Course Overview: two separate topics

1. Gröbner Bases – solving systems of polynomial equations

$$\begin{cases} xyz^2 - x^3 + yz + 3 = 0 \\ xz^3 + 4xy^2z - y^2 + z + 4 = 0 \\ x + y^2 + yz - z^2y = 0 \end{cases}$$

find all solutions. Find (x_1, y_1, z_1) which satisfy all 3 equations.
Maybe finitely many points and/or a curve in 3-space

Example: (Lagrange Multipliers) Minimize the function

$f(x,y,z) = xz + y^3 + y^2z + xyz$ on the sphere $g(x,y,z) = x^2 + y^2 + z^2 - 1 = 0$

Method of Lagrange Multipliers:
minima of f subject to constraint $g(x,y,z)=0$ are pts on the sphere when
$\nabla f = \lambda \nabla g$. This gives

$$\begin{bmatrix} \frac{\partial f}{\partial x} \\ \frac{\partial f}{\partial y} \\ \frac{\partial f}{\partial z} \end{bmatrix} = \lambda \begin{bmatrix} \frac{\partial g}{\partial x} \\ \frac{\partial g}{\partial y} \\ \frac{\partial g}{\partial z} \end{bmatrix} \sim \begin{cases} z + yz = \lambda 2x \\ 3y^2 + 2yz + xz = \lambda 2y \\ x + y^2 + xy = \lambda 2z \\ x^2 + y^2 + z^2 - 1 = 0 \end{cases}$$

$g(x,y,z) = 0$

Algebraic geometry: understanding solution sets to polynomial equations.

Representation theory of finite groups

Def: A real n-dimensional representation of a finite group G
is a group homomorphism $\rho: G \to GL_n(\mathbb{R})$

Example: 1-dimensional reps of a finite group

$\rho: G \to GL_1(\mathbb{R}) \cong \mathbb{R}^\times$

Consider V a n-dim real vector space.
$End(V)$ = endomorphisms of V is a ring!
" linear transformations $V \to V$.

Given $T, S \in End(V)$, $(T+S)(v) := T(v) + S(v)$
multiplication in $End(V)$ is composition of linear transformations $(T \cdot S)(v) := T(S(v)) = (T \circ S)(v)$
multiplicative identity = Id_V

$\mathrm{End}_{\mathbb{R}}(V) \cong M_n(\mathbb{R})$ — choice of basis induces explicit isomorphism

not strictly necessary, but reminds us that these maps are $\mathbb{R}$-linear

$\mathrm{End}(V) \xrightarrow{\sim} M_n(\mathbb{R})$ Choose basis $v_1, \dots, v_n$ of V

$T \mapsto (r_{ij})$ Columns of (r_{ij}) are $T(v_i)$.

Since $\mathrm{End}(V) \cong M_n(\mathbb{R})$, we have $\mathrm{End}(V)^\times \cong GL_n(\mathbb{R})$

Thus a rep of G is a group homomorphism $G \to \mathrm{End}(V)^\times$

Ex: 1-dim reps $\rho : G \to GL_1(\mathbb{R}) \cong \mathbb{R}^\times = \mathbb{R} \setminus \{0\}$

But we must have $|\rho(g)| < \infty$ for all $|g| < \infty$ which is all $g \in G$ since G is finite.

Thus $\rho : G \to \{\pm 1\}$.

What about 1-dim <u>complex</u> reps? $\rho : G \to GL_1(\mathbb{C}) \cong \mathbb{C}^\times = \mathbb{C} \setminus \{0\}$

$S^1 = \{z \in \mathbb{C} \mid |z| = 1\}$

$|z| = d(0, z)$

Analogously to above, we must have $\rho : G \to S^1$

finite subgroups of S^1 are cyclic groups!

e.g. $\langle e^{2\pi i/n} \rangle \cong \mathbb{Z}/n\mathbb{Z}$

Theory works much more nicely with $GL_n(\mathbb{C})$.

1-dim reps with $|G| < \infty$

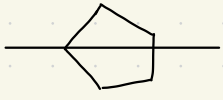
$\mathbb{R}$: $\rho : G \to \{\pm 1\} < \mathbb{R}^\times \cong GL_1(\mathbb{R})$

$\mathbb{C}$: $\rho : G \to \mathbb{Z}/n\mathbb{Z} < S^1 < \mathbb{C}^\times \cong GL_1(\mathbb{C})$

<u>2-dim reps</u>

Ex: dihedral group with $2n$ elements $D_n = \langle r, s \mid r^n = s^2 = srsr = e \rangle$ ($srsr = e \Leftrightarrow srs = r^{-1}$)

Symmetry group of regular n-gon



$\rho : D_5 \to GL_2(\mathbb{R}) = \mathrm{End}(\mathbb{R}^2)^\times$ invertible linear transformations

$\rho(x)$ = reflection through x-axis $= \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}$

$\rho(y)$ = rotation by $2\pi/5 = \begin{bmatrix} \cos 2\pi/5 & -\sin 2\pi/5 \\ \sin 2\pi/5 & \cos 2\pi/5 \end{bmatrix}$

3-dim reps : rotational symmetries of the tetrahedron $\triangle = T \subset \mathbb{R}^3$

rotational aut $(T) \cong A_4 \leq S_4$

$(132), (243), (143), (142)$
$(123), (234), (134), (124)$
$(24)(13), (14)(23), (12)(34)$
e

induces $\rho: A_4 \to GL_3(\mathbb{R})$

adding orientation reversing automorphisms completes S_4

ex. reflect through xy-plane $\begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & -1 \end{bmatrix} \xmapsto{\det}$ negative sign (-1)

Sulfur hexafluoride:

7 atoms, each moves in 3 dimension

Space of atomic displacements is a 21-dim real vector space $=: V \cong \mathbb{R}^{21}$

$G =$ (finite) symmetry group of $SF_6 < S_6$

$\rho: G \to GL_{21}(\mathbb{R}) \cong End(V)^\times$

Theorem: Every finite group has up to isomorphism only finitely many irreducible representations

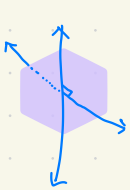
Def: direct sum of two rep of G

$\rho_m: G \to GL_m(\mathbb{R})$ $\rho_n: G \to GL_n(\mathbb{R})$

Define new rep $\rho = \rho_m \oplus \rho_n : G \to GL_{m+n}(\mathbb{R})$

$$g \mapsto \begin{bmatrix} \rho_m(g) & 0 \\ 0 & \rho_n(g) \end{bmatrix}$$

Ex:



$$\begin{bmatrix} \cos\frac{2\pi}{6} & -\cos\frac{2\pi}{6} & 0 \\ \sin\frac{2\pi}{6} & \sin\frac{2\pi}{6} & 0 \\ 0 & 0 & 1 \end{bmatrix} \quad (D_6 \to GL_2(\mathbb{R})) \oplus (S_2 \to GL_1(\mathbb{R}))$$

$$D_6 \to GL_3(\mathbb{R}) \quad \begin{bmatrix} -1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & -1 \end{bmatrix}$$

Def a rep is irreducible if it cannot be written as a direct sum of two positive dim subreps

1- dim subreps = vectors which are eigenvectors $\rho(g)\ \forall g \in G$

Ex (cont from above)

This rep is direct sum $\begin{bmatrix} \rho_2(g) & 0 \\ 0 & \rho_1(g) \end{bmatrix}$ $\quad \rho_1 : D_6 \to D_6/C_6 \cong \{\pm 1\} \mapsto \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & \pm 1 \end{bmatrix}$

The regular representation

G = finite group
M = $\mathrm{Maps}(G, \mathbb{C})$
This gives a representation of G: $\rho \to GL_n(\mathbb{C})$ where $n = \dim_{\mathbb{C}} M$

$GL(M)$
$\| $
$\mathrm{End}_{\mathbb{C}}(M)^\times$

Given a function $f : G \to \mathbb{C}$,
$\rho(g)(f)$ is $h \mapsto f(g^{-1}.h)$
$\uparrow$
G

Ex. $G = S^1 = \{z \in \mathbb{C} \mid |z| = 1\}$
$M = \mathrm{Maps}(S^1, \mathbb{C})$ have interesting "basis"
$\{e^{2\pi i n t} \mid t = \mathbb{R}/\mathbb{Z} \cong S^1\}$
$\uparrow$ set of 1-dim reps of S^1

Write $f : \mathbb{R}/\mathbb{Z} \to \mathbb{C}$ in terms of the basis: $f = \sum_{n \in \mathbb{Z}} c_n e^{2\pi i n t} = \sum_{n \in \mathbb{Z}} c_n \cos(2\pi i n t) + c_n i \sin(2\pi i n t)$
"Approximate" $\mathbb{R}/\mathbb{Z}$ with finite groups $\frac{1}{N}\mathbb{Z}/\mathbb{Z} \cong \mathbb{Z}/N\mathbb{Z}$

The 1-dim reps of $\frac{1}{N}\mathbb{Z}/\mathbb{Z}$ are
$t \mapsto \{e^{2\pi i m t} \mid m \in \mathbb{Z}/N\mathbb{Z}\}$

fourier theory on $\frac{1}{N}\mathbb{Z}/\mathbb{Z}$:
There are two natural bases of M:
One is the on-dim reps $\{e^{2\pi i n t}\}$
The other is a natural way of writing a function $f : \frac{1}{N}\mathbb{Z}/\mathbb{Z} \to \mathbb{C}$
in terms of values $f(\frac{m}{n})$ for $\frac{m}{N} \in \frac{1}{N}\mathbb{Z}/\mathbb{Z}$

Let $\delta_{m/N} : \frac{1}{N}\mathbb{Z}/\mathbb{Z}$ be a function s.t.

$$\frac{l}{N} \to \begin{cases} 1 & l = m \\ 0 & l \neq m \end{cases}$$

Then $f = \sum_{n \in \mathbb{Z}/N\mathbb{Z}} f\left(\frac{n}{N}\right)\delta_{n/N}$

Change of basis matrix is the fourier transform.

