(B. Poonen)
22/9/04

II. Curves

$$\left\{\begin{array}{l}\text{geometrically irreducible } k\text{-varieties, of dim 1} \\ \text{dominant rational maps}\end{array}\right\} \longleftrightarrow \left\{\begin{array}{l}\text{f.g. field extension } K \text{ of } k \text{ of transcendence degree 1, in which } k \text{ is relatively alg. closed} \\ k\text{-algebra homomorphisms}\end{array}\right\}$$

$$V \longmapsto k(V)$$

In the left, there a whole isomorfism class which goes to the same extension.

Fact: Within the collection of all 1-dim varieties with a given function field (of tr.deg. 1) there exist one that is smooth and projective, and it is unique up to isomorphism. (means over k)

In the 1-dimensional case,

$$\left\{\begin{array}{l}\text{smooth proj. geometrically irred. 1-dim varieties} \\ \text{dominant morphisms}\end{array}\right\}$$ is equivalent to the first category (k-varieties, dominant rat. maps).

For dim > 1 $\left\{\begin{array}{l}\text{uniqueness is false} \\ \text{existence is known only if char } k = 0. \text{ (resolution of singularities).}\end{array}\right.$

From now on, a curve$/k$ means smooth, projective, geometrically irreducible, 1-dimensional k-variety.

Let be $\phi : C_1 \longrightarrow C_2$ a morphism of curves.

1) If ϕ is constant, $\deg \phi := 0$.

2) Otherwise, ϕ will be dominant, and we get $k(C_2) \hookrightarrow k(C_1)$, and we define $\deg \phi := [k(C_1) : k(C_2)]$.

We will call ϕ $\left\{\begin{array}{l}\text{separable} \\ \text{purely inseparable} \\ \text{galois}\end{array}\right\}$ if $k(C_1)/k(C_2)$ is $\left\{\begin{array}{l}\text{separable} \\ \\ \\ \end{array}\right\}$.

We similarly define $\deg_s \phi$ and $\deg_i \phi$.

Valuations and ramifications.

Let C be a curve, let $\overline{C} = C_{\overline{K}}$, and let $\overline{K}(C)$: the function field of $\overline{C}$.

Let P be a point in $C(\overline{K})$.

Def: The <u>local ring of $\overline{C}$ at P</u> is

$$\mathcal{O}_{\overline{C},P} := \{ f \in K(\overline{C}) : f \text{ is defined at } P \}.$$

It can also be defined as a localization $A_{\mathfrak{m}}$ where A is the affine coordinate ring of an affine patch of $\overline{C}$ containing P, and $\mathfrak{m}$ is the maximal ideal that corresponds to P: $\mathfrak{m} = \{ f \in A : f(P) = 0 \}$.

<u>Fact</u>: there's a discrete valuation $v_P = \operatorname{ord}_P : \overline{K}(C) \twoheadrightarrow \mathbb{Z} \cup \{\infty\}$ such that $\mathcal{O}_{\overline{C},P} = \{ f \in \overline{K}(C) : v_P(f) \geq 0 \}$. It is called the <u>order</u> of f at P.

<u>Def</u>: An element of valuation 1, $t \in \overline{K}(C)$ is called <u>a uniformizer at P</u>.

<u>Example</u>: Suppose P is a (smooth) point in ~~$\overline{C}$~~, $P = (a,b)$ in an affine patch of C defined by $f(x,y) = 0$ in $\mathbb{A}^2$.
Since C is smooth, either $\frac{\partial f}{\partial x}(P) \neq 0$ or $\frac{\partial f}{\partial y}(P) \neq 0$.
In the first case, for instance, it means that C is not horizontal at P (its tangent line) and $y - b$ will be a uniformizer.
(in the second case we'd had taken $x - a$).

Suppose $\phi: C_1 \to C_2$ is a non-constant morphism of curves.
Suppose $\phi(Q) = P$.
Then $v_Q \big|_{\bar{K}(C_2)} = e \cdot v_P$ for some $e = e_\phi(Q) = e_{Q/P} \in \mathbb{Z}_{\geq 1}$

e is called the ramification index of ϕ at Q.

ϕ is called <u>étale</u> (unramified) at $Q \Leftrightarrow e_\phi(Q) = 1$.
ϕ is étale if $e_\phi(Q) = 1 \quad \forall Q \in C_1(\bar{k})$.

<u>Divisors</u>

Def: A <u>divisor</u> on $\bar{C}$ is a formal sum $\sum_{P \in C(\bar{k})} n_P P$ | with $n_p \in \mathbb{Z}$, $n_p = 0$ for all but finite amount of P's.

$\mathrm{Div}(\bar{C}) := \{\text{divisors on } \bar{C}\}$ is the free abelian group generated by all the divisors.
(the set $C(\bar{k})$ is a basis over $\mathbb{Z}$).

A <u>divisor</u> on C is a formal $\mathbb{Z}$-linear combination of irreducible 0-dimensional k-subvarieties of C.
(such a $\mathfrak{P}$ has the form $\bigcup_{\sigma \in G} {}^\sigma P$ for some $P \in C(\bar{k})$. We call them "closed points").

$$\begin{array}{ccc} \mathrm{Div}(C) & \hookrightarrow & \mathrm{Div}(\bar{C}) \\ \mathfrak{P} & \longmapsto & P_1 + \cdots + P_n \\ \| & & \\ \{P_1, \ldots, P_n\} & & \end{array}$$

So $\boxed{\mathrm{Div}(C) = \mathrm{Div}(\bar{C})^G}$

If $D_1 = \sum n_P P$, $D_2 = \sum m_P P$ then we will say

$D_1 \geq D_2$ iff $n_P \geq m_P$ $\forall P$.

The divisors D satisfying $D \geq 0$ are called <u>effective</u>.

Suppose $f \in \bar{k}(C)^*$.

Def: the <u>divisor of f</u> $\operatorname{div}(f) = (f) := \sum_{P \in C(\bar{k})} v_P(f) P \in \operatorname{Div}(\bar{C})$ one has to prove that a rational function has finitely many zeros and poles

If $f \in k(C)^*$ then $(f) \in \operatorname{Div}(C)$ (easy).

A divisor "coming" from $f \in \bar{k}(C)^*$ is called <u>principal</u>.

