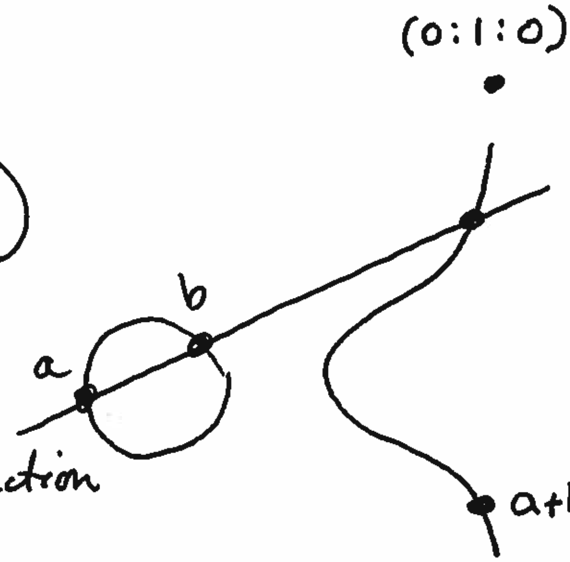
Lecture 37:



Last time: Elliptic Curves

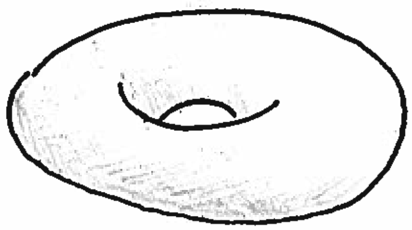
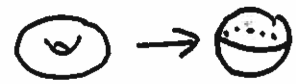
$$C = V_{\mathbb{P}^2_{\mathbb{C}}}\left(y^2 - x(x-\alpha)(x-\beta) \right)$$

which has a group law

Have $\pi : C \longrightarrow \mathbb{P}^1_{\mathbb{C}}$ which is projection

$$(x:y:z) \longmapsto (x:z)$$

onto the x-axis. This is 2-to-1, except for $\{0, \alpha, \beta, \infty\}$ which have only two preimages.

Fact: $C =$  and $\pi :$ 

is the quotient of C by  π; with respect to the group law, this map is $a \mapsto -a$.

Plausibility Arguments: (a)  $= S^1 \times S^1$ is a group since $S^1 \leq (\mathbb{C} \setminus \{0\}, \times)$

(b) π is locally a homeomorphism except at $(0,0)$, $(\alpha,0)$, $(\beta,0)$ and $\mathcal{O} = (0:1:0)$. This is called a branched cover, and it turns out the above is the only one with this data.

Topology of curves in $\mathbb{P}^2_{\mathbb{C}}$:

$V = \mathbb{V}(f)$ where f = homogenous poly in $\mathbb{C}[x, y, z]$.

with V smooth and irreducible.

So far, we've seen:

1. f linear, i.e. V is a line, which are all the same by HW. Moreover

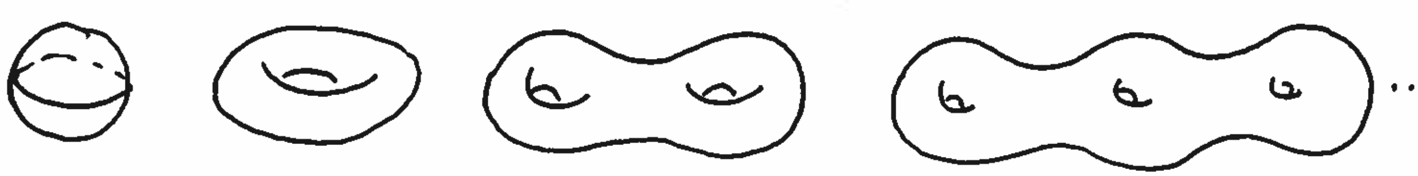
$$V = \mathbb{V}(y) = \begin{pmatrix} x\text{-axis} \\ +(1:0:0) \text{ at } \infty \end{pmatrix} = \mathbb{P}^1_{\mathbb{C}} =$$ 

2. f quadratic, i.e. V a conic.

$$V = \mathbb{P}^1_{\mathbb{C}} =$$ 

3. f cubic, i.e. V = elliptic curve = . Has a group law.

In general, V is a compact surface, namely one of:



$g=0$ $g=1$ $g=2$ $g=3 \ldots$

g is called the genus of V. While this is over $\mathbb{C}$, there are important consequences for $k = \mathbb{Q}$.