Thm: Any rep of a finite group G is isomorphic to a sum of irreducible representations.

Example: The irreducible reps of A_4:

$\rho_0 : \alpha \mapsto 1$
ρ_1
ρ_2

$A_4 \to A_4/V_4 \cong C_3 \cong \mathbb{Z}/3\mathbb{Z} \to GL_2(\mathbb{C}) \cong \mathbb{C}^\times$
$m/3 \mapsto e^{2\pi i m n/3}$
$n \in \{0, 1, 2\}$

$\rho_1\left((1\,2\,3)\right) = e^{2\pi i/3}$
$\rho_2\left((1\,2\,3)\right) = e^{-2\pi i/3}$ complex conjugate rep

$\rho : A_4 \to GL_3(\mathbb{R})$
im of ρ = rotational symmetries of regular tetrahedron

$A_4 \to GL_3(\mathbb{C})$
$w \mapsto$ [$\rho_0(\alpha)$; $\overline{\rho_2(\alpha)}$; $\overline{\rho_1(\alpha)}$]

Given a rep. $\rho : G \to GL(V) = End(V)^\times$,
a subspace $W \subset V$ is g-stable if $\rho(g)w \in W$
$\forall w \in W$ and $\forall g \in G$.
In other words, g-stable means $\rho(g)$ maps W to W
injectively. Thus $\rho(g)|_W$ is injective
from linalg: $\dim \ker(\rho(g)|_W) + \dim \mathrm{Im}(\rho(g)|_W) = \dim(W)$
$\therefore \dim \mathrm{Im}(\rho(g)|_W) = \dim(W)$
$\therefore \rho(g)|_W$ is bijective.
This means $\rho|_W$ is a group homomorphism $G \to GL(W) = Isom(W, W)$
$\therefore W \subset V$ is a g-stable subspace $\Leftrightarrow \rho|_W$ is a representation of G.
we call it a subrepresentation of $\rho : G \to GL(V)$

Def: $\rho : G \to GL(V)$ is an irreducible rep. if the only G-stable subspaces are trivial

Decomposition of representations

They over $\mathbb{R}$ and $\mathbb{C}$ is the same.

Theorem: Every rep. of G is a direct sum of irreducible reps.

Two ways to talk about a representation:

i) as homomorphism $\rho: G \to GL(V) = End(V)^\times$

ii) as a left action of G on V by invertible linear transformations

$G \times V \xrightarrow{*} V: \quad g * v = \rho(g)(v)$

Def: given a rep of G on V a subspace $W \subset V$ is G-stable if $g * w = \rho(g)(w) \in W$ for all $w \in W$ and $g \in G$

This means that $\rho(g)$ maps W to W. So W is a subrep of V.

Def $\rho: G \to GL(V)$ is an irreducible representation if the only G-stable subreps are $\{0\}$ and V and $G \neq V$.

Def A vector space V is a direct sum of two subspaces W and W' if every $v \in V$ can be written as $v = w + w'$ for exactly one $w \in W$, $w' \in W'$. We write $V = W \oplus W'$ or $V = \bigoplus_i W_i$

Ex: $\mathbb{R}^{\oplus 2} = \mathbb{R}^2$, $W = Span\left\{\begin{pmatrix}1\\0\end{pmatrix}\right\}$, $W' = Span\left\{\begin{pmatrix}0\\1\end{pmatrix}\right\}$

Theorem Every representation $\rho: G \to GL(V)$ may be written as a direct sum of irreps.

Prop: Let $\rho: G \to GL(V)$ be a rep of $|G| < \infty$ and $0 \neq W \neq V$ a G-stable subspace. Then $\exists$ a G-stable subspace W' s.t. $V = W \oplus W'$.

Def: A linear projection from V to subspace W is a linear transformation $p: V \to W$ s.t. $p|_W = Id_W$

Def Given reps of $G \xrightarrow[\exists]{\rho} GL(V)$, $GL(U)$

A linear transformation $L: V \to U$ is G-equivariant if L respects the actions of G, i.e. $L(\rho(g)(v)) = \tau(g)(L(v))$

In terms of group action, $L(g * v) = g * L(v)$

Lemma: Let $T: V \to U$ be a G-equivariant linear transformation. Then $\ker(T)$ is G-stable in V.

Proof: Let $w \in \ker(T)$. Show $\rho(g)(w) \in W$. T is G-stable means

$T \circ \rho(g) = \xi(g) \circ T$. Thus $w \in \ker(T)$ implies $0 = \xi(g) \circ T(w) = T \circ \rho(g)(w) \therefore \rho(g)(w) \in \ker T$

Lemma: Given any linear projection $p: V \to W$, a G-equivariant linear projection is given by averaging p over G.

Proof: Given $p: V \to W$, define $P: V \to V$ by $P_{(v)} = \frac{1}{|G|} \sum_{g \in G} \xi(g) \circ p \circ \rho(g^{-1})(v)$

$$P \in \mathrm{End}(V) \qquad V \xrightarrow{\rho(g^{-1})} V \xrightarrow{p} W \xrightarrow{\xi(g)} W$$

Check: $P \circ \rho(h)(v) = \xi(h) \circ P(v)$

$$\left(\frac{1}{|G|} \sum_{g \in G} \xi(g) \circ p \circ \rho(g^{-1})\right) \rho(h)(v)$$

$$= \frac{1}{|G|} \sum_{g \in G} \xi(g) \circ p \circ \rho(g^{-1}h)(v)$$

let $j = h^{-1}g \in G \quad g = hj$ (left-multi is isomorphism)

$$= \frac{1}{|G|} \sum_{j \in G} \xi(hj) \circ p \circ \rho(j^{-1})(v)$$

$$\xi(h)\left(\frac{1}{|G|} \sum_{j \in G} \xi(j) \circ p \circ \rho(j^{-1})\right)(v)$$

$$= \xi(h) P(v)$$

Proof of prop above: Set $W' = \ker(P)$

Proof of theorem: $V = W_1 \oplus \cdots \oplus W_n$ irreps W_i by induction on $\dim(V)$.

Inner Product Spaces

Def An **inner product space** $(V, \langle , \rangle)$ is a v.s. $V/\mathbb{R}$ or $\mathbb{C}$ together with a positive definite inner product.

Def (for $\mathbb{R}$) A positive definite symmetric bilinear form on a real v.s. V is a map $\langle , \rangle : V \times V \to \mathbb{R}$ satisfying

(i) linearity: $\langle r_1 v_1 + r_2 v_2, w \rangle = r_1 \langle v_1, w \rangle + r_2 \langle v_2, w \rangle$

(ii) symmetry: $\langle v_1, v_2 \rangle = \langle v_2, v_1 \rangle$

(iii) positive definite: $\langle v, v \rangle \geq 0$ with equality iff $v = 0$

Examples: 1) $V = \mathbb{R}^n$, $\langle v, w \rangle$ = dot product

2) X = finite set $V = \text{maps}(X, \mathbb{R})$ $\langle f, g \rangle = \sum_{x \in X} f(x) g(x)$

3) integral analog to (2)

In $(V, \langle \cdot, \cdot \rangle)$, length of $v \in V$ is $\|v\| = \langle v, v \rangle^{1/2}$

Def $v \perp w \Leftrightarrow \langle v, w \rangle = 0$

Def for $W \subseteq V$, $W^\perp = \{ v \in V \mid \langle v, w \rangle = 0 \ \forall w \in W \}$

Then $V = W \oplus W^\perp$

Orthogonal Group = linear symmetries of the inner product space $(V, \langle \cdot, \cdot \rangle)$

$$O(V, \langle \cdot, \cdot \rangle) \leq GL(V)$$

$$\| \quad \{ g \in GL(V) \mid \langle gv, gw \rangle = \langle v, w \rangle \ \forall v, w \in V \}$$

for representation theory, we need G-invariant inner product $\langle g * v, g * w \rangle = \langle \rho(g)(v), \rho(g)(w) \rangle$ $\forall g$ in a finite group

This means $G \xrightarrow{\rho} GL(V)$, with $G \dashrightarrow O(V, \langle \cdot, \cdot \rangle) \hookrightarrow GL(V)$

Given a G-stable subspace $W \subseteq V$, $W^\perp$ will be a representation when $\langle \cdot, \cdot \rangle$ is G-invariant.

$V \cong W \oplus W^\perp$ direct sum rep.

Complex Theory

Complex conjugation $\overline{(r + si)} = r - si$

Def: A positive definite hermetian form is a map $\langle \cdot, \cdot \rangle : V \times V \to \mathbb{C}$ where V is a v.s./$\mathbb{C}$ s.t.

(i) linearity in first term: $\langle c_1 v_1 + c_2 v_2, w \rangle = c_1 \langle v_1, w \rangle + c_2 \langle v_2, w \rangle$

(ii) Hermetian symmetry: $\langle v_1, v_2 \rangle = \overline{\langle v_2, v_1 \rangle}$

(iii) $\langle v, v \rangle = \overline{\langle v, v \rangle} \in \mathbb{R}_{\geq 0}$ $\langle v, v \rangle \geq 0$ with equality iff $v = 0$.

