Lecture 37:

Last time: Elliptic Curves

\[ C = V_\mathbb{P}^2( y^2 - \chi(x-\alpha)(x-\beta) ) \]

which has a group law

Have \( \pi: C \to \mathbb{P}^1 \) which is projection

\((x:y:z) \mapsto (x:z)\)

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

Fact: \( C = \quad \) and \( \pi: \cdots \to \cdots \)

is the quotient of \( C \) by \( \pi \); with respect to the group law, this map is \( x \mapsto -x \).

Plausibility Arguments:

(a) \( S^1 \times S^1 \) is a group since \( S^1 \leq (C \setminus \{0\}, \times) \)

(b) \( \pi \) is locally a homeomorphism except at \((0,0), (\alpha,0), (\beta,0)\) and \(\infty = (0:1:0)\). This is called a branched cover, and it turns out the above is the only one with this data.
Topology of curves in $\mathbb{P}_C^2$:

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

So far, we've seen:

1. If linear, i.e. $V$ is a line, which are all the same by HW. Moreover
   \[ V = V(y) = (x - \text{axis} + (1:0:0) \text{ at } \infty) = \mathbb{P}_C^1 = \bigcirc \]

2. If quadratic, i.e. $V$ a conic.
   \[ V = \mathbb{P}_C^1 = \bigcirc \]

3. If cubic, i.e. $V$ = elliptic curve = $\bigcirc$. Has a group law.

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

\[ \begin{align*}
& g = 0 \quad g = 1 \quad g = 2 \quad g = 3 \ldots \\
& \bigcirc \quad \bigcirc \quad \bigcirc \quad \bigcirc \\
\end{align*} \]
$g$ is called the genus of $V$. While this is
clear over $\mathbb{C}$, there are important consequences for $k=\mathbb{Q}$.

**Ex:** Fermat's Last Thm: When $n \geq 3$

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

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

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

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

Euclidean Torus

Euclidean Torus

Uniform up to scale

Random affine

Geometry of V

Symmetrics of V

\[ a \rightarrow \frac{c \cdot z + d}{a \cdot z + b} \]

\[ \mathbb{P}^{2}_{D} \]

\[ x^2 + y^2 = z^2 \]

\[ \text{Pro or } \phi \]

\[ \text{or } \phi \]

\[ \text{of } \phi \]

\[ \text{and no further} \]

\[ \Theta \]

\[ \Theta \]

\[ \text{on a move} \]

\[ \text{and no further} \]

\[ \text{C} \]

\[ \text{F} \]

\[ \text{G} \]

\[ \text{H} \]

\[ \text{I} \]

\[ \text{J} \]

\[ \text{K} \]

\[ \text{L} \]

\[ \text{M} \]

\[ \text{N} \]

\[ \text{O} \]

\[ \text{P} \]

\[ \text{Q} \]

\[ \text{R} \]

\[ \text{S} \]

\[ \text{T} \]

\[ \text{U} \]

\[ \text{V} \]

\[ \text{W} \]

\[ \text{X} \]

\[ \text{Y} \]

\[ \text{Z} \]
Goal:

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

First, we need to associate a field to a variety somehow...

$V$ alg. variety $\subseteq \mathbb{A}^n$ [affine variety]

$k[V] = \{ f: V \rightarrow k \mid f = \text{rest of poly} \}$

$= \mathbb{k}[x_1, \ldots, x_n] / \mathcal{I}(V)$

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

An elt of $k(V)$ is called a rational function.
and has the form

\[ f = \frac{g}{h} \text{ for } g, h \in \mathbb{C}[x_1, \ldots, x_n] \]

**Ex.** Let \( k = \mathbb{C}, \ V = \mathbb{C} \). Then \( \mathbb{C}[V] = \mathbb{C}[t] \)

and \( \mathbb{C}(V) = \text{rat'ns in } t = \mathbb{C}(t) \) \[ \text{[Note connection to goal!]} \]

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

Not quite a function \( f : V \to \mathbb{C} \) as not defined at the \( b_i \).

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

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

**Ex.** For \( f \) as above, \( \text{dom}(f) = \mathbb{C} \setminus \{ b_1, \ldots, b_k \} \)
Ex: \( V = V(xw - yz) \subseteq k^4 \), \( f = \frac{x}{y} \in k(V) \).

As \( xw = yz \) in \( k[V] \), another expression for \( f \) is \( \frac{z}{w} \). So \( \text{dom}(f) = \{ \text{all pts of } V \text{ with } y \neq 0 \text{ or } w \neq 0 \} \).

**Underlying point:** \( k[V] \) is not a U.F.D.