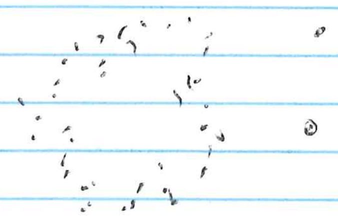
Lecture 1
TDA

§0. Big Picture, where we're going.

<u>Input</u>: Point cloud data = a bunch of points X



<u>Goal</u>: Extract <u>meaning</u> from X. Suppose X was sampled from some object Y. "Find" Y

What does "Find Y" mean? If Y is some space, we might want to analyze the topology with some <u>invariants</u> = algebraic topology.

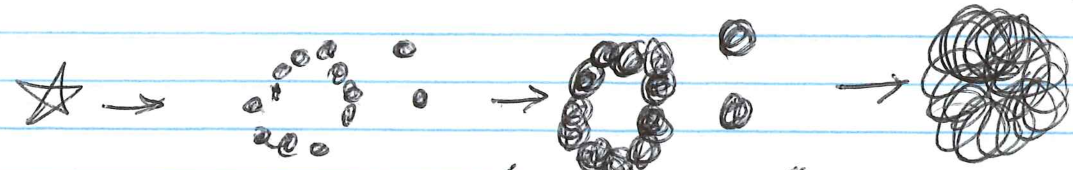
algebraic → First 3 lectures

topology → Second 3 lectures.

Lecture 7 → <u>Idea</u>: $X = \bigcup_{p \in X} p$. Start fattening the points

$$X_\varepsilon = \bigcup_{p \in X} N_\varepsilon(p)$$

Revert back to our halycon days of childhood, and "connect the dots"



ε Too Small — "Goldilocks Zone" — ε Too Big

Lecture 1

For the "Goldilocks Zone" picture, we have, topologically,  $= S^1 + 2$ points. $= X_G$

Once we have the tools of algebraic topology in hand, we'll see that

$$H_1(X_G) \{\text{say, with } \mathbb{Q} \text{ coeffs}\} = \mathbb{Q} \rightsquigarrow \text{tells us } S^1$$

$$H_0(X_G) = \mathbb{Q}^3 = 3 \ \underline{\text{components}}$$

This is persistent homology PH. We have a parameter ε. What if we have more than one parameter? In the one parameter case, $H_i(X_\varepsilon)$ is a module over $\mathbb{R}[\varepsilon] \leftarrow$ PID {first 3 Lectures}

Lecture 8 $\rightarrow$ But with more parameters, we get modules over Polynomial rings $\mathbb{R}[x_1 .. x_n] \leftarrow$ Algebraic Geometry!

GAME ON!

Algebra Boot Camp

1. Rings, ideals, Hilbert Basis Thm modules, quotients, localization.
2. Lin Alg review, Lin transforms, $K[t]$ modules, Rat. Can. Form.
3. Euclidean domains, PID, structure theory for module / PID.

Lecture 1

Rings: R is a set of objects with two operations, $+, \cdot$; satisfying

- R is closed under the opns.
- R is an abelian group under $+$
- multiplication $(\cdot)$ is associative
- $+, \cdot$ distributive $(a+b)\cdot c = ac+bc$.

In general, a ring need not have a multiplicative identity (1), and need not be commutative (e.g. square matrices).

☆ In this class, all rings will be commutative with unit.

Examples:
- any field $\mathbb{Q}, \mathbb{R}, \mathbb{C}, \mathbb{Z}/\text{prime}$ { I'll use k for field
- polynomials with coefficients in k.

Homomorphisms For rings R, S, a homomorphism $R \xrightarrow{\phi} S$ is a map that "preserves the operations"

i.e. $\phi(r_1+r_2) = \phi(r_1)+\phi(r_2)$

$\phi(r_1 \cdot r_2) = \phi(r_1)\cdot\phi(r_2)$

Easy Check

$\phi(0_R) = 0_S$, $\phi(1_R) = 1_S$.

Examples: $\mathbb{Z} \to \mathbb{Z}/\langle\alpha\rangle$ $\alpha \in \mathbb{Z}$

$K[x_1] \longrightarrow K[y_1, y_2]$ $x_1 \longmapsto g(y_1, y_2)$

$K[x_1, x_2] \longrightarrow k[y_1]$ $x_1 \longmapsto g_1(y_1)$
$x_2 \longmapsto g_2(y_1)$

Lecture 1

Modules: "Module is to ring as
Vector space is to field"

DEF: An R-module M is
- an abelian group under $+$ {can add vectors}
- with an action of R on M s.t.