Ex. 1) Standard inner product on $\mathbb{C}^n$ is $\langle v, w \rangle = \sum_i v_i \bar{w}_i \in \mathbb{C}$

2) X finite set $V = \text{maps}(X, \mathbb{C})$ $\langle f, g \rangle = \sum_{x \in X} f(x) \overline{g(x)}$

3) Hilbert spaces → replace X with $\mathbb{R}$ and sum with integral

$(V, \langle , \rangle)$ = inner product space
= v.s / $\mathbb{C}$ + pos. def Hermitian form

length of vector $\|v\| = \sqrt{\langle v, v \rangle}$

$v \perp w \Leftrightarrow \langle v, w \rangle = 0$

Gram-Schmidt orthogonalization process applied to any $\mathbb{C}$-basis of V gives an orthonormal basis.

Unitary Group

$$U(V, \langle , \rangle) = \{ g \in GL(V) \mid \langle gv, gw \rangle = \langle v, w \rangle \ \forall v, w \in W \}$$

fix an orthonormal basis to write elements of $U(V, \langle , \rangle)$ as matrices.

Then for $C \in U(V, \langle , \rangle)$, $C^T \bar{C} = I$

Standard unitary group on n-dim v.s / $\mathbb{C}$
$\cong \{ C \in M_{n \times n}(\mathbb{C}) \mid C^T \bar{C} = I \}$

Let $\rho : G \to GL(V)$ hom.

Lemma: A G-invariant pos. def. Hermitian form $\langle , \rangle : V \times V \to \mathbb{C}$ is obtained from any pos def Herm form by averaging over the fin group G: i.e.

$$\langle v, w \rangle := \frac{1}{|G|} \sum_{g \in G} (\rho(g)v, \rho(g)w)$$

Proof: for $h \in G$, $\langle \rho(h)v, \rho(h)w \rangle = \frac{1}{|G|} \sum_{g \in G} (\rho(g)\rho(h)v, \rho(g)\rho(h)w)$

Let $k = gh$ b/c left mult is isomorphism

$$= \frac{1}{|G|} \sum_{g \in G} (\rho(gh)v, \rho(gh)w)$$

$$= \frac{1}{|G|} \sum_{k \in G} (\rho(k)v, \rho(k)w)$$

$$= \langle v, w \rangle$$

$\blacksquare$

$\rho: G \to GL_n(\mathbb{C})$ $\quad \rho : G \to GL_n(\mathbb{C})$

$c_g \in Inn(G)$ $\quad \rho \circ c_g : G \to GL_n(\mathbb{C})$

$\rho(c_g(h))$

$\rho(ghg^{-1})$

$\rho(g)\rho(h)\rho(g^{-1})$

$\rho(g)\rho(h)\rho(g)^{-1}$

$\rho_1, \rho_2 : G \to GL_n(\mathbb{C})$ non equivalent

$\rho_1(G) = \rho_2(G)$

$\exists$ Automorphism f s.t. for any g,

$f(\rho_1(g)) = \rho_2(g)$

further more, for any $\rho_1(g) = \rho_2(g')$ then must exist

$2\pi m/n = x$

$\left(e^{2\pi i m/n} + e^{-2\pi i m/n}\right)\overline{e^{2\pi i m/n}}$

$\left(e^{ix} + e^{-ix}\right)e^{-ix}$

$(\cos x + i\sin x + \cos(-x) + i\sin(-x))(\cos x - i\sin x)$

$2\cos x(\cos x - i\sin x)$

$2\cos^2 x - 2i\cos x \sin x$

$-i\sin 2x$

$1 + \cos 2x - i\sin 2x$

$1 + e^{-2x}$

$2\cos(2\pi a^n/p)$

$(p-1)/2 \cdot 2\pi/p$

$\pi(p-1)/p$

<u>G-equivariant</u> S, T sets with G ⟲ S, G ⟲ T

$f: S \to T$ G equivariant if $\forall h \in G, s \in S$,

$f(h \times s) = h \times f(s)$

~ linearity

$\ker f$ = G-stable subspace

Arbitrary $\rho: G \to GL(V)$, $\rho: V \to W$

$\rho(g) \circ \rho \circ \rho(g^{-1})(v)$

$V \to V$ $\quad V \to W$ $\quad V \to V$

$W \subset V$

Def $P: V \to V$ by $P(v) := \frac{1}{|G|} \sum_{g \in G} \rho(g) \circ \rho \circ \rho(g^{-1})(v)$

G-invariant inner product: $(\rho_g v, \rho_g w) = (v, w)$ $\forall g \in G, \forall v, w \in V$

Given any $(,)$, construct $\langle v, w \rangle = \frac{1}{|G|} \sum_{g \in G} (\rho_g v, \rho_g w)$

$\longrightarrow$ still pos def bilinear symmetric and G-invariant

Hermitian form $(v, w) = \overline{(w, v)}$

ρ, ρ irreps,
$T: \rho \to \rho$, then
T invertible or $T = 0$
$\Rightarrow$ 2 irreps are either equivalent or not

Character $\chi(g) = \mathrm{Tr}(\rho(g))$ for any rep ρ

χ same up to isomorphic reps.

$\chi(g) = \chi(g')$ if g, g' in same conjugacy class

Char table
1) determine conjugacy classes + size
2) find 1 dim irreps $\# = |G/G'|$
3) look at non faithful irreps $\Leftrightarrow$ irreps of G/N for $N \trianglelefteq G$ make sure $N \not\subseteq G'$

$\rho: G \to GL(V)$ faithful if ρ injective

Inner product of characters
$\langle \chi_1, \chi_2 \rangle := \frac{1}{|G|} \sum_{g \in G} \chi_1(g) \overline{\chi_2(g)}$

if ρ irrep with char χ, then $\langle \chi, \chi \rangle = 1$

for any χ' (of irreps) $\neq \chi$, $\langle \chi, \chi' \rangle = 0$

Any rep ρ has a unique decomp into irreps.

ρ irrep $\Leftrightarrow \langle \chi_\rho, \chi_\rho \rangle = 1$

# of irreps = # of conjugacy classes

ρ is permutation matrix if it is just a permutation of columns of identity matrix

$\rho: S_n \to GL(\mathbb{C}X)$ by decompose into trivial rep (identity) and $(n-1)$ dim augmentation rep
$\Rightarrow$ all matrices that don't have all 1 on diag

Regular rep of G is: $\rho: G \to GL(\mathbb{C}G)$
$\chi_{reg}(e) = |G|$, $\chi_{reg}(g) = 0$ for $g \neq e$

NOT irreducible $\to$ in decomp, every irrep of dim d occurs d times

- $|G| = \sum_{\rho \text{ irrep}} (\dim \rho)^2$
- # of irreps = # of conj classes
- # of one-dim irreps = $|G/G'|$

Ways to get new reps

- compose with one dim rep (sign if common)
- 2 reps equivalent iff $\text{Tr}(\rho_1) = \text{Tr}(\rho_2)$ (some char)
- compose with automorphism

