RECAP

Main course topics:

I. Field extensions

- characterizing algebraic & transcendental extensions

II. Gröbner bases

- monomial orders
- construction/detection of Gröbner bases (Buchberger)

III. Ideal-variety correspondence

- various operations, e.g. $\cup$, $\cap$, $+$, $\cdot$, $:$

IV. Polynomial & rational functions

- properties of V from functions $V \to K$
- isomorphism & birational equivalence

I. Field extensions

Algebraic extensions

$$K \hookrightarrow K(\alpha) \qquad \longleftrightarrow \qquad K \hookrightarrow K[t]/\langle m \rangle$$

$\alpha \in \mathbb{C}$ root of minimal poly $m \in K[t] \subset \mathbb{C}[t]$
(see Stewart for the abstract version without $\alpha \in \mathbb{C}$)

Compare to the coordinate ring construction:
If $p \in K[t]$, $LT(p) = t^N$, then
$$K[t]/\langle p \rangle \cong \mathrm{span}_K\{1, t, \ldots, t^{N-1}\}$$
and for $V = V(p) \subset K$
$$K[V] = K[t]/I(V(p)) = K[t]/\langle q \rangle \cong \mathrm{span}_K\{1, t, \ldots, t^{M-1}\}$$
where
$$q = (t-\alpha_1)\cdots(t-\alpha_M),$$
$\alpha_1, \ldots, \alpha_M \in K$ roots of p in K

Transcendental extensions

$$K \hookrightarrow K(\alpha) \qquad \longleftrightarrow \qquad K \hookrightarrow K(t)$$

II Gröbner bases

Monomial orders

Total order (transitive & every pair can be compared) with

- $x^\alpha > x^\beta \Rightarrow x^{\alpha+\gamma} > x^{\beta+\gamma} \quad \forall \alpha,\beta,\gamma \in \mathbb{N}^n$
- $x^\alpha \geq 0 \quad \forall \alpha \in \mathbb{N}^n$

⇝ used to define $LT(p)$, $LM(p)$
to make polynomial division algorithmic (no arbitrary choices)

Gröbner basis

Finite subset $G \subset I$ with $\langle LT(G) \rangle = \langle LT(I) \rangle$

Characterizations:

- $p \in I \Rightarrow \exists g \in G : LT(g) \mid LT(p)$
- Buchberger: $\overline{S(g_i, g_j)}^G = 0 \quad \forall g_i, g_j \in G$

$$S(p,q) = \frac{x^\gamma}{LT(p)} p - \frac{x^\gamma}{LT(q)} q, \quad x^\gamma = \mathrm{lcm}(LM(p), LM(q))$$

Sufficient criterion: $LT(g)$ all coprime
$LT(p)$, $LT(q)$ coprime $\Rightarrow \overline{S(p,q)}^{(p,q)} = 0$.

Buchberger's algorithm:
If $\overline{S(g_i, g_j)}^G = r \neq 0$, add r to G.

III Ideal-variety correspondence

Perfect correspondence for radical ideals & alg closed fields

ALGEBRA		GEOMETRY
I	$\longrightarrow$	$V(I)$
$I(V)$	$\longleftarrow$	V
$I+J$	$\longrightarrow$	$V(I)\cap V(J)$
$\sqrt{I(V)+I(W)}$	$\longleftarrow$	$V\cap W$

($I(V)+I(W)$ might not be radical: $V=V(x^2-y)$, $W=V(x^2+y)$)

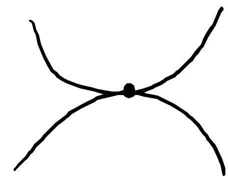
IJ or $I\cap J$	$\longrightarrow$	$V(I)\cup V(J)$
$\sqrt{I(V)I(W)} = I(V)\cap I(W)$	$\longleftarrow$	$V\cup W$

($I(V)I(W)$ might not be radical: $V=V(x)$, $W=V(x)$)