We have these exact sequences: by definition, the Picard group (= divisor class group)

$$\begin{tikzcd}
0 \arrow[r] & k^* \arrow[r] \arrow[d, hook] & k(C)^* \arrow[r] \arrow[d, hook] & \operatorname{Div}(C) \arrow[r] \arrow[d, hook] & \operatorname{Pic}(C) \arrow[r] \arrow[d, hook] & 0 \\
0 \arrow[r] & \bar{k}^* \arrow[r] & \bar{k}(C)^* \arrow[r] & \operatorname{Div}(\bar{C}) \arrow[r] & \operatorname{Pic}(\bar{C}) \arrow[r] & 0
\end{tikzcd}$$

fact: it is injective (need th 90 Hilbert).

<u>Warning</u>: there's an injective map from $\operatorname{Pic}(C) \hookrightarrow \operatorname{Pic}(\bar{C})$, but it is <u>not</u> true that $\operatorname{Pic}(C) = \operatorname{Pic}(\bar{C})^G$!!

In fact, $\operatorname{Pic}(C) \subseteq \operatorname{Pic}(\bar{C})^G$.

There's a map $\operatorname{Div}(\bar{C}) \xrightarrow{\deg} \mathbb{Z}$.

$$\sum n_P P \longmapsto \sum n_P$$

$\operatorname{Div}^0(\bar{C})$ is defined as the kernel of this map.

$\operatorname{Div}^0(C)$ is the kernel of $\deg|_{\operatorname{Div}(C)}$.

<u>Fact</u>: If $D = (f)$ for some $f \in \bar{k}(C)$, then $\deg D = 0$.

(so functions have the same # of zeros and poles).

We also get $\deg : \operatorname{Pic}(\bar{C}) \twoheadrightarrow \mathbb{Z}$ and so we can define

$\operatorname{Pic}(C) \longrightarrow \mathbb{Z}$

$\operatorname{Pic}^0(C)$ and $\operatorname{Pic}^0(\bar{C})$

Example : $C = \mathbb{P}^1_{\mathbb{C}}$

$\mathbb{P}^1(\mathbb{C}) = \mathbb{A}^1(\mathbb{C}) \cup \{\infty\}$. where $\mathbb{A}^1 = \operatorname{Spec} \mathbb{C}[t]$, $t = \frac{X_0}{X_1}$ in terms of homogeneous coordinates $[X_0, X_1]$ on $\mathbb{P}^1$,

Any $f \in \mathbb{C}(\mathbb{P}^1)^*$ has the form $c \cdot \prod_{\alpha \in \mathbb{C}} (t-\alpha)^{n_\alpha}$, $n_\alpha \in \mathbb{Z}$. and finitely many non-zero n_α.

Then $(f) = \sum_{\alpha \in \mathbb{C}} n_\alpha (\alpha) + n_\infty (\infty)$ where n_∞ is such that $\sum_{\alpha \in \mathbb{C}} n_\alpha + n_\infty = 0$.

Thus

$$\mathbb{C}(\mathbb{P}^1)^* \longrightarrow \operatorname{Div}(\mathbb{P}^1) \xrightarrow{\deg} \mathbb{Z} \to 0 \quad \text{is exact.}$$

Therefore, $\operatorname{Pic}(\mathbb{P}^1) \xrightarrow[\sim]{\deg} \mathbb{Z}$ <u>is an isomorphism.</u>

Example: $C : x^2+y^2+z^2=0$ in $\mathbb{P}^2_{\mathbb{R}}$; $G = \operatorname{Gal}(\mathbb{C}/\mathbb{R})$

Since $C(\mathbb{R})$ is empty, every point in $C(\mathbb{C})$ has a G-orbit of size 2.

This means that the image of $\deg : \operatorname{Div}(C) \to \mathbb{Z}$ is $2\mathbb{Z}$. (also $\deg : \operatorname{Pic}(C) \to \mathbb{Z}$).

But over $\mathbb{C}$,

$C_{\mathbb{C}}$, $x^2+y^2+1=0$ (dehomogenization).

Making a change of variables, we can see that is birational to $x^2+y^2=1$, which is birational to $\mathbb{P}^1$ (stereographic projection). So $C_{\mathbb{C}} \simeq \mathbb{P}^1_{\mathbb{C}}$.

By the previous example, $\operatorname{Pic}(C_{\mathbb{C}}) \xrightarrow[\sim]{\deg} \mathbb{Z}$, so $\operatorname{Pic}(C_{\mathbb{C}})^G = \mathbb{Z}$.

$\operatorname{Pic}(C) = 2\mathbb{Z}$

<u>Differentials.</u>

<u>Def</u> Ω_C is called the space of meromorphic differentials on a curve C.

$$\Omega_C := \frac{k(C)\text{-vector space with basis } \{\overset{\text{symbol}}{dx} : x \in k(C)\}}{\left\langle \begin{array}{ll} \text{relations } d(x_1+x_2) = dx_1 + dx_2 & \text{for } x_1, x_2 \in k(C) \\ d(x_1 x_2) = x_1\, dx_2 + x_2\, dx_1 & a \in k \\ da = 0 & \end{array} \right\rangle}$$

<u>Fact</u>: Ω_C is a 1-dimensional vector space over $k(C)$.

<u>Def</u> (order of a differential at a point).

Given $P \in C(\bar{k})$, $\omega \in \Omega_C$, choose $t \in k(C)$ a uniformizer at P.

It turns out that $dt \neq 0$ in Ω_C, so

$\omega = f\, dt$ for some $f \in k(C)$

We will define $v_P(\omega) := v_P(f)$.

<u>Def</u> (divisor of a differential): If $\omega \neq 0$, $(\omega) := \sum_{P \in C(\bar{k})} v_P(\omega) P \overset{\text{fact}}{\in} \operatorname{Div}(C)$.

Any divisor of this type is called $\boxed{a}$ <u>canonical divisor</u>.

If $\tilde{\omega}$ is another nonzero element of Ω_C, then

$\tilde{\omega} = f\omega$ for some $f \in k(C)^*$, so

$(\tilde{\omega}) = (f) + (\omega)$, or also $(\tilde{\omega}) \equiv (\omega)$ in $\operatorname{Pic}(C)$.