$-6x^2 + 7x + 5$

$-3x + 5$

	$-6x^2$	$+10x$
$2x$		
$+1$	$-3x$	$+5$

-30, 10, -3, 7

	$2x$	1
$-3x$	$-6x^2$	$-3x$
5	$10x$	$+5$

$(-3x+5)(2x+1)$

$-6x^2 + 10x - 3x + 5$

$= -6x^2 + 7x + 5$

$-6x + 7x + 5$

$(ax+b)(cx+d)$

$acx^2 + bcx + adx + bd$

$ac = 6$

$bc + ad = 7$

$bd = 5$

$12x^2 - 3$

$3((2x)^2 - 1)$

$(2x)^2 - (1)^2$

$(2x+1)(2x-1)$

$ax^2 - b$

$(a+b)^2 = a^2 + 2ab + b^2$

$(4)^2 \quad 2(4)\cdot 4 \quad 16^2$

$y = x^2 + 8x + 11$

$a^2 - b^2$

$(a+b)(a-b)$

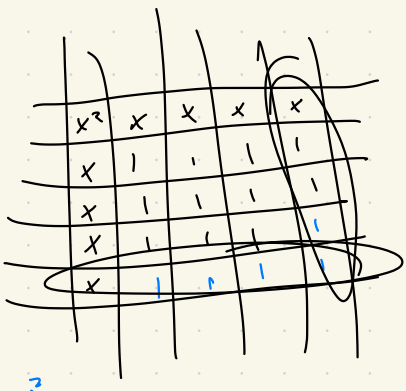
$a^2 + \cancel{ab} - \cancel{ab} - b^2$

$a^2 - b^2$

$(a+b)(a-b)$	$(a+b)^2$	$(a-b)^2$
$a^2 - b^2$	$a^2 + 2ab + b^2$	$a^2 - 2ab - b^2$

$x^2 + 8x + 11 \quad +5 -5$

$y = (x+4)^2 - 5$



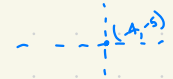
$x^2 + 8x + 16 - 5 = x^2 + 8x + 11$

$x^2 + 8x + 11 = ?$ $\quad x^2 + 8x + 16 = (x+4)^2$

$x^2 + 8x + 11 + 5 - 5$ //

$x^2 + 8x + 16 - 5$ //

$y = (x+4)^2 - 5$



$x^2 + 8x + 11$

$(x+4)^2 - 5$

$(x+a)(x+b)$

$x^2 + 10x - 3$

$x^2 + 10x - 3 + 25 - 25$

$x^2 + 10x + 25 - 28$

$(x+5)^2 - 28$

$x^2 \quad 10x \quad 25$

$a^2 + 2ab + b^2$

$(a+b)^2$

$(x+5)^2$

$(x+a)^2 + b$

$x^2 + 2 \cdot a \cdot x + a^2 + b$

$x^2 + 2ax + a^2 + b$

$x^2 + 10x - 3$

$2ax = 10x$

$5 = a$

$x^2 + 10x - 3$

$x^2 + 10x + 25 + b$

$-3 + 25 - 25$

$(x+5)^2 - 25$

$x^2 + 10x$

$a^2 \quad 2 \cdot a \cdot b$

$x^2 + 2 \cdot x \cdot b$

$x^2 + 10x$

$2bx = 10x$

$2b = 10$

$b = 5$

$(x+5)^2$

$$y = \frac{3x^2}{3} + \frac{18x}{3} + \frac{60}{3}$$

$$\frac{y}{3} = x^2 + 6x + 20$$

$a^2 + 2ab + b^2$

$(1x)^2 + 2(1x)b$

$1x \cdot b = bx$

$9x$

$(x + 9/2)^2$

$x^2 + 9x + 20 + a - a$

$(x + 9/2)^2 + L$

$y = 3x^2 + 18x + 60$

$y/3 = x^2 + 6x + 20$

$= x^2 + 6x + 9 + 20 - 9$

$y/3 = (x+3)^2 + 11$

$y = 3(x+3)^2 + 33$

$x^2 x^2 \quad x^{2\cdot 2}$

$2+2 = 2\cdot 2 = 2^2$

$(a+b)^2$

$x^a x^b = x^{a+b}$

$(x^a)^b$

$x^a \cdot x^a \cdot \ldots \cdot x^a = x^{ba}$ (b times)

$(x-5)^2$

$x^2 - 10x + 25$

$x^2 - 10x + 25 - 5/2 - 25$

$2\left[(x-5)^2 - 5/2 - 25\right]$

$2(x-5)^2 - 5 - 50$

$2(x-5)^2 - 55$

$x^2 + (11)x + \frac{121}{4}$

$\downarrow$

$11/2$

$(x + 11/2)^2$

$x^2 + 2 \cdot x \cdot \frac{11}{2} + (\frac{11}{2})^2$

$x^2 + 11x + \frac{121}{4}$

$(x+a)^2 + b$

$b = 0$

$a^3 - b^3 = (a-b)(a^2 + ab + b^2)$

$a^3 + b^3 = (a+b)(a^2 - ab + b^2)$

$x^2 - 10x - 25$

$(x+a)^2$ ✗

$x^2 - 2ax + a^2$

$x^2 - 10x + 25$

$x^2 + 11x + \frac{121}{4}$

$(x + \frac{11}{2})^2$ ✓

$x^2 + 11x + \frac{121}{4}$

$y = mx + b$

slope $= m = \frac{\text{rise}}{\text{run}} = \frac{\Delta y}{\Delta x} = \frac{3}{3} = 1$

$+ \ (10, 3)$

$-(7, 0)$

$(3, 3)$

$\Delta x \quad \Delta y$

(11, −12)

(−3, 6) $\frac{6}{-3} = -2$

$\Delta x \quad \Delta y$

(−8, −6)

(−8, 4)

(0, −2)

Δx Δy = 0 then it equals 0

1. $(-8, -1)$

$(-8, -11)$

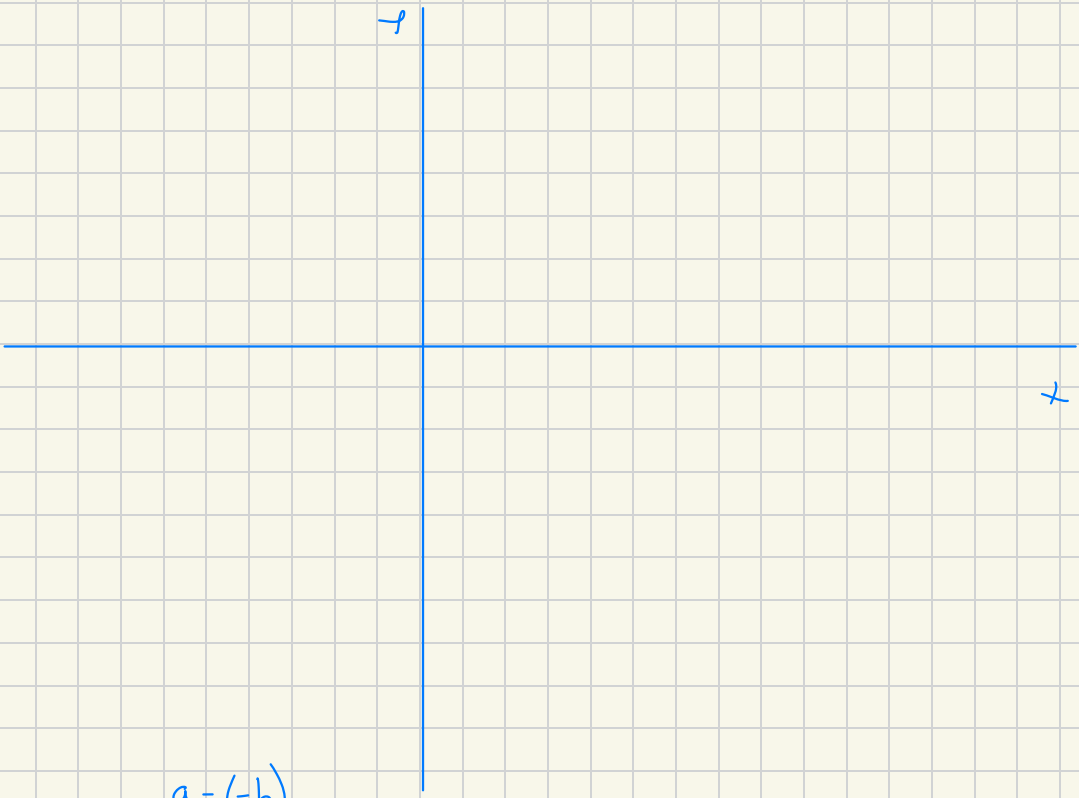
$(0$

$y = mx + b$

$y = -2x + 2$

slope $= m = -2$

y-intercept $= b = 2$



$a-(-b)$

$=a+b$

$y=-\frac{1}{4}(x+5)-3$

$y+3=-\frac{1}{4}(x+5)$ $(-5,-3)$

$y-y_1=m(x-x_1)$

$G = \mathbb{Z}/N\mathbb{Z}$ $\quad i \in \mathbb{Z}/N\mathbb{Z}$, $\quad \delta_i = \begin{cases} 1 & \text{if } g = i + N\mathbb{Z} \\ 0 & \text{otherwise} \end{cases}$

Nth power of δ_i in $L(G)$ by computing convolutions explicitly

$$\delta_i * \delta_i(x) = \sum_{y \in G} \delta_i(xy^{-1})\,\delta_i(y)$$

nonzero if $y = i$ $\qquad xy^{-1} = i$

$xi^{-1} = i$

$x = i^2$

$$(\delta_i * \delta_i)(x) = \begin{cases} 1 & \text{if } x = i^2 \\ 0 & \text{otherwise} \end{cases} = \delta_{i^2}$$

$$\widehat{f}(1)(\alpha) = \frac{1}{|N|} \sum_{\chi \in \widehat{G}} 1 \cdot \chi$$

$0 \le k \le N-1$

$G = \mathbb{Z}/N\mathbb{Z}$ $\qquad \widehat{G} = \{\varepsilon^k : \mathbb{Z}/N\mathbb{Z} \to \mathbb{C}^\times = GL_1(\mathbb{C})\}$

$\varepsilon^k(j + N\mathbb{Z}) = e^{2\pi i/N \cdot j \cdot k}$

input changes

$\varepsilon^0 = e^{2\pi i/N \cdot j \cdot 0} = e^0 = 1$

$$\widehat{f}(\varepsilon^0) = \widehat{f}(1) = \frac{1}{N} \sum_{\varepsilon^k \in \widehat{G}} 1 \cdot \varepsilon^k$$

$$= \frac{1}{N} \sum_{0 \le k \le N-1} \varepsilon^k$$

$$= \frac{1}{N}(N + 0 + \cdots + 0)$$

$$= 1$$

$G = \mathbb{Z}/N\mathbb{Z}$ $\quad \hat{G} = \{\xi^k \mid 0 \le k \le N-1\}$

$T \in L(G) \Rightarrow T : G \to \mathbb{C}$ by $T = \frac{1}{2}(\delta_1 + \delta_{-1})$

$$T(g) = \begin{cases} 1/2 & \text{if } g = 1, -1 \\ 0 & \text{otherwise} \end{cases}$$

$\rho_t(g) \in L(G)$ = probability that random walker on G at position $g \in G$ after time t.

