this for $R = \mathbb{Z}$. His goal was to show that $\cos(2\pi/n) \in \mathbb{R}$ is expressible in terms of $\mathbb{Z}$ & square roots iff $\phi(n)$ is a power of 2.

e.g. $n = 17$, $\phi(17) = 16 = 2^4$ ✓]

Proof:

(a) For any prime $p \in R$ we have a ring hom. $R[x] \longrightarrow (R/pR)[x]$.

$$f(x) \longmapsto f_p(x).$$

Observe $c(f) = 1 \iff f_p(x) \neq 0$

for all primes p. Suppose $c(f) = c(g) = 1$ so that $f_p(x), g_p(x) \neq 0$.

Then since R/pR is a domain, so is $(R/pR)[x]$, hence

$$(fg)_p(x) = f_p(x)\, g_p(x) \neq 0. \qquad ///$$

(b) Let $f(x) \in \mathbb{F}[x]$, let $a \in R$ be any common multiple of denominators of the coeffts., so $af(x) \in R[x]$.

Then we have $af(x) = c(af)\, f'(x)$ where $f'(x) \in R[x]$ is primitive.

Let $\alpha = c(af)/a \in \mathbb{F}$ so, $f = \alpha f'$.

Uniqueness? Let $\alpha f' = \beta f'' = f$, with $f', f'' \in R[x]$ primitive.

Let $d \in R$ be such that $d\alpha, d\beta \in R$.

Then since $(d\alpha) f' = (d\beta) f''$ we have

$d\alpha = c(f) = d\beta$. Cancel d to get $\alpha = \beta$, hence $f' = f''$. ///

(c) Suppose $f(x) = \prod g_i(x)$ in $\mathbb{F}[x]$.

From (b) let $f = \alpha f'$, $g_i = \alpha_i g_i'$.

Then $\alpha f' = \prod \alpha_i \prod g_i'$.

Choose $d \in R$ so $d\alpha \in R$, $d \prod \alpha_i \in R$.

Then $df = (d\alpha) f' = (d \prod \alpha_i) \prod g_i'$.

Since $\prod g_i'$ is primitive from (a), take content on both sides to get

$$d\alpha = c(df) = d \prod \alpha_i.$$

Cancel this common factor to get

$$f' = \prod g_i'.$$

///

Theorem: R UFD $\Rightarrow$ $R[x]$ UFD.

Corollary: $\mathbb{Z}[x_1, \dots, x_n]$, $\mathbb{F}[x_1, \dots, x_n]$ are UFDs.

Proof: Existence: Let $f(x) \in R[x]$ and consider $f(x) \in \mathbb{F}[x]$ where $\mathbb{F} = \mathrm{Frac}(R)$. Since $\mathbb{F}$ is a field, $\mathbb{F}[x]$ is PID, hence Noetherian, we can factor

$$f(x) = q_1(x) \cdots q_m(x)$$

with $q_i(x) \in \mathbb{F}[x]$ irreducible.

It follows from Gauss' Lemma that

$$f'(x) = q_1'(x) \cdots q_m'(x) \quad \text{in } R[x]$$

$$f(x) = c(f) f'(x) = c(f) q_1'(x) \cdots q_m'(x),$$

where $c(f) \in R$, $g_i'(x) \in R[x]$ are irreducible & primitive. (Indeed, if g_i' factors in $R[x]$ then g_i factors in $\mathbb{F}[x]$.) Then factor $c(f)$ in R to obtain

$$f(x) = u p_1 \cdots p_n g_1'(x) \cdots g_m'(x).$$

Uniqueness: Suppose

$$p_1 \cdots p_k g_1(x) \cdots g_\ell(x) \sim p_1' \cdots p_m' g_1'(x) \cdots g_n'(x)$$

with $p_i, p_i' \in R$ prime,

$g_i, g_i' \in R[x]$ primitive irreducible.

Compare content to get

$$p_1 \cdots p_k \sim p_1' \cdots p_m'$$

Since R is UFD: $k = m$ and

$p_i \sim p_i'$ after relabeling.

Cancel constants to get

$$q_1(x) \cdots q_\ell(x) \sim q_1'(x) \cdots q_n'(x).$$

Claim $q_1(x)$ is <u>prime</u> in $R[x]$.

Indeed, suppose $q_1(x) \mid f(x) g(x)$ in $R[x]$ hence also in $\mathbb{F}[x]$. Since $\mathbb{F}[x]$ is PID, $q_1(x)$ irreducible, then q_1 is prime in $\mathbb{F}[x]$. This implies

$$q_1(x) \mid f(x) \quad \text{or} \quad q_1(x) \mid g(x) \quad \text{in } \mathbb{F}[x].$$

WLOG, say $q_1 \mid f$ so

$$f(x) = q_1(x) h(x), \quad h(x) \in \mathbb{F}[x].$$

From Gauss' Lemma:

$$f'(x) = q_1'(x) h'(x).$$

Since $q_1' = q_1$ is primitive, this implies $q_1 \mid f'$ hence $q_1 \mid f$ in $R[x]$.

Back to $q_1(x) \cdots q_\ell(x) \sim q_1'(x) \cdots q_n'(x)$.

Since q_1 is prime, have $q_1(x) \mid q_i'(x)$ for some i. WLOG, $q_1(x) \mid q_1'(x)$ hence $q_1(x) \sim q_1'(x)$ since both are irreducible. Cancel this factor, then uniqueness follows by induction.

$\square$

From this we will get

Study's Lemma: If $\mathbb{F}$ is alg. closed, then have a bijection

curves $\subseteq \mathbb{F}^2 \longleftrightarrow$ square-free polynomials $\in \mathbb{F}[x,y]$

irreducible curves $\longleftrightarrow$ irreducible polynomials.