$I:J$	$\longrightarrow$	$\overline{V(I)\setminus V(J)}$
$I(V):I(W)$	$\longleftarrow$	$\overline{V\setminus W}$
$I\cap k[x_{\ell+1},\dots,x_n]$	$\longrightarrow$	$\overline{\pi_\ell(V(I))}$
$I(V)\cap k[x_{\ell+1},\dots,x_n]$	$\longleftarrow$	$\overline{\pi_\ell(V)}$
$I=I(V(I))$ prime	$\longleftrightarrow$	$V(I)$ irreducible
$I=I(V(I))$ maximal	$\longleftrightarrow$	$V(I)=\{a\}$ point
ACC	$\longleftrightarrow$	DCC
$I_1\subset I_2\subset\cdots \Rightarrow I_N=I_{N+1}$		$V_1\supset V_2\supset\cdots \Rightarrow V_N=V_{N+1}$

Non-radical ideals and ideals in non-algebraically closed fields contain more information than varieties:

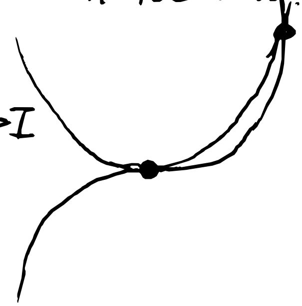
1) $V(x^2-y) \cap V(x^2+y) = \{(0,0)\}$



$\langle x^2-y \rangle + \langle x^2+y \rangle = \langle x^2, y \rangle$

degree 2 intersection visible in ideal sum

2) $V(x^3-y) \cap V(x^2-y) = \{(0,0), (1,1)\}$



$\langle x^3-y \rangle + \langle x^2-y \rangle = \langle x^2-y,\ xy-y,\ y^2-y \rangle = I$

y^2-y

$y=0$ $\qquad\qquad$ $y=1$

$\boxed{g_1(x,0)=x^2}$ $\qquad$ $g_1(x,1)=x^2-1$

$g_2(x,0)=0$ $\qquad$ $\boxed{g_2(x,1)=x-1}$

deg 2 intersection $\qquad$ deg 1 intersection

Compare $\sqrt{I} = \langle x-y,\ y^2-y \rangle$

3) $I = \langle x^2+1 \rangle$ & $J = \langle x^2+x+1 \rangle$ in $\mathbb{Q}[x]$

$V(I) = V(J) = V(I+J) = \emptyset$,

I detects the missing roots $\pm i \in \overline{\mathbb{Q}}$

J detects the missing roots $-\frac{1}{2} \pm \frac{\sqrt{3}}{2} i \in \overline{\mathbb{Q}}$

$I+J = \langle 1 \rangle \iff$ no common missing roots.

IV Polynomial & rational mappings

$\phi : V \to K$ polynomial mapping:

$\exists p \in K[x_1 \dots x_n] \quad \forall a \in V \quad \phi(a) = p(a)$

$\phi : V \dashrightarrow K$ rational mapping: (require V irreducible)

$\exists p, q \in K[x_1 \dots x_n] \quad \forall a \in V \quad \phi(a) = \frac{p(a)}{q(a)},$

$\exists b \in V \quad q(b) \neq 0$

Note: only values $\phi(a)$ matter:

If $V = V(x-y^2, x-z^3) \subset \mathbb{R}^3$, then $\phi : V \to \mathbb{R}$,

$\phi(x,y,z) = x^2 + \sin^2(y^4) + \cos^2(z^6)$

is a polynomial mapping!

Indeed $y^4 - z^6 \in \langle x-y^2, x-z^3 \rangle$ so on V

$\sin^2(y^4) + \cos^2(z^6) = \sin^2(y^4) + \cos^2(y^4) = 1$

$\Rightarrow \phi(x,y,z) = x^2+1$

Isomorphic varieties:

$V \underset{\beta}{\overset{\alpha}{\rightleftarrows}} W \quad \alpha, \beta$ polynomial $\quad \alpha \circ \beta = id_W, \ \beta \circ \alpha = id_V$

Birationally equivalent varieties:

$V \underset{\beta}{\overset{\alpha}{\dashrightarrow \atop \dashleftarrow}} W, \quad \alpha, \beta$ rational $\quad \alpha \circ \beta = id_W, \ \beta \circ \alpha = id_V$

equality wherever defined