So there's a well defined element in $\operatorname{Pic}(C)$.

<u>Def</u>: The <u>canonical class</u> in $\operatorname{Pic}(C)$ is $[(\omega)]$ for any $\omega \in \Omega_C$.

<u>Def</u> If $\omega = 0$ or $(\omega) \geq 0$, then ω is called <u>regular</u> (or holomorphic) (i.e. has no poles)

Riemann-Roch

Def If $D \in \mathrm{Div}(C)$, define a k-vector space

$$L(D) := \{ f \in k(C)^* : (f) \geq -D \} \cup \{0\}.$$

(e.g. $L(3P - 2Q)$ is the space of rational functions on $\mathbb{C}$ with at most a pole of order 3 at P, and a double zero (at least) at Q.)

Fact: if we used the same D, but took $f \in \bar{k}(C)^*$ instead of $f \in k(C)^*$, we would have got the

$\bar{k}$-vector space with the same basis as the k-basis for the original k-vector space $L(D)$.

(the proof is a generalization of H90 for GL_n).

Def: $\ell(D) := \dim_k L(D)$

Fact: $\ell(D) < \infty$

Remark: if $D' = D + (h)$ for some $h \in k(C)^*$, then.

$$L(D') = h^{-1} L(D) \qquad \text{so} \qquad \ell(D) = \ell(D')$$

Example: If $\deg(D) < 0$, then $L(D) = \{0\}$, because $\deg((f)) = 0$, and $\ell(D) = 0$.

Def: The genus of C is $g := \ell(K)$ where K is any canonical divisor.

Then $g = \dim_k \{ \omega \in \Omega_C : \omega \text{ is regular everywhere} \}$.

Fact: if $k = \mathbb{C}$, then $g =$ the topological genus of the compact Riemann surface $C(\mathbb{C})$. (number of holes)

Th (Riemann-Roch):

$$\ell(D) - \ell(K-D) = \deg D - g + 1$$

<u>Consequences</u>:

- $\deg K = 2g-2$ (taking $D=K$, $\ell(0)=1$).
- If $\deg D > 2g-2$, $\ell(D) = \deg D - g + 1$
- If $\deg D \geq 2g+1$ and $f_1, \dots, f_m$ is a basis for $L(D)$, then the rational map

$$\begin{aligned} C &\longrightarrow \mathbb{P}^{m-1} \\ P &\longmapsto (f_1(P) : \cdots : f_m(P)) \end{aligned}$$

is a morphism mapping C isomorphically to its image.

<u>Hurwitz's theorem</u>

$$\begin{array}{c} X \\ f \big\downarrow \\ Y \end{array}$$

separable morphism of curves.

~~For~~ $P \in X(\bar{k})$, let e_P be the ramification index of f at P.

Then,

$$2g_X - 2 = \underbrace{(\deg f)}_{[k(X):k(Y)]}(2g_Y - 2) + \deg \underbrace{R}_{\text{ramification divisor}}$$

and $R = \sum_{P \in X(\bar{k})} (e_P - 1) P$ if $\underbrace{\text{no } e_P \text{ is divisible by char } K}_{\boxed{\text{tame ramification}}}$

almost all e_P are 1

Galois cohomology (H^0, H^1): math.berkeley.edu/~poonen/f01/weakmw.pdf

Let G be a profinite group (i.e. topological group isomorphic to an inverse limit of finite groups)

Example: if K is a perfect field,

$$G_K = Gal(\bar{K}/K) = \varprojlim_{L/K \text{ finite galois}} Gal(L/K)$$

Let A be a discrete, left G-module. This means that A is an abelian group acting on G and the map

$G \times A \longrightarrow A$ is continuous, considering A with discrete topology.

(think finite, it's easier.).

Def $A^G = H^0(G, A) := \{ a \in A : ga = a \ \ \forall g \in G \}$.

Example:

K a number field, $G = G_K$, let E be an elliptic curve $/K$.

Then $E(\bar{K})$ is a G_K-module (acting on the coordinates of each point).

Then $H^0(K, E) := H^0(G_K, E(\bar{K})) = E(K)$

Remark: Suppose that $0 \to A \to B \to C \to 0$ is an exact sequence of G-modules (exact sequence that commutes with action by G)

Then $0 \to A^G \to B^G \to C^G$ is exact, by the last map may NOT be surjective.

Theorem 1: There exists a collection of functors $H^i(G, -)$ $i \geq 0$ s.t. for each exact sequence of G-modules $0 \to A \to B \to C \to 0$, there's a long exact sequence

$0 \to H^0(G, A) \to H^0(G,B) \to H^0(G, C) \to H^1(G, A) \to H^1(G, B) \to H^1(G, C) \to \cdots$

which is functorial with respect to the input exact sequence: given a morphism of exact sequences, $f^*(A, B, C)$, there exists a morphism of the long exact sequence.

How to compute the $H^i(G,-)$?

One way is by defining $H^i(G,A)$ via i-cochains, i-cocycles, i-coboundaries, and then to set $H^i(G,A) = \{i\text{-cocycles}\}/\{i\text{-coboundaries}\}$

For instance,

A 1-cocycle is a continuous function $\xi: G \to A$, $g \mapsto \xi_g$ such that

$$\xi_{gh} = \xi_g + g\xi_h \quad \forall g,h \in G.$$

A 1-coboundary is a continuous functions $G \to A$ of the form $g \mapsto ga - a$ for some $a \in A$.

To understand how to build the other H^i, we need some more abstraction.

Need to see pdf and check the references. (projective resolution construction).

Special case: if G acts trivially on A, then $H^1(G,A) = \mathrm{Hom}_{\mathrm{conts}}(G,A)$

Pf: a 1-cocycle is a homomorphism $G \to A$ (i.e. $\xi_{gh} = \xi_g + \xi_h$).
a 1-coboundary is only the zero homomorphism. //.

Facts: • If G is any profinite group, and A is any G-module, and $i > 0$, then $H^i(G,A)$ is a torsion abelian group (can be $\mathbb{Q}/\mathbb{Z}$ i.e. each element has finite order).
• (Hilbert's Th. 90): if K is a perfect field, $H^1(G_K, \bar{K}^*) = 0$

Exercise: Use H90 to prove that if m is an integer not divisible by the characteristic of K, then if $\mu_m = \{x \in \bar{K}^* : x^m = 1\}$ then

$$H^1(G_K, \mu_m) \simeq K^*/K^{*m}$$

Restriction.