$\alpha_i \in R$
$v_i \in M$

- $\alpha_i v_i \in M$
- $(\alpha_1 \alpha_2) v_i = \alpha_1(\alpha_2 v_i)$
- $(\alpha_1 + \alpha_2) v_i = \alpha_1 v_i + \alpha_2 v_i$
- $1 \cdot v_i = v_i$
- $0 \cdot v_i = 0$
- $\alpha_i (v_1 + v_2) = \alpha_1 v_1 + \alpha_2 v_2$.

Remark If your linear algebra is rusty, next lecture will include a turbo review ☺.

DEF: An R-module M which is a subset of R is an *ideal*.

Example 1: The set of all multiples of a fixed $n \in \mathbb{Z}$. (which we write as $\langle n \rangle$)

Example 2: if $\{f_1, \dots f_k\} \subseteq R$, we can take all elements $\sum_1^k \alpha_i f_i$, $\alpha_i \in R$, which is an ideal, written $\langle f_1, \dots, f_k \rangle$.

Example 3 $\phi : R \to S$ a ring homomorphism.
$\operatorname{Ker} \phi = \{ r \in R \mid \phi(r) = 0 \}$ is an ideal.

Lecture 1

Special Types of Rings

DEF R is a field if $\forall\ 0 \neq \alpha \in R$, $\exists\ \beta$ s.t. $\alpha\beta = 1$ ((if R not commutative, could have different left + right inverses, and we get a division ring (quaternions))

Examples $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$, $\mathbb{Z}/\text{prime}$, $K(t_1 \ldots t_n)$ ← who is this

"rational functions" → $K(t_1 \ldots t_n) = \dfrac{f(t_1 \ldots t_n)}{g(t_1 \ldots t_n) \neq 0}$ where $f, g \in k[t_1 \ldots t_n]$

DEF: R is an integral domain if there are no (non-trivial) zero divisors.

SUB-DEF: $a \in R$ is a zero divisor if $\exists\ b \neq 0$ in R with $a \cdot b = 0$.

Example of zero divisors: in $\mathbb{Z}/6$, $2 \neq 0 \neq 3$, but $2 \cdot 3 = 0$ }

Example: $\mathbb{Z}/6$ is not an integral domain.

DEF: An ideal $I \subseteq R$ is prime if $f \cdot g \in I \Rightarrow f \in I$ or $g \in I$

An ideal $I \subsetneq R$ is maximal if $\neg \exists\ J$ with $I \subsetneq J \subsetneq R$.

Examples: $p \in \mathbb{Z}$ prime, then $\langle p \rangle$ is prime.

Exercise Prove maximal $\Rightarrow$ prime, but prime $\not\Rightarrow$ maximal.

DEF I an ideal in R, then R/I is a ring, with objects $\alpha + [I]$, $\alpha \in R$, and $+, \cdot$ inherited from R.

Lecture 1

Theorem (A) R/I is an integral domain $\iff$ I is prime.
(B) R/I is a field $\iff$ I is maximal.

Pf: (A) R/I domain $\iff a \cdot b = 0 \Rightarrow a = 0$ or $b = 0$
$\iff a \cdot b \in I \Rightarrow a \in I$ or $b \in I$
$\iff$ I prime. $\blacksquare$

(B) Suppose R/I field, I not max $\Rightarrow I \subsetneq J \subsetneq R$
take $j \in J$. $\exists j'$ s.t. $(j + [I]) \cdot (j' + [I]) = 1$
(since R/I field) $\Rightarrow jj' + \underbrace{j i_1 + j' i_2 + i_1 i_2}_{= 0 \text{ in } R/I} = 1$
$\Rightarrow j \cdot j' = 1 \Rightarrow$ J not a proper ideal $\blacksquare$

- One way to study an object is to simplify it by quotienting; we saw this in group theory where $N \triangleleft G$ and we have $0 \to N \to G \to G/N \to 0$. Can study rings the same way $0 \to I \to R \to R/I \to 0$. But there is another way to simplify a ring

Localization: Let S be a multiplicatively closed subset of R.

Example $f \in R$, $S = \{1, f, f^2, \ldots\}$.

Example P a prime ideal, $S = P^{\text{complement}}$.

Q: Is P^{comp} mult closed? $\mathcal{S}$ $a, b \in P^c$

If $a \cdot b \notin P^c$, $a \cdot b \in P$, but P prime $\Rightarrow a \in P$ or $b \in P$, $\Rightarrow\Leftarrow$

Lecture 1

DEF $R_S = \{ f/g \mid f \in R, g \in S \} / \sim$

where $\frac{f_1}{g_1} \sim \frac{f_2}{g_2}$ if $(f_1 g_2 - f_2 g_1) s = 0$ ← some $s \in S$.