$\rho_0 = \delta_0 \quad \rho_t = \underbrace{T * \cdots * T}_{t} * \delta_0$

$$(T * T)(x) = \sum_{y \in G} T(x-y)\,T(y) \qquad y = -1, 1$$

$$\rho_n = T^{*(n-1)} * (T * \delta_0) = T^{*n} * \rho_0$$

$$T(x) = \begin{cases} 1/2 & \text{if } x = -1, 1 \\ 0 & \text{otherwise} \end{cases}$$

$$T(x-a) = \begin{cases} 1/2 & \text{if } x = a-1, a+1 \\ 0 & \text{otherwise} \end{cases}$$

$$\frac{1}{2}T(x-1) + \frac{1}{2}T(x+1)$$

$\frac{1}{2}$ if $x = 0, 2$ $\quad$ $\frac{1}{2}$ if $x = -2, 0$

$$T * \delta_0(x) = \sum_{y \in G} T(x-y)\,\delta_0(y) \qquad y = 0$$

$$= T(x-0)$$

$$= T$$

So $T^{*n} * \rho_0 = T^{*n}$

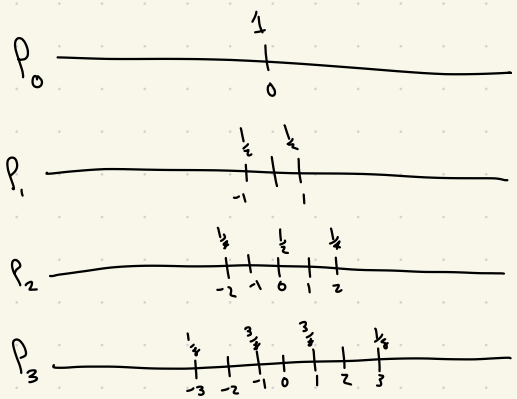
$$\rho_1 = \frac{1}{4}(\delta_{-2} + 2\delta_0 + \delta_2)$$

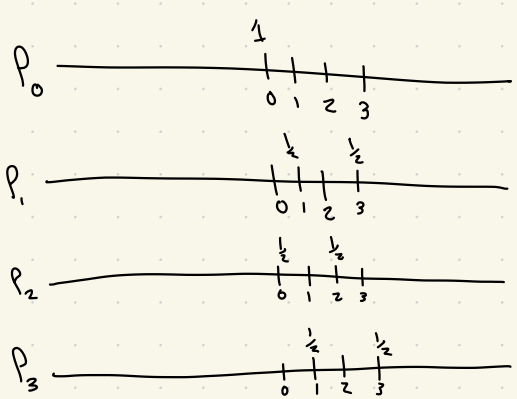
$$\rho_2 = (T * \rho_1)(x) = \sum_{y \in G} T(x-y)\,\rho_1(y) \qquad y = -2, 0, 2$$

$$= \frac{1}{4}\left(T(x+2) + 2T(x) + T(x-2)\right)$$

$$= \frac{1}{4}\left(\frac{1}{2}(\delta_{-3} + \delta_{-1}) + \delta_1 + \delta_{-1} + \frac{1}{2}(\delta_1 + \delta_3)\right)$$

$$= \frac{1}{8}(\delta_{-3} + 3\delta_{-1} + 3\delta_1 + \delta_3)$$





$$\hat{\mathcal{F}}\left(\mathcal{F}\left(T^{*t} * P_0\right)\right)(j) = \frac{1}{5}\sum_{0\le k\le N-1} \overbrace{\mathcal{F}\left(T^{*t} * P_0\right)(j)}^{\text{number in chart}}\, \varepsilon^k(j)$$

$$= \frac{1}{5}\sum_{0\le k\le 4} \# \cdot e^{2\pi i kj/5}$$

$$= \frac{1}{5}\sum_{0\le k\le 4} \frac{1}{3^t}\left(1+2\cos(2\pi j/5)\right)^t e^{2\pi i jk/5}$$

$$G = \langle x, y \mid x^8 = y^2 = yxyx^5 = e \rangle$$

$x^8 = e \Rightarrow |x| \mid 8 \Rightarrow |x| \in \{1,2,4,8\}$

$y^2 = e \Rightarrow |y| \in \{1,2\}$ ← $y^{-1} = y$

$yxyx^5 = e \Rightarrow yxy = x^3$

$yxyx^5 = x^3x^5 = e$

$\Rightarrow (yxy)^{-1} = x^5$

$\Rightarrow |yxy| \mid 8$

e	x	$\cdots$	x^7
y	xy	$\cdots$	x^7y

$yx^ny = yx(x^{n-1}y)$

$yxy = x^3$

$yx = x^3y$

$= x^3yx(x^{n-2}y)$

$= x^6yx^{n-2}y$

$= x^{3n}y^2$

$x^iy^jx = x^iy^{j-1}yx$

$= x^iy^{j-1}x^3y$

$= x^iy^{j-2}x^6y$

$= x$

What came to mind:

↳ for me to feel safe, I generally need my own space somewhat regularly → dorm/bed room
↳ familiarity with surrounding environment → comfort/safety → but also access to people I trust
↘ nature, gym
↓
self-care/physical wellness

Stability → financial, relational

feeling welcomed
action welcomed rather than being judged

What has to change for you to stop being hypervigilant?
↓
how long will that take? Whose work is it?

Organizing: The dynamic multi-layered process of getting ever-increasing numbers of ordinary people to take collective action on their behalf
↳ building a base ↳ Take collective action
↳ Develops leaders & leadership ↳ shifting the balance of power

"Funders' collaborative on youth organizing"

Leadership: People who accept responsibility to create the conditions to achieve a shared goal in the face of uncertainty

"BOLD
Black organizers for leadership & dignity"

"If you don't put your plans into action, you're not leading - you're just making plans"

Campaign: a sequence of tactics with a clear goal, demand, and target that builds capacity and shifts public opinion on your issue, and that can win or lose
- Problem: what is the issue we're trying to address
- Demands: what are some possible solutions
- Target(s): who has the power to meet our demands

- How can others get involved
- Landscape Analysis: what already exists & make this more/less possible? What do we know about our targets?

$$\left(\mathrm{Ind}_H^{D_n} K_k\right)(g) = \begin{pmatrix} K_k(g) & K_k(gs) \\ K_k(sg) & K_k(sgs) \end{pmatrix}$$

$g_1 = e \quad g_2 = s$

$$\left(\mathrm{Ind}_H^{D_n} K_k\right)\left(r^m\right) = \begin{pmatrix} K_k(r^m) & K_k(r^m s) \\ K_k(sr^m) & K_k(sr^m s) \end{pmatrix}$$

$$= \begin{pmatrix} K_k(r^m) & 0 \\ 0 & K_k(r^{-m}) \end{pmatrix}$$

$sr^m = r^{-m}s$

$$\left(\mathrm{Ind}_H^{D_n} K_k\right)(r^m s) = \begin{pmatrix} K_k(r^m s) & K_k(r^m) \\ K_k(sr^m s) & K_k(sr^m) \end{pmatrix}$$

$$= \begin{pmatrix} 0 & K_k(r^m) \\ K_k(r^{-m}) & 0 \end{pmatrix}$$

$\begin{pmatrix} x & y \\ 0 & 1 \end{pmatrix}$ $a, x \in \{1,2,4\}$ $b, y \in \{0,1,\dots,6\}$

$\begin{pmatrix} a & b \\ 0 & 1 \end{pmatrix}$ $a \in \{1,2,4\}$ $b \in \{0,\dots,6\}$ $ay - bx + b \pmod 7$

$x \neq 4$ $ay + 3b$ anything

$3b \in \{0,3,6,2,5,1,4\}$ (0 1 2 3 4 5 6)

y: 0 1 2 3 4 5 6

$2y$: 0 2 4 6 1 3 5

$4y$: 0 4 1 5 2 6 3

$\begin{pmatrix} 4 & y \\ 0 & 1 \end{pmatrix}$ ay

$\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \cdots \begin{pmatrix} 1 & 6 \\ 0 & 1 \end{pmatrix}$

$\begin{pmatrix} 2 & 0 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 2 & 1 \\ 0 & 1 \end{pmatrix} \cdots \begin{pmatrix} 2 & 6 \\ 0 & 1 \end{pmatrix}$

$\begin{pmatrix} 4 & 0 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 4 & 1 \\ 0 & 1 \end{pmatrix} \cdots \begin{pmatrix} 4 & 6 \\ 0 & 1 \end{pmatrix}$

$\begin{pmatrix} a & b \\ 0 & 1 \end{pmatrix} \begin{pmatrix} x & 0 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} ax & b \\ 0 & 1 \end{pmatrix}$

$\begin{pmatrix} a & b \\ 0 & 1 \end{pmatrix} \begin{pmatrix} x & y \\ 0 & 1 \end{pmatrix} \begin{pmatrix} a^{-1} & -a^{-1}b \\ 0 & 1 \end{pmatrix}$

$\begin{pmatrix} ax & ay+b \\ 0 & 1 \end{pmatrix} \begin{pmatrix} a^{-1} & -a^{-1}b \\ 0 & 1 \end{pmatrix}$

$\begin{pmatrix} x & -a^{-1}b \cdot ax + ay + b \\ 0 & 1 \end{pmatrix}$

$\begin{pmatrix} x & ay - bx + b \\ 0 & 1 \end{pmatrix}$

$\begin{pmatrix} \frac{1}{x} & 0 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} ax & b \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} \frac{ax}{x} & \frac{b}{x} \\ 0 & 1 \end{pmatrix}$

0 1 2 3 4 5 6

Def monomial $x_1^{i_1}\cdots x_n^{i_n} =: x^I$

Monomial order $<$ relation on all monomials $k[x_1,\dots,x_n]$ (field, ring) satisfying

i) Exactly one of $x^A < x^B$, $x^A = x^B$, $x^B < x^A$ holds ($A=B$ componentwise)

ii) $x^A < x^B \Rightarrow x^{A+C} < x^{B+C}$

iii) Every set of monomials has a least element

Division Algorithm: Divide $h \in k[x_1,\dots,x_n]$ by $f_1,\dots,f_m \in k[x_1,\dots,x_n] =: \mathcal{R}$, to get $h = a_1f_1+\cdots+a_mf_m+r$ where $a_i, r \in \mathcal{R}$ and the terms of r are not divisible by $LM(f_j)\ \forall j$.

for $f \in k[x_1,\dots,x_n]$, $LM(f)$ = largest monomial with nonzero coefficients in f.