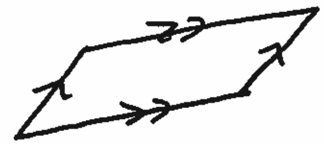
<u>Ex</u>: <u>Fermat's Last Thm</u>: When $n \geq 3$

$$\mathbb{V}_{\mathbb{P}^2_{\mathbb{Q}}}(x^n + y^n - z^n) = \emptyset.$$

Suppose $f \in \mathbb{Q}[x,y,z]$ is homogenuous. Consider

$$\left(\mathbb{V}_{\mathbb{Q}} = \mathbb{V}_{\mathbb{P}^2_{\mathbb{Q}}}(f)\right) \subseteq \left(\mathbb{V}_{\mathbb{C}} = \mathbb{V}_{\mathbb{P}^2_{\mathbb{C}}}(f)\right)$$

Amazing fact: How many points $V_{\mathbb{Q}}$ has depends on the genus of $V_{\mathbb{C}}$!

genus	$V_{\mathbb{Q}}$	Symmetries of $V_{\mathbb{C}}$	Geometry of $V_{\mathbb{C}}$
0 	$\mathbb{P}^1_{\mathbb{Q}}$ or ϕ $x^2+y^2-z^2$ vs. $x^2+y^2-3z^2$	$PGL_2\mathbb{C}$ = $z \longmapsto \frac{az+b}{cz+d}$	Round sphere  unique up to scale
1 	$V_{\mathbb{Q}}$ is a subgp of $V_{\mathbb{C}}$ and is finitely generated: $\exists\ p_i \in V_{\mathbb{Q}}$ s.t. $V_{\mathbb{Q}} = \{n_1p_1 + \cdots + n_kp_k \mid n_i \in \mathbb{Z}\}$	Trans by group elts + a finite group	Euclidean Torus  $\dim_{\mathbb{C}}\left(\text{moduli space of elliptic curves}\right) = 1$
≥ 2 	Falting's Thm (1980s) $V_{\mathbb{Q}}$ is finite. [Almost proved FLT!]	finite	Hyperbolic Geometry $3g-3$ dim'l moduli space.

Goal:

Thm: G a finite gp. Then $\exists$ a Galois extension $K/\mathbb{C}(t)$ with group G.

[First, we need to assoc a field to a variety somehow...]

V alg. variety $\subseteq k^n$ [affine variety]

$$k[V] = \{ f : V \to k \mid f = \text{rest of poly} \}$$
$$= k[x_1, \ldots, x_n] / \mathbb{I}(V)$$

If V is irreducible, then $k[V]$ is an integral domain. In this case, the <u>function field</u> of V, denoted $k(V)$, is the field of fractions of $k[V]$.

An elt of $k(V)$ is called a <u>rational function</u>

and has the form

$$f = \frac{g}{h} \quad \text{for} \quad g, h \in k[x_1, \dots, x_n]$$

Ex: $k = \mathbb{C}$, $V = \mathbb{C}$. Then $\mathbb{C}[V] = \mathbb{C}[t]$

and $\mathbb{C}(V) = \begin{array}{c}\text{rat'l fns}\\ \text{in } t\end{array} = \mathbb{C}(t)$ [Note connection to goal!]

$$f = c\,\frac{(t-a_1)\cdots(t-a_k)}{(t-b_1)\cdots(t-b_k)} \quad \text{no } a_i = b_j, \; c \in \mathbb{C}.$$

Not quite a function $f: V \longrightarrow \mathbb{C}$ as not defined at the b_i.

Def: $f \in k(V)$ is regular at $p \in V$ if it has an expression $f = \frac{g}{h}$ where $h(p) \neq 0$.

Set $\operatorname{dom}(f) = \{p \in V \mid f \text{ regular at } p\}$

Ex: for f as above, $\operatorname{dom}(f) = \mathbb{C} \setminus \{b_1, \dots, b_k\}$

<u>Ex</u>: $V = \mathbb{V}(xw - yz) \subseteq k^4$, $f = \frac{x}{y} \in k(V)$.

As $xw = yz$ in $k[V]$, another expression for f is $\frac{z}{w}$. So $\mathrm{dom}(f) \supseteq \left\{ \text{all pts of } V \text{ with } \begin{matrix} y \neq 0 \ \underline{\underline{\text{or}}} \\ w \neq 0 \end{matrix} \right\}$.

<u>Underlying point</u>: $k[V]$ is not a U.F.D.