If $H \subseteq G$ is a closed subgroup and A is a G-module, then A can be considered also as an H-module, and then there exist restriction homomorphisms $H^i(G,A) \to H^i(H,A)$ $\forall i \geq 0$

Examples: On H^0: $A^G \hookrightarrow A^H$

On H^1: $[\xi] \longmapsto [\xi|_H]$ (exercise: prove it is all well defined).

Example: Let k be a # field, let k_v be the completion of k at a place v.

If we identify $\bar{k} \hookrightarrow \bar{k}_v$, then we have an injection of groups

$$G_v := Gal(\bar{k}_v/k_v) \hookrightarrow G_k := Gal(\bar{k}/k)$$
$$\sigma \longmapsto \sigma|_{\bar{k}}$$

Suppose E is an elliptic curve over k.

using H^1 functoriality and inclusion $E(\bar{k}) \hookrightarrow E(\bar{k}_v)$

$$H^1(k,E) := H^1(G_k, E(\bar{k})) \xrightarrow{Res} H^1(G_v, E(\bar{k})) \to H^1(G_v, E(\bar{k}_v)) = H^1(k_v, E)$$

The composition is called Res_v.

We are interested on H^0 because for instance H^1 classifies twists of some objects over a field.

Example: Let k be a perfect field, let V be an k-object over k. (for instance, a variety equipped with some extra structure).

We assume that k-objects form a category, and that there's a notion of base extension (given a k-object and a field extension $L \supset k$, then there's an associated L-object, called V_L).

Then a twist (or k-form) of V is a k-object W s.t there exist an isomorphism (preserving the structure of) ~~from~~ $W_{\bar{k}} \xrightarrow{\sim} V_{\bar{k}}$.

Then, there's an injection (fixed V). may not be abelian: but we can extend H^1 in some way (then we lose the fact that it is a group).

$$\{\text{twists of } V\}/_{k\text{-isom}} \hookrightarrow H^1(G_k, \mathrm{Aut}(V_{\bar{k}}))$$

that in many situations is a bijection.

This injection is defined as follows:

Suppose W is a twist of V. Fix an isomorphism $\phi : W_{\bar{k}} \xrightarrow{\sim} V_{\bar{k}}$. Then, for $g \in G_k$, we can apply g to ϕ to obtain a new isomorphism ${}^g\phi : W_{\bar{k}} \xrightarrow{\sim} V_{\bar{k}}$

Then $\left[g \mapsto {}^g\phi \cdot \phi^{-1} \in \mathrm{Aut}(V_{\bar{k}}) \right]$ is a 1-cocycle, representing a class in $H^1(G_k, \mathrm{Aut}(V_{\bar{k}}))$. (excercice: all is well defined).

<u>Torsors</u> (principal homogeneous spaces):

Let G be a (commutative) algebraic group over a perfect field k.
(i.e. a variety equipped with a group structure

$$\left\{ \begin{array}{l} G \times G \xrightarrow{m} G \\ G \xrightarrow{i} G \\ \underset{\text{point}}{\mathrm{spec}\, k} \xrightarrow{e} G \end{array} \right\} \quad \text{satisfying the group actions.}$$)

Let $\underline{G}$ denote G equipped with the additional structure of a G-action

$$G \times \underline{G} \longrightarrow \underline{G} \quad \text{given by the group multiplication.}$$

Def. A <u>homogeneous space</u> of G over k is a k-variety X, equipped with a transitive action of G. (i.e a morphism

$$G \times X \to X$$ which gives a transitive action of $G(\bar{k})$ on the set $X(\bar{k})$).

Such an X is a <u>principal hom. space (torsor)</u> if

$$\forall x_1, x_2 \in X(\bar{k}),\ \exists !\, g \in G(\bar{k}) \text{ s.t. } g x_1 = x_2$$

and we'll say $\underline{G}$ is a torsor under G.

Analogy between number fields and function fields.

There's an extensive analogy, which is specially good if k is finite.

Number field object	Function field analogue.
$\mathbb{Z}$	$k[t]$ (assume k is perfect)
$\mathbb{Q}$	$k(t)$
$\mathbb{Q}_p$	$k((t))$
number field K	finite extension $K \supset k(t)$ (equivalently, field that is finitely generated over k, of tr. degree 1) ← WLOG (analogy) we can assume K = function field of some curve X/k.
$\operatorname{Spec} \mathbb{Z}$	$\operatorname{Spec} k[t] = \mathbb{A}^1$
$\operatorname{Spec} \mathcal{O}_K$ + infinite primes (Arakelov theory).	X projective variety
places (= absolute values)	$\mathrm{Gal}(\bar{k}/k)$ - conjugacy classes of points in $X(\bar{k})$

Let S be a finite set of places, containing all archimedean ones.

$\mathcal{O}_{K,S}$ (ring of S-integers)	$\mathcal{O}_{K,S} := \{f \in K : v(f) \geq 0 \text{ outside } S\} =$ = ring of regular functions of the curve $\underbrace{X - S}_{\text{affine curve if } S \neq \emptyset}$ $= \begin{cases} k & \text{if } S = \emptyset \\ \text{some Dedekind ring with fraction field } K & \text{if } S \neq \emptyset \end{cases}$
Dirichlet Unit Theorem $\left(\mathcal{O}_{K,S}^* \cong \mathbb{Z}^{\#S-1} \times \mathbb{Z}/\underset{\substack{\# \text{ roots} \\ \text{of } 1 \text{ in } K}}{w}\mathbb{Z}\right)$	⇝ (if $S \neq \emptyset$) (and k is finite) $\mathcal{O}_{K,S}^* \cong \mathbb{Z}^{\#S-1} \times k^*$
fractional ideal $\prod \mathfrak{p}^{n_p}$	→ divisor $\sum n_P P$
principal ideal (α)	→ principal divisor (f)
class group (finite)	$\mathrm{Pic}\, X$. When k is finite $0 \to \mathrm{Pic}^0 X \to \mathrm{Pic}\, X \xrightarrow{\deg} \mathbb{Z} \to 0$, $\mathrm{Pic}^0 X = J(k)$ finite set.