Algorithm: Given $h, f_1,\dots,f_m \in \mathcal{R}$

LT = leading term (includes constant)

so if $f = 11x^{23}$ then $LT(f) = 11x^{23}$ $LM(f) = x^{23}$

1. Initialize: Set $i=0$, $a_1 = \cdots = a_m = r = 0$, $p = h$.
2. If $p=0$, output $a_1,\dots,a_m, r$ and terminate. Else, continue to step 3.
3. Run through j's starting at 1. $j \in \{1,\dots,m\}$
   test: Does $LM(f_j)$ divide $LM(p)$?
   If yes, set $p := p - \frac{LT(p)}{LT(f_j)}\cdot f_j$ $a_j := a_j + \frac{LT(p)}{LT(f_j)}$
   Return to step 2.
   If no, $j := j+1$, goto step 3 or if $j=m$ go to step 4
4. Set $r := r + LT(p)$, set $p := p - LT(p)$
   go to step 2

$f_j = x^{13}+x^9$ $h = x^{23}+x^9$ $x^{13} | x^{23}$

$h - x^{10}f_j = x^{14} - x^9$

lex $\Rightarrow y^{23}+y^{11}-y+1$

Eventually terminates because every set of monomials has a least element! $p \to 0$.

Ideal membership problem: Determine if $h \in \mathcal{R}$ is in the ideal $(f_1,\dots,f_m)$.

Partial result: if division with remainder algorithm returns $r=0$, then $h = \sum_{j=1}^{m} a_jf_j + 0 \in (f_1,\dots,f_m)$.
Unfortunately, we need to do more work. It can happen that the final remainder is $r \neq 0$ but $r \in (f_1,\dots,f_m)$. Thus algorithm does not solve IMP without further work.

Ex. $h=1$, $f_1 = x$, $f_2 = x+1$ $(f_1,f_2) = (1) = k[x]$ but algorithm gives $r=1$.
$LM(f_1) \nmid LM(1)$ and $LM(f_2) \nmid LM(h)$ so return $a_1 = a_2 = 0$, $r=1$.

Def. A monomial ideal $M \subset k[x_1,\dots,x_n]$ is an ideal generated by monomials.

Dickson's Lemma: Every monomial ideal is generated by a finite set of monomials.

Def: Given $I \subset k[x_1,\dots,x_n]$, the ideal $LM(I)$ generated by $\{LM(f) \mid f \in I\}$ is called the ideal of leading monomials of I.

It follows from Dickson's Lemma $\exists$ that $\exists$ a finite subset $\{g_1,\dots,g_\ell\} \subset I$ s.t. $(LM(g_1),\dots,LM(g_\ell)) = LM(I)$.
Such a finite subset $\{g_1,\dots,g_\ell\} \subset I$ is called a Gröbner basis of I

Convention $\emptyset$ is a Gröbner basis for $I = 0$.

Proposition: i) Every ideal $I \subset k[x_1,\dots,x_n]$ has Gröbner bases.
ii) If $\{g_1,\dots,g_\ell\}$ is a Gröbner basis of I, then $I = (g_1,\dots,g_\ell)$
iii) Division algorithm applied to Gröbner basis solves IMP.

Proof: i) follows from Dickson's lemma $\exists$ that $LM(I)$ generated by finite subset of $\{LM(f) \mid f \in I\}$
ii) Given $h \in k[x_1,\dots,x_n]$ run division algorithm to divide h by Gröbner Basis $g_1,\dots,g_\ell$
If $h \in I = (g_1,\dots,g_\ell)$ then $LM(p)$ will always be divisible by $LM(g_i)$ for some $i_j \leq \ell$ since Gröbner basis generates $LM(I)$. Alg terminates with $p = 0$ $h = \sum_j a_j g_j$
iii) If division algorithm yields a non-zero remainder when h is divided by $g_1,\dots,g_\ell$ then $h \notin (g_1,\dots,g_\ell)$ as known previously.

Remaining questions: Dickson's Lemma proof? How to find Gröbner bases?

recall monomial $= x_1^{i_1} x_2^{i_2} \dots x_n^{i_n} =: x^I$
term $= c x^I$, $c \in \mathbb{R}$

Lemma: i) Every ideal $I \subset k[x_1,\dots,x_n]$ has a gröbner basis.
ii) Every gröbner basis for I generates I.

Proof: Let $f \in I$. Fix a monomial order $>$. Let G be a corresponding gröbner basis for I.
$f = LT(f) + \text{lower order terms}$. Choose $g_i \in G$ s.t. $LT(f) = c\, LM(g_i)$ for some $c \in k$.
So $\exists$ monomial $m_i \in k[x_1,\dots,x_n]$ s.t. $LT(f) = \underset{k}{a_i} m_i LT(g_i)$.

Then $f_1 := f - m_1 a_1 g_1 \in I$ or $f_1 = 0$

we repeat until $f_1 = 0$. In a monomial ideal, every set of monomials has a least term.

Solution to ideal membership problem.

Question: Given $f \in k[x_1, \dots, x_n]$, is $f \in I$?

Algorithm: Let $\{g_1, \dots, g_t\}$ be a Gröbner basis for I.

Apply division with remainder to divide f by $g_1, \dots, g_t$. This leads to $f = g_1 q_1 + \dots + g_t q_t + r$.

Then $LM(r)$ is not a multiple of any $LM(g_i)$ $\forall i$ or $r = 0$.

In case a, $r \notin I \Rightarrow f \in I$

otherwise, $r = 0 \in I \Rightarrow f \in I$.

Def: Let $M < k[x_1, \dots, x_n]$ be a monomial ideal. A monomial $m \in M$ is indivisible if it is not a multiple of another monomial in M.

Ideal equality problem: how to tell if $(f_1, \dots, f_n) = (h_1, \dots, h_s)$

The underlying point: Given fixed $<$, $k[x_1, \dots, x_n]$, every ideal has a unique best Gröbner basis called the reduced Gröbner basis.

$\Leftrightarrow$ Same reduced Gröbner bases?

Lemma: Every monomial ideal has a unique best generating set:

i) Every monomial generating set for M contains all indivisible monomials

ii) Set of indivisible monomials of M is finite

iii) The indivisible monomials generate M.

Pf: i) Clear (think about it)

ii) follows from (i) and Dickson's lemma

iii) Every monomial in M is a multiple of an indivisible monomial.

Lemma: Let $I \neq (0)$ be an ideal in $k[x_1, \dots, x_n]$

Then $\exists$ a Gröbner basis $\{g_1, \dots, g_p\}$ for I s.t.

i) Taking leading monomials gives a bijection

$\{g_1, \dots, g_p\} \longleftrightarrow$ set of all indivisible monomials in $LM(I)$.

ii) No term in g_i is divisible by $LM(g_j)$ for $j \neq i$.

iii) Leading coeff of each g_i is 1.

Proof: i) Given any Gröbner basis for I, $\{g_1, \dots, g_q\}$, we have $\{LM(g_1), \dots, LM(g_q)\}$ generate $LM(I)$. By previous lemma, $\exists$ subset $\{g_1, \dots, g_p\}$ s.t. $\{LM(g_1), \dots, LM(g_p)$ are distinct indivisible

Monomials. Then generate $LM(I)$ by iii) above, so $\{g_1,\dots,g_p\}$ is a Gröbner basis. → reduced Gröbner basis

ii) applied division with remainder

iii) Let $\{g_1,\dots,g_p\} \subset I$ is a reduced Gröbner basis. Suppose $\{g_1,\dots,g_p\}$ and $\{h_1,\dots,h_p\}$ are two ordered reduced Gröbner bases for I s.t. $LM(g_i) = LM(h_i)$.

Then $LM(g_i - h_i)$ is not divisible by any $LM(g_i)$ or $LM(h_i)$ by property ii).

and $g_i - h_i$ has no leading term divisible by $LM(g_i) = LM(h_i)$ $\therefore g_i - h_i = 0$.

Solving systems of polynomial equations

Ex.

$$\begin{aligned} x + 2y + 3z + 4w &= 5 \\ x + 3y + 6z + 7w &= 8 \\ x + 2y + 9z - 2w &= 10 \end{aligned} \rightsquigarrow \left[\begin{array}{cccc|c} 1 & 2 & 3 & 4 & 5 \\ 1 & 3 & 6 & 7 & 8 \\ 1 & 2 & 9 & -2 & 10 \end{array}\right] \rightsquigarrow \left[\begin{array}{cccc|c} 1 & 0 & 0 & -5 & 3/2 \\ 0 & 1 & 0 & 6 & 1/2 \\ 0 & 0 & 1 & -1 & 5/6 \end{array}\right] \rightarrow \begin{aligned} x &= 3/2 + 5w \\ y &= 1/2 - 6w \\ z &= 5/6 + w \end{aligned}$$

line in 4-space parametrized by w

Try to extend this method to systems of nonlinear polynomials → "Elimination"

Choose a monomial order to eliminate first r variables in $x_1,\dots,x_n$. Meaning: every monomial in subring $k[x_{r+1},x_{r+2},\dots,x_n]$ is less than all monomials in $k[x_1,\dots,x_n] \setminus k[x_{r+1},\dots,x_n]$.