Seems hideous ☹.

What we're doing is making everything in S invertible.

__Example 1__ $R = \mathbb{Z}$, $S = \langle 0 \rangle^c$ (note that 0 is a prime ideal in $\mathbb{Z}$)

$$\Rightarrow R_S = \left\{ \frac{\alpha}{\beta} \;\middle|\; \alpha, \overset{\neq 0}{\beta} \in \mathbb{Z} \right\}$$

$$\frac{\alpha}{\beta} = \frac{\gamma}{\Delta} \text{ if } \underbrace{(\alpha\Delta - \beta\gamma) \cdot s = 0}$$

$\Longleftrightarrow$ ($\mathbb{Z}$ a domain, so $\Longleftrightarrow (\alpha\Delta - \beta\gamma) = 0$

$\Longleftrightarrow \begin{vmatrix} \alpha & \gamma \\ \beta & \Delta \end{vmatrix} = 0 \Longleftrightarrow \frac{\alpha}{\beta} = \frac{\gamma}{\Delta}$ in $\mathbb{Q}$.

i.e. $\mathbb{Z}_{0^c} = \mathbb{Q}$.

DEF M an R-module, then M_S is an R_S module, with M_S defined analogously to above.

//

We'll be applying localization as a tool to understand modules over $K[X_1, \ldots X_n]$.

//

Why?
PH ⟷ modules over $K[X]$
MPH ⟷ modules over $K[X_1, \ldots X_n]$
} very different rings!

Lecture 1

Polynomial Rings

Lecture 8 → It will turn out to be the case, when analyzing MPA, that we need to understand

Modules over $K[x_1 .. x_n] = S$ (symmetric algebra)

First, lets analyze the simplest modules over S
ideals

DEF A ring is Noetherian if it satisfies ACC

ACC: [there are no ∞ ↗ chains of ideals $I_1 \subsetneq I_2 \subsetneq I_3 \cdots$] $\Longleftrightarrow$ every ideal is finitely generated

{ to see these are the same, take an ∞ ascending chain of ideals, $\cup I_i$ is an ideal, Zorn }

{ same def. for modules }.

Thm (Hilbert Basis Theorem) If A is Noetherian, so $A[x]$ is Noetherian.

Pf: ~~Let~~ Let I be an ideal in $A[x]$

$I = \langle f_i(x) \mid f_i$ coeffs in $A \rangle$ ← maybe ∞ # gens!

Let $I' = \{$ lead coeffs of elts of I $\}$.
$f = \boxed{a_n} x^n + \cdots + a_0$

Check I' an ideal, so f'gend, say by $g_1 \dots g_m$. For each g_i, $\exists$ f_i of form $f_i = g_i x^{m_i} +$ lower order terms.

Lecture 1

Set $m = \max\{m_i\}$.

Now, given any $f \in I$, we can chop it down by the f_i until it has lead term of degree $< m$

i.e $f = \sum_{j=1}^{n} a_i f_i + f'$ deg $f' < m$.

Now consider the A-module M generated by $\{1, x, \dots x^{m-1}\}$

it is f'gend, so Noetherian, so $M \cap I$ is f'gend, by $h_1, \dots, h_k$.

By construction, $I = \langle f_1, \dots f_n, h_1, \dots h_k \rangle$ ∎

<u>KEY POINT</u> An ideal $I \subseteq S = k[x_1, \dots x_n]$ is finitely generated.

<u>Varieties</u>: We can visualize I geometrically

Let $V(I) = \{ p \in k^n \mid f_i(p) = 0 \ \forall f_i \in I \}$

$V(I)$ is just the solution set of all the $f \in I$: because I is f'gend, say by $f_1 \dots f_m$, we only need to find $V(f_i)$, $i = 1 \dots m$.

<u>Example</u> f_i are linear, then this is just solns to a system of linear eqns!

<u>Algorithm</u>: In above example, we find solns by <u>Gaussian</u> <u>Elim</u>

For higher degree eqns, we find solns via <u>Gröbner</u> <u>Bases</u>.

Lecture 1

Exercises (Hw)

1. Prove a maximal ideal is prime, but a prime ideal need not be maximal.

2. Prove a finite integral domain R is a field
   (Hint: need to show any $0 \neq r \in R$ has an inverse. Write R as $\{0, 1, r_1, \ldots r_n\}$, and consider multiplication by $r = r_1$)

3. We know if $p \in \mathbb{Z}$ is a prime #, then $\langle p \rangle$ is a prime ideal. Prove it is also maximal, i.e. show $\mathbb{Z}/\langle p \rangle$ is a field.