Twists of $\underline{G}$ as a torsor under G:

By definition,

$$\left\{\begin{array}{l}\text{twists of } \underline{G} \text{ as a torsor} \\ \text{under } G\end{array}\right\} = \{\text{torsors under } G\}.$$

$$\| \qquad\qquad \updownarrow$$

$$H^1(G_k, \mathrm{Aut}(\underline{G}_{\bar{k}}))$$

i.e. an element of $\mathrm{Aut}(\underline{G}_{\bar{k}})$ is an $\bar{k}$-morphism $\underline{G}_{\bar{k}} \longrightarrow \underline{G}_{\bar{k}}$ respecting the structure of $\underline{G}$, i.e. if $0 \mapsto b$, then $a \mapsto a+b$

So they are only the translation maps $\cong G(\bar{k})$

So we can write $H^1(k, G) = \{\text{torsors under } G\}$.

Then, the following are equivalent, for a torsor X under G:

1) $X \simeq \underline{G}$ as a torsor

2) $X(k)$ is nonempty

3) X corresponds to 0 in $H^1(k, G)$.

Going on with the analogy btw Num. fields and Function fields:

Number field object		Function field analogue.
$\prod \mathfrak{p}^{n_\mathfrak{p}}$ (fractional ideal)		$\sum n_P P$ (divisor)
$L \supseteq K$ extension of # fields	$\longleftrightarrow$	<u>nonconstant</u> morphisms of curves $f: X \longrightarrow Y$ (so $f^*k(Y) \subseteq k(X)$) <u>surjective on $\bar{k}$-points</u> $\Leftrightarrow$ <u>dominant</u>
Extension of ideals: $\mathfrak{a} \longmapsto \mathfrak{a}\mathcal{O}_L$ $\mathfrak{p} \longmapsto \prod_{\mathfrak{q} \mid \mathfrak{p}} \mathfrak{q}^{e_\mathfrak{q}}$	$\longleftrightarrow$	pull-back of divisors: $f^*: \mathrm{Div}\, Y \longrightarrow \mathrm{Div}\, X$ (over $k=\bar{k}$) $P \longmapsto \sum_{Q \text{ s.t. } f(Q)=P} e_Q Q$
Norm of ideals $N(\mathfrak{q}) = \mathfrak{p}^f$	$\longleftrightarrow$	Push-forward of divisors $f_*: \mathrm{Div}\, X \longrightarrow \mathrm{Div}\, Y$ ($k=\bar{k}$) $P \longmapsto f(P)$
Absolute discriminant $\Delta_{K/\mathbb{Q}}$	$\longleftrightarrow$	if $k = \mathbb{F}_q$, can take q^{g-1} (genus of the curve) (reason: to do this..)
(relative) different	$\longleftrightarrow$	ramification divisor (see Hurwitz formula, i.e. $2g_X - 2 = d(2g_Y - 2) + \deg R$)
Estimate for the number of points in adelic parallelotopes (cf Lang)	$\longleftarrow$	Riemann-Roch theorem
Functional equation for $\zeta(s)$, Riemann-Hypothesis generalization to number fields	$\longleftrightarrow$	Weil conjectures (all proven)

Remember from first lecture:

Fact: $D \in \mathrm{Div}(X)$. If $\deg D \geq 2g+1$, and $f_0, \dots, f_n$ is a basis for $\mathcal{L}(D)$ (so $n = \deg D - g$ by R-R).

Then $X \longrightarrow \mathbb{P}^n$ is a morphism, that maps X isomorphically to its image.
$P \longmapsto (f_0(P) : \cdots : f_n(P))$

We'll call the image of X as X'.

Also, $\deg X' = \deg D$, where.

Def The degree of a curve embedded in $\mathbb{P}^n$, $X \hookrightarrow \mathbb{P}^n$, means $\#(H \cap X')$ (finite) number of points, with multiplicity.
for any hyperplane $H \subseteq \mathbb{P}^n$ not containing all of X'.

Genus 0 curves

Theorem: Let X be a genus-0 curve.

1) Then X is isomorphic to a conic (i.e. a smooth plane (in $\mathbb{P}^2$) curve of degree 2)
2) Moreover, if X has a k-point, then $X \cong \mathbb{P}^1_k$
3) If k is a global field $\left(\begin{matrix}[k:\mathbb{Q}] < \infty \\ \text{or} \\ [k : \mathbb{F}_p(t)] < \infty\end{matrix}\right)$ then

X has a k-point $\Leftrightarrow$ X has a k_v-point for all places v of k.

(Hasse principle for genus 0 curves).

Pf

1) $\deg K = 2g-2 = -2$

Take $D = -K$ (have $\deg D = 2 \geq 2g-1$), so a basis of $\mathcal{L}(D)$ gives an embedding $X \hookrightarrow \mathbb{P}^{2 = \deg D - g = \deg D - 0}$, and the image X' has degree 2, also. So X is $f(x,y,z) = 0$ for some f homogeneous of degree 2.

2) Take P the k-point. Define $D := P$, it is a degree-1 divisor, so the fact implies that ~~these sets~~, taking a basis $\{1, f\}$ of $\mathcal{L}(D)$ defines an embedding $X \hookrightarrow \mathbb{P}^1$ but $\mathbb{P}^1$ is also a curve, and so $X \cong \mathbb{P}^1$.

(3) It's a special case of the Hasse-Minkowski theorem for quadratic forms, thanks to part 1. //

Remark: If char $k \neq 2$, and X is a genus-0 curve over k, one can perform a linear change of variables ("complete the square repeatedly"), to show that $X \simeq$ a curve $\alpha X^2 + \beta Y^2 + \gamma Z^2 = 0$ in $\mathbb{P}^2$ (all non-zero) otherwise, wouldn't be smooth! $\alpha, \beta, \gamma \in k$
which is isomorphic also to a curve

$x^2 - a y^2 - b z^2 = 0$, $a, b \in k^*$ ~~for k~~

For k global,

X has a k_v-point $\iff (a,b)_v = +1$ ← Hilbert symbol.