Example: $x_1 > x_2 > \cdots > x_n$. Then lexicographic order is an elimination order for every r.

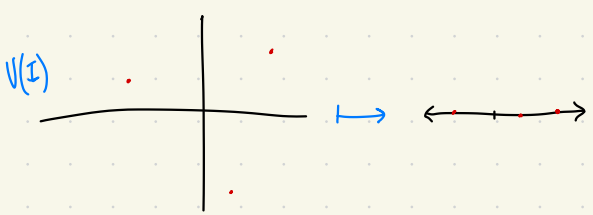
Projection on last $n-r$ coordinates $\mathbb{C}^n \xrightarrow{pr} \mathbb{C}^{n-r}$

$(a_1,\dots,a_n) \mapsto (a_{r+1},\dots,a_n)$

Variety $V(f_1,\dots,f_m) = V(I)$ $\subset \mathbb{C}[x_1,\dots,x_n]$

$I = (f_1,\dots,f_m) = \{\sum g_i f_i \mid g_i \in \mathbb{C}[x_1,\dots,x_n]\}$

We can project $V(I) \longmapsto pr(V(I))$



Idea: if we can describe projection down to x-axis and y-axis, then we know solution set up to finite problem (checking intersections)

"Projective varieties"

Projection of Varieties $\Leftrightarrow$ intersection of ideals

$\mathbb{C}^n \to \mathbb{C}^{n-r}$

$V(I) \to pr(V(I))$ $\qquad I \to I \cap k[x_{r+1},\dots,x_n]$

Let $\{g_1, \dots g_p\} = G$ be a Gröbner basis for $I \subset k[x_1, \dots, x_n]$ in an elimination order for first r variables.

Lemma: $G \cap k[x_{r+1}, \dots, x_n]$ is a Gröbner basis for $I \cap k[x_{r+1}, \dots, x_n]$.
How to compute intersection? Just choose polynomials involving only the last $n-r$ variables!

Proof: $LM(I) \cap k[x_{r+1}, \dots, x_n] = LM(I \cap k[x_{r+1}, \dots, x_n])$ immediate from definition of elimination on order of first r variables

Solve a problem: Describe solution set $V(\underbrace{f_1(x,y), f_2(x,y)}_{I = (f_1, f_2)}) \subset \mathbb{R}^2$ ($f_1, f_2 \in \mathbb{R}[x,y]$)

Choose lex order with $x > y$, eliminate x.
Compute Gröbner basis for I with singular:
Smallest terms in Gröbner basis listed first: $(g_1(y), g_2(x,y), g_3(x,y), \dots)$
Find real roots of $g_1(y)$ using your favorite method.
Next, repeat with $y > x$ to eliminate y, find basis etc.
Finally, plug in (x,y) into polynomials to check.

Lemma: Let R be a commutative ring. TFAE
i) Every ideal I is finitely generated
ii) Every ascending chain of ideals stabilizes: for
$J_1 \subset J_2 \subset \cdots$
There exists some N s.t. for $n \geq N$, $J_n = J_N$

Problem: Describe solution set to systems of polynomial equations

$$f_1(x_1, \dots, x_n) = \cdots = f_m(x_1, \dots, x_n) = 0$$

Equivalently, describe $V(I)$ where $I = (f_1, \dots, f_m) \subset \mathbb{C}[x_1, \dots x_n]$
(eliminate first r variables)
Project $\pi_r : \mathbb{A}^n \to \mathbb{A}^{n-r}$ then $\pi_r(V(I)) \subset V(I')$ where $I' = I \cap k[x_{r+1}, \dots, x_n]$
Projections of varieties need not be varieties themselves. $\subset$ not always an isomorphism
fortunately, $\subset$ is always almost $=$. This is a long story and won't be proved.
If $n - r = 1$ → project onto one dimensional space then equality always holds $\pi_r(V(I)) = V(I \cap k[x_n])$

Implicitization: Given a parametrization, we want to know what we are parametrizing

Example: $\mathbb{A}^1 \to \mathbb{A}^3$, $t \overset{\varphi}{\mapsto} (t^2-1, t^3, t^2+t+1)$

find I such that $V(I)$ = Closure of image of φ.

$$\mathbb{A}^1 \longrightarrow \Gamma \subset \mathbb{A}^1 \times \mathbb{A}^3 \overset{pr}{\to} \mathbb{A}^3$$
$$\qquad\qquad\quad\ \ y_1, y_2, y_3$$

"graph" of $\varphi(t)$

$t \mapsto (t, \varphi_1(t), \varphi_2(t), \varphi_3(t))$

$\Gamma = V(\underbrace{y_1 - (t^2-1),\ y_2 - t^3,\ y_3 - (t^2+t+1)}_{\text{generate an ideal } I \subset \mathbb{C}[t, y_1, y_2, y_3]})$

image $\varphi(\mathbb{A}^1) \subset \mathbb{A}^3$ contained in $V(I \cap k[y_1, y_2, y_3])$

equal up to finitely many pts

$k[t, y_1, y_2, y_3]$

Computation

1. choose monomial order s.t. any non-constant polynomial in $y_1, y_2, y_3 < t$
2. ask singular to compute a Gröbner basis for $I \subset K[t, y_1, y_2, y_3]$
   first entries in output will be polynomials in y_1, y_2, y_3 only.
3. Take these polys in y_1, y_2, y_3, call them $g_1, \dots, g_k$. Then $V(g_1, \dots, g_k) \subset \mathbb{A}^3$ is the closure of the image.

Can we go backwards? Only the "simpled" curves can be parametrized. $y^2 - x^3 = 0 \iff t \mapsto (t^2, t^3)$

Existence of Gröbner bases ← Dickson's lemma

↳ Let $J \subset k[x_1, \dots, x_n]$ (k: field) be an ideal generated by a set of monomials.
Then J is generated by a finite subset of monomials

Proof based on ascending chain condition:

Lemma: An ideal $J \subset R$ (commutative ring) is generated by a finite set S $\iff$ every ascending chain of subideals stabilizes. i.e. for $I_1 \subset I_2 \subset \dots \subset J$
$\exists N$ s.t. for all $n > N$, $I_n = I_N$.

Proof: Consider $\mathcal{U} = \bigcup_i I_i \subset J$. Note $\mathcal{U}$ is an ideal

$\Rightarrow$ assume every monomial ideal in J is generated by a finite set of monomials. Let $I_1 \subset I_2 \subset \cdots$ be an ascending chain of monomial ideals. Then $\mathcal{U}$ is generated by a finite set of monomials $m = \{m_1, \ldots, m_n\}$ the chain stabilizes when $I_N = m$.

$\Leftarrow$ Suppose $\mathcal{U}$ is not finitely generated. Take a generating set containing $i_1, i_2, i_3, i_4, \ldots$ (monomials) then $I_N = (i_1, \ldots, i_N)$ is an ascending chain that does not stabilize.

Dickson's Lemma Proof:

Proof: Suffices: Every ascending chain of monomial ideals stabilizes.
Use induction on n.
$n=1$ $k[x_1]$ Euclidean domain $\Rightarrow$ PID.
Assume assertion holds for $n = N+1$. Let $I \subset k[x_1, \ldots, x_{N+1}]$ be a monomial ideal
For each m define monomial ideal $J_m \subset k[x_1, \ldots, x_N]$ to be generated by all monomials $x_1^{a_1} \cdots x_N^{a_N} := x^a$ s.t. $x^a \cdot x_{N+1}^m \in I$. Note $J_m \subset J_{m+1}$. We have ascending chain of monomial ideals. It stabilizes at some J_M.
$I \subset k[x_1, \ldots, x_N, x_{N+1}]$ is generated by all $x_1^a \cdots x_N^a x_{N+1}^m$ s.t. $x_1^{a_1} \cdots x_n^{a_n} \in J_m$.
By induction, J_m is generated by a finite set $\{x^a \mid a \in A_m\}$ (A_m finite)
$\therefore I$ generated by the finite set $\bigcup_{m=1}^{M} \{x^a x_{N+1}^m \mid a \in A_m\}$.

Given an ideal $I \subset k[x_1, \ldots, x_n]$ fix a monomial order.
We take the ideal of leading monomials $LM(I)$. This monomial ideal is finitely generated by $\{g_1, \ldots, g_s\}$ s.t. $LM(g_1), \ldots, LM(g_s)$ generate $LM(I)$.
By def this is a Gröbner basis for I, so we have proven their existence.

We can compute the closure of the image of an algebraic set under any polynomial map.

V
$\vdots$
$\parallel$

More precisely, given $V(f_1(x_1, \ldots, x_l), \ldots, f_m(x_1, \ldots, x_l)) \subset \mathbb{A}^l$ (think $\mathbb{C}^l$)
and $\rho : \mathbb{A}^l \to \mathbb{A}^n$, $\rho(a_1, \ldots, a_l) = (\rho_1(a_1, \ldots, a_l), \ldots, \rho_n(a_1, \ldots, a_l))$, $\rho_i \in k[x_1, \ldots, x_l]$

Then we can find an ideal $I' \subset k[x_1, \ldots, x_l]$
s.t. $V(I) \setminus W \subset \rho(V) \subset V(I') \subset \mathbb{A}^n$ where $W \subset V(I')$ is a variety with $\dim(W) < \dim(V(I'))$.