The Hilbert symbol (we can define it as because of this property), can be defined in terms of the quaternion algebra $k \oplus k_i \oplus k_j \oplus k_{ij}$ with $i^2 = a$, $j^2 = b$, $ij = -ji$
and it is $+1$ iff it is isomorphic as k-algebra to $M_2(k)$.

Hyperelliptic curves

Def: A <u>hyperelliptic curve</u> over k is a curve X (of genus $g \geq 2$) that has a separable degree-2 map π to a genus 0 curve Y.

Want to know what does X look like in terms of ~~explicit~~ equations.

- Let's assume that Y has a k-point. Then $Y \simeq \mathbb{P}^1_k$

$$k(Y) \overset{\text{def}}{=} \mathrm{Frac}\Big(\underbrace{k[x]}_{\text{coordinate ring of one of the affine patches}}\Big) = k(x)$$

$k(X)$ is a separable degree-2 extension of $k(Y) = k(x)$

Assume char $k \neq 2$ (otherwise use Artin-Schreier theory). Then, (by Kummer theory), $k(X) = k(x)(\sqrt{f})$ for $f \in k(x)$

WLOG (since $k[x]$ is a UFD) we may assume f is a squarefree <u>polynomial</u>.

Then $k(X) = \mathrm{Frac}\left(\dfrac{k[x,y]}{(y^2 - f(x))}\right) =$ function field of the affine curve $y^2 = f(x)$ in $\mathbb{A}^2_k$.

So X is the smooth projective model of $y^2=f(x)$

<u>Claim</u>: $y^2=f(x)$ is smooth

Pf. The partial derivatives $2y$, $f'(x)$ do not vanish simultaneously on $y^2=f(x)$.

because f is squarefree and K is perfect ($\gcd(f,f')=1$).

We can ask if X is then the projective closure of $y^2=f(x)$.

(i.e. is the projective closure smooth?). The answer is <u>NO</u>:

$$y^2z^{n-2}=F(x,z) \quad \text{in } \mathbb{P}^2$$ where $n=\deg f$, F is the homogenization of f.

(assume $\underline{n\geq 2}$)

The only points we have to check are the ones for which $\overbrace{z=0}^{\text{line at infinity}}$ (the others have already been checked. Its

The only such point is (if $\underline{n\geq 3}$) $(0:1:0)=P$

Dehomogenize by setting $y=1$ (so that P is on the affine patch, and in fact corresponds to the origin in this patch:

$$z^{n-2}=F(x,z).$$

If $\underline{n\geq 4}$ then $(0,0)$ is singular (since there are no monomials of degree ≤ 1).

Correct approach: (for constructing the smooth projective model). (assume $\deg f\geq 4$)

Choose $g\in\mathbb{Z}_{>0}$ s.t. $\deg f=2g+1$ or $2g+2$.

(eventually we'll prove that g is the genus of X, but we don't know that, yet).

Let $F(x,z):=z^{2g+2}f\left(\frac{x}{z}\right)$. Will be a homogeneous polynomial of degree $2g+2$ (even!)

Consider $Y^2=F(X,Z)$ in a weighted projective space with $\begin{pmatrix} wt(X)=1 \\ wt(Y)=g+1 \\ wt(Z)=1 \end{pmatrix}$

More concretely, we can describe

$$\begin{array}{c} X \\ \downarrow \\ \mathbb{A}^1_0\cup\mathbb{A}^1_\infty=\mathbb{P}^1 \end{array}$$

So we can describe the parts of X lying above the affine patches of $\mathbb{P}^1$.

We already have one of the patches: $\begin{array}{c} y^2=f(x) \text{ in } \mathbb{A}^2 \\ \downarrow \\ \mathbb{A}^1 \end{array}$

The other patch should be birational to this one.

Rewrite the equation $y^2 = f(x)$: ↙ is a polynomial, as f has degree $\leq 2g+2$

$$\frac{y^2}{x^{2g+2}} = \frac{f(x)}{x^{2g+2}} \underset{\substack{X=\frac{1}{x} \\ Y=\frac{y}{x^{g+1}}}}{\rightsquigarrow} Y^2 = X^{2g+2} f\left(\frac{1}{X}\right) = f^{rev}(X) \qquad \left(\begin{array}{l} f(x) = x^5+2x+3 \\ f^{rev}(X) = 3X^6+2X^5+X \end{array}\right)$$

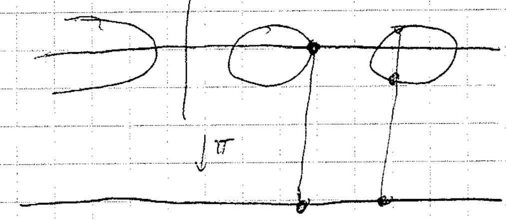
Can check that $f^{rev}(X)$ is squarefree so this other patch is smooth.

X is obtained by "gluing" the two patches, identifying the $\{x \neq 0\}$ of patch one with $\{X \neq 0\}$ of patch 2 with the relations $\left\{ \begin{array}{l} X = 1/x \\ Y = \frac{y}{x^{g-1}} \end{array} \right\}$

Prop: The genus of X is g (defined so that $\deg f = 2g+1$ or $2g+2$).

Pf: Apply Hurwitz formula to the degree-2 separable map

$$\begin{array}{c} X \\ \downarrow \pi \\ \mathbb{P}^1 \end{array}$$ over $\bar{k}$ (the genus doesn't change if we consider $\bar{k}$ instead of k).



For each point $P \in \mathbb{P}^1(\bar{k})$, there are either two points Q with $e_Q = 1$, or there is one point Q with $e_Q = 2$.

So ~~all~~ the ramification is tame (char $k \neq 2$) and so $R = \sum_{P \in X(\bar{k})} (e_P - 1) P$

$$\deg R = \sum_{Q \in X(\bar{k})} (e_Q - 1) = \# Q\text{'s with } e_Q = 2 = \begin{cases} \deg f + 1 & \text{if } f^{rev}(0) = 0 \ (\Leftrightarrow \deg f = 2g+1) \\ \deg f & \text{if } f^{rev}(0) \neq 0 \ (\Leftrightarrow \deg f = 2g+2) \end{cases}$$

So $\deg R = 2g+2$.