Identify $\Gamma: \mathbb{A}^l \xrightarrow{\text{graph}} \mathbb{A}^l \times \mathbb{A}^n \xrightarrow{\rho_n} \mathbb{A}^n$ } implicitization

$(a_1, \dots, a_l) \mapsto (a_1, \dots, \rho_1(a), \dots, \rho_n(a))$

Image of graph map is an algebraic set:

$\Gamma = V(I) \quad I = (f_1(x_1, \dots, x_k), \dots, f_m(x), y_1 - \rho_1(x), \dots, y_n - \rho_n(x))$

Define $I' = I \cap k[y_1, \dots, y_n]$.

Last time

Radical ideals in $k[x_1, \dots, x_n]$ in bijective correspondence with varieties in $\mathbb{A}^n_k = k^n$. (V one way, I the other)

$V(I) = \{\vec{a} = (a_1, \dots, a_n) \in \mathbb{A}^n_k \mid f(\vec{a}) = 0 \ \forall f \in I\}$

$I(V) = \{f \in k[x_1, \dots, x_n] \mid f(\vec{a}) = 0 \ \forall \vec{a} \in V\}$

V, I mutually inverse bijections

$V(\langle x \rangle) = V(\langle x^2 \rangle)$ ← not radical

operations on ideals ↔ operations on varieties

Bijections are inclusion reversing: $I \subset J \Rightarrow V(I) \supset V(J)$

$V \subset W \Rightarrow I(V) \supset I(W)$

Ideals $\rightleftarrows$ (I, V) Varieties

$I = (f_1, \dots, f_n)$

$J = (h_1, \dots, h_m)$ $\longleftrightarrow$ $V(I) \cap V(J) = V(I+J)$

$I + J := (f_1, \dots, f_n, h_1, \dots, h_m)$

$I \cdot J = (f_1 h_1, \dots f_n h_1, f_1 h_2, \dots, f_n h_m) \longleftrightarrow V(I \cdot J) = V(I) \cup V(J)$

$I \cap J \longleftrightarrow V(I \cap J) \overset{?}{=} V(I) \cup V(J)$

not necessarily radical ideals ⇒ no bijective correspondence

If we have a function f in the intersection, $f \in I \cap J$, then f vanishes on $V(I)$ and $V(J)$ $\Rightarrow V(I \cap J) \supset V(I) \cup V(J)$

But $I \cdot J \subset I \cap J \Rightarrow V(I \cdot J) \supset V(I \cap J)$ ∎
$V(I) \cup V(J)$

Computing GCDs in $k[x_1, \dots, x_n]$

Note: $(f(x_1, \dots, x_n)) \cap (h(x_1, \dots, x_n)) =$ all polynomials which are multiples of both f and h.
$= (LCM(f,h))$

Computing $I \cap J$: $I = (f_1, \dots, f_n)$ $J = (h_1, \dots, h_m)$
define ideals $tI = (tf_1, \dots, tf_n)$ $(1-t)J = ((1-t)h_1, \dots, (1-t)h_m)$

Lemma $I \cap J = \underbrace{k[x_1, \dots, x_n] \cap (tI + (1-t)J)}_{\text{eliminate a variable! we can do this using Gröbner bases}} \subset k[t, x_1, \dots, x_n]$

Proof: call $\mathcal{L} := tI + (1-t)J$. let $t = 0$. Then $\mathcal{L} = J$.
$t = 1$, Then $\mathcal{L} = I$

$k[t, x_1, \dots, x_n] \to k[x_1, \dots, x_n]$
$m_a(t) = 0$ $\mathcal{L} \to J$
$m_1(t) = 1$ $\mathcal{L} \to I$
⋮

$\mathcal{L} \cap k[x_1, \dots, x_n]$ polynomials in x's
$\cap$
$I \cap J$

The inclusion $I \cap J \subset k[x_1, \dots, x_n] \cap \mathcal{L}$ is clear

∎

Summarize:
1. we can compute intersections of ideals $I \cap J \subset k[x_1, \dots, x_n]$ by computing $k[t, x_1, \dots, x_n] \cap (tI + (1-t)J)$,
compute Gröbner basis using lex order with $t > x_1 > \dots > x_n$

2. $(LCM(f,h)) = (f) \cap (h)$ so we can compute it!

3. $GCD(f,h) = f \cdot h \,/\, LCM(f,h)$ so we can compute it as well!

Task: Describe solution set to $f(x,y) = 0 = h(x,y)$
In Singular,
```
> ring R = 0, (x,y), lp;
> ideal I = f(x,y), h(x,y);
> ideal J = std(I);
> J;
```

$J[1] = g_1(y)$ (increasing monomial order of leading terms)

$J[2] = g_2(x,y)$

If $g_1(y) = 1$, solution set is empty

$\Downarrow$ no $J[2], J[3], \dots$,

$J = k[x_1, \dots, x_n]$,

$V(J) = \emptyset$

If $J[1] = p(y)$, solution set contained in set of lines $V(f,h) \subset V(y-r_1) \cup \dots \cup V(y-r_n)$

where $r_1, \dots, r_n$ are roots of $p(y)$

now, reverse order $(y,x) \leftrightarrow (x,y)$ and repeat.

Suppose $J[1]$ has both x and y.

$I = (f,h) \Rightarrow I \cap k[y]$ has Gröbner basis empty, which is the basis for the ideal (0)

$\Rightarrow$ vanishes everywhere

So

$V(f,h)$ contains a curve in $\mathbb{C}^2$. This curve is $V(GCD(f,h))$

what's left after we remove the curve from our solution set?

$V\left(\frac{f}{GCD(f,h)}, \frac{h}{GCD(f,h)}\right)$ $\rightarrow$ finite set of points, use method above to compute.

We've proved the existence of Gröbner bases, but how can we construct them?

Tools for construction

Given $I = (f_1, \dots, f_n) \subset k[x_1, \dots, x_n]$, we wish to construct a Gröbner basis for I.

LCM of $x_1^{a_1} \cdots x_n^{a_n}$ and $x_1^{b_1} \cdots x_n^{b_n}$ is $x_1^{\max(a_1,b_1)} \cdots x_n^{\max(a_n,b_n)}$

The S-polynomial $S(f_1, f_2)$ cancels the leading monomials in f_1 and f_2.

$\gamma_{1,2} := (\gamma_1, \dots, \gamma_n) = (\max(a_1,b_1), \dots, \max(a_n,b_n))$

$x^{\gamma_{1,2}} := LCM(LM(f_1), LM(f_2))$

$$S(f_1,f_2) = \frac{x^{\gamma_{1,2}} \cdot f_1}{LT(f_1)} - \frac{x^{\gamma_{1,2}} \cdot f_2}{LT(f_2)}$$

Note that $x^{\gamma_{1,2}}/LT(f_1)$ is a polynomial because of LCM.

$S(f_1, f_2) \in (f_1, f_2)$

$h_1 f_1 + h_2 f_2$ $\quad x^{\gamma_{1,2}} > LM(h_1 f_1)$ $> LM(h_2 f_2)$

Buchberger's criterion for when $f_1, \dots, f_s$ is a Gröbner basis for $I = (f_1, \dots, f_s)$

Thm: $f_1, \dots, f_s$ is a Gröbner basis $\iff$ division of every $S(f_i, f_j)$ $1 \le i < j \le s$ gives remainder zero.

Thm 2 Buchberger's algorithm: the following constructs a Gröbner basis for $I = (f_1, \dots, f_r) < k[x_1, \dots, x_n]$

Step 1: Initialize $i = 1$, $j = 2$

Run through $2 \le j \le r$

is remainder of dividing $S(f_i, f_j)$ by $f_1, \dots, f_r$ zero?

if yes, go to step 2. If no, go to step 3.

Step 2: Increase j by 1 if $j < r$ and go to step 1.

If $j = r$, increase i by 1 if $i < r-1$ and go to step 1

If $i = r-1$ then output $f_1, \dots, f_r$, which is the desired Gröbner basis.

Step 3: Set f_{r+1} = remainder. Increase r by 1 and return to step 1.

Note: $(f_1, \dots, f_r) \subset (f_1, \dots, f_{r+1}) \subset \cdots$ is an ascending chain of ideals in $K[x_1, \dots, x_n]$. When it stabilizes, there will be no more remainders. Thus step 2 must give (eventually) a Gröbner basis.

Proof of thm 1: Show all remainders of all $S(f_i, f_j)$ on division by $f_1, \dots, f_r = 0$

$\Rightarrow f_1, \dots, f_r$ is a Gröbner basis for $(f_1, \dots, f_r)$.

Proof by contradiction $\rightarrow$ assume all remainders of above divisions are zero but that $f_1, \dots, f_r$ is not a gröbner basis. So there exists $h \in (f_1, \dots, f_r) = I$ s.t. $LM(h) \notin (LM(f_1), \dots, LM(f_r))$

$h = h_1 f_1 + \cdots + h_r f_r$

i) we may assume that maximum of $LM(h_j f_j) = x^\gamma$ is minimal for all such expressions

ii) We may assume $x^\gamma = LM(h_1 f_1) = LM(h_2 f_2)$

iii) We may assume this s.t. $x^\gamma = LM(h_j f_j)$ is minimal

Subtract $c x^\gamma S(f_1, f_2) - \sum_{j=1}^{r} h_j f_j = 0$

from both sides of

When $\frac{LM(h_1 f_1) x^\gamma}{LT(h_1 f_1)} = \frac{LM(h_2 f_2) x^\gamma}{LT(h_2 f_2)}$

This gives a new relation which is somehow a contradiction ...?
contradicts minimality

$f(t_v) = f'(t_v)\, v$