Hurwitz says $2g_X - 2 = 2(2g_{\mathbb{P}^1} - 2) + (2g+2) = 2\cdot(0-2) + 2g+2 = 2g-2 \Rightarrow$

$\Rightarrow g_X = g$. //

Prop: $\frac{dx}{y}, x\frac{dx}{y}, \dots, x^{g-1}\frac{dx}{y}$ is a k-basis for the (g-dimensional) space of regular differentials on X.

Let $K = \mathrm{div}\left(\frac{dx}{y}\right)$

Remember $\mathcal{L}(K) = \{ f \in k(X)^* : \mathrm{div}(f) + K \geq 0 \} \cup \{0\} = \langle 1, x, \ldots, x^{g-1} \rangle$

We will call the <u>canonical map</u>:

$$|K| : X \longrightarrow \mathbb{P}^{g-1}$$
$$P \longmapsto (1 : x(P) : x(P)^2 : \cdots x(P)^{g-1})$$

This is a 2-to-1 map onto its image, which is $\simeq \mathbb{P}^1$.

Calculating genus: some facts

- Plane curves:

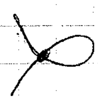
Let $f(x,y,z)$ be a geometrically irreducible homogeneous poly'l in 3 variables of degree d.

Let X be ~~the smooth projective model of~~ $\{f(x,y,z) = 0\} \subseteq \mathbb{P}^2$.

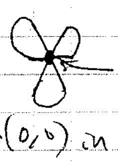
a) If X is smooth, then its genus is
$$\frac{(d-1)(d-2)}{2}$$

b) In general, if g is the genus of the smooth projective model of X,
$$g = \frac{(d-1)(d-2)}{2} - \sum_{\substack{\text{singularities} \\ P \in X(\bar{k})}} \delta_P$$
where $\delta_P \geq 1$ measures "how bad" the singularity is.

Examples:

 node $(xy + x^3 + y^3)$ $\quad \delta_P = 1$

 cusp $(y^2 - x^3)$ $\quad \delta_P = 1$

 $\delta_P = 3$.

If $P = (0,0)$ in $\mathbb{P}^2$ and X is given by $\underbrace{g_m(x,y)}_{\text{homogeneous of degree } m} + g_{m+1}(x,y) + \cdots = 0$ and g_m factors over $\bar{k}$ into distinct linear factors, then $\delta_P = \binom{m}{2}$.

(See Hartshorne).

• Let X be the smooth, projective model of

$$\Big(\underbrace{\sum a_{ij} X^i Y^j}_{f(x,y)} = 0 \quad \text{in } \mathbb{A}^2 \Big)$$

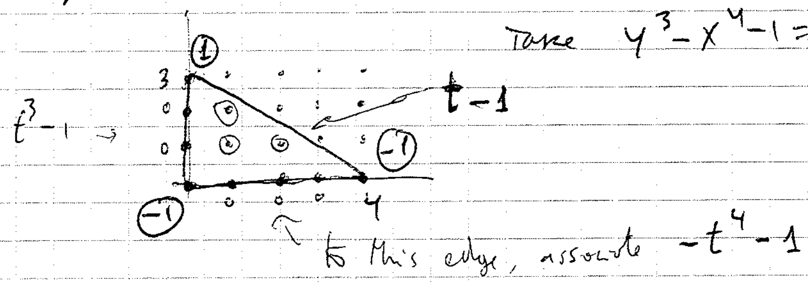
Form the Newton polygon $P :=$ convex hull ~~of~~ $\mathbb{R}^2$ of $\{(i,j) \in \mathbb{Z}^2 : a_{ij} \neq 0\}$

Then
$g = \#$ interior lattice points of P

if no point (a,b) with $a \neq 0, b \neq 0$ is singular on $\{f=0\}$, and ~~the~~ 1-variable polynomial corresponding each edge is squarefree.

Example: $y^3 = x^4 + 1$ over $\mathbb{Q}$:

Take $y^3 - x^4 - 1 = 0$



Moreover, if it satisfies such conditions, the differentials

$$\text{"} x^i y^j \frac{dx}{x} \frac{dy}{y} \frac{1}{df} \text{"} := x^{i-1} y^{j-1} \frac{dx}{\partial f / \partial y} \qquad \text{for interior lattice points } (i,j)$$

form a basis for the regular differentials on X.

Now we go to a different problem. Instead of finding the genus of a curve, let's find all the curves with a given genus.

Describing all curves of a given genus.

Over $k=\bar{k}$.

$g=0$: only $\mathbb{P}^1$ (they have a rational point ($k=\bar{k}$) so they are isomorphic to $\mathbb{P}^1$).

$g=1$: one elliptic curve for each $j \in k$ (j-invariant).

any g: there exists an irreducible quasi-projective variety $\mathcal{M}_g$ (the coarse moduli space of curves of genus g) and a natural bijection

$$\left\{ \begin{matrix} \text{curve of genus} \\ g \text{ over } k \end{matrix} \right\} \Big/ \cong \quad \longleftrightarrow \quad \mathcal{M}_g(k).$$

($\mathcal{M}_0 = \text{point}$; $\mathcal{M}_1 = \mathbb{A}^1$; $\dim \mathcal{M}_g = 3g-3$ $(g\geq 2)$).

When g is large $\mathcal{M}_g$ is not birational to $\mathbb{A}^{3g-3}$

Over k perfect.

$g=0$: conics

$g=1$: elliptic curves and their ppl homogeneous spaces. ((complicated)).

General fact: for $g\geq 2$,

If X is not hyperelliptic (this case has already been covered before), then the canonical map $X \longrightarrow \mathbb{P}^{g-1}$ given by a basis of $L(K)$ (K canonical divisor) embeds X as a degree $2g-2$ in $\mathbb{P}^{g-1}$.

$g=2$: The canonical map $X \longrightarrow \mathbb{P}^1$ cannot be an embedding (because $X \not\cong \mathbb{P}^1$).

so X is hyperelliptic and in fact the canonical map is the degree-2 map, to a genus 0 curve.

If char $k \neq 2$, X is the smooth proj model of $y^2 = f(x)$, where f is a squarefree polynomial of degree 5 or 6.

Exercise: For any hyperelliptic curve of even genus, the underlying genus 0 curve is isomorphic to $\mathbb{P}^1_k$.

$\underline{g=3}$: • Hyperelliptic curves:

(char $k \neq 2$) $\rightarrow y^2 = f(x)$ $\quad f$ squarefree of degree 7 or 8

or $\rightarrow$ double cover of a nontrivial conic ramified above 8 $\bar{k}$-points. (Hurwitz's formula.)

• Non-hyperelliptic curves:

$X \hookrightarrow \mathbb{P}^2$ smooth plane curve of degree $2g-2=4$.

(In this case it can be given by an equation $f(x,y,z)=0$ of degree 4).

$\underline{g=4}$: • Hyperelliptic curves:

$y^2 = f(x)$ $\quad f$ squarefree of degree 9 or 10.

• Non-hyperelliptic:

$X \hookrightarrow \mathbb{P}^3$ of degree 6, X is an intersection of a deg 2 hypersurface and a degree 3 surface. (in $\mathbb{P}3$)

Jacobians

Let $G = \mathrm{Gal}(\bar{k}/k)$.

X curve over k; $\quad \overline{X} = X_{\bar{k}}$ (the same curve, but considering the equation as defined over $\bar{k}$)

$\mathrm{Div}(\overline{X}) :=$ the free abelian group with basis $X(\bar{k})$.

$\mathrm{Div}(X) :=$ the free abelian group with basis $\{0\text{-dimensional irreducible subvarieties of } X\} =$
$= \mathrm{Div}(\overline{X})^G$

Then we have:

$$\begin{tikzcd} k(X)^* \arrow[r, "f \mapsto (f)"] \arrow[d, hook] & \mathrm{Div}(X) \arrow[r, "D \mapsto {[D]}"] \arrow[d, hook] & \mathrm{Pic}(X) \arrow[r] \arrow[d] & 0 \\ k(\overline{X})^* \arrow[r] & \mathrm{Div}(\overline{X}) \arrow[r] & \mathrm{Pic}(\overline{X}) \arrow[r] & 0 \end{tikzcd}$$

defined as to fit in this sequence

to find this, need to use H90. (exercise)

In fact, $\mathrm{Pic}\, X \hookrightarrow (\mathrm{Pic}\, \overline{X})^G$ but not need to be isomorphism.

The degree map is $\operatorname{Div}\bar{X} \xrightarrow{\deg} \mathbb{Z}$

$\sum n_P P \mapsto \sum n_P$

As $\deg(f)=0$, we get

$$\begin{tikzcd} \operatorname{Div}\bar{X} \arrow[r, "\deg"] \arrow[d] & \mathbb{Z} \\ \operatorname{Pic}\bar{X} \arrow[ur, dashed, "\deg"'] & \end{tikzcd}$$

we have the same

$$\begin{tikzcd} & \operatorname{Pic}X \arrow[dr, dashed, "\deg"] & \\ \operatorname{Div}X \arrow[ur] \arrow[rr, "\deg"'] & & \mathbb{Z} \end{tikzcd}$$

And their kernels define respectively $\operatorname{Div}^\circ\bar{X}$, $\operatorname{Div}^\circ X$, $\operatorname{Pic}^\circ\bar{X}$, $\operatorname{Pic}^\circ X$.

Also $\operatorname{Pic}^\circ X \hookrightarrow (\operatorname{Pic}^\circ\bar{X})^G$ but ~~need~~ not need to be equal.

this is weaker, but sufficient!

Theorem: Suppose X has a k-point (at least a divisor of degree 1).

There is a ~~ka~~ variety J, called the Jacobian of X, such that

$$J(k) \text{ is naturally in bijection with } \operatorname{Pic}^\circ X.$$

we say that J represents the functor $L \mapsto \operatorname{Pic}^\circ(X_L)$

By "naturally" we mean that for each extension $L \supseteq k$, there should exist a bijection $J(L) \xrightarrow{\sim} \operatorname{Pic}^\circ(X_L)$ and there should be compatible with base changes.

In particular, if $\sigma: L \to L'$ restricts to the identity on k, then

$$\begin{tikzcd} J(L) \arrow[r, "\sim"] \arrow[d] & \operatorname{Pic}^\circ(X_L) \arrow[d] \\ J(L') \arrow[r, "\sim"] & \operatorname{Pic}^\circ(X_{L'}) \end{tikzcd}$$

applying σ to the coordinates of the point

applying σ to the points on the divisor.

should commute.

Pf: See Milne, "Jacobian varieties" in the Cornell-Silverman volume. (hard proof)

Corollary: If X has a k-point (or divisor of deg. 1), then $\operatorname{Pic}^\circ X = (\operatorname{Pic}^\circ\bar{X})^G$.

Pf: Taking $L=L'=\bar{k}$ and $\sigma \in \operatorname{Gal}(\bar{k}/k)$,

we see that $J(\bar{k}) \xrightarrow{\sim} \operatorname{Pic}^\circ(\bar{X})$ as G-modules.

Take G-invariants: $J(\bar{k})^G \cong \operatorname{Pic}^\circ(\bar{X})^G$

Galois theory $\Rightarrow$ $\|$

$J(k) \cong \operatorname{Pic}^\circ(X)$ //

Fact: If X has no k-point, one can still define a k-variety J, but it represents a slightly different functor:

$$J(L) = \left(\mathrm{Pic}^{\circ} X_{\bar{L}}\right)^{\mathrm{Gal}(\bar{L}/L)}$$

and this group always has elements!

Note that ~~…~~ J has always a rational point, as $J(k) \leftrightarrow \mathrm{Pic}^{\circ} X$

Elements of $J(L)$ will be written as $[D]$, where D is a divisor of degree 0 (on $X_{\bar{L}}$).

Facts:

(1) J is an abelian variety (~~connected~~, irreducible, projective group variety).

(2) $\dim J = g$, where g is the genus of X.

(3) If X has a k-point P (or a divisor of degree 1), each point in $J(k)$ can be written as $[D - g \cdot P]$ for some $D \geq 0$, of degree g.

Pf: A point in $J(k)$ is an element of $\mathrm{Pic}^{\circ} X$, hence is $[E]$ for some $E \in \mathrm{Div}^{\circ} X$.

Apply R-R to $E + gP \in \mathrm{Div}\, X$ (of degree g):

$$\ell(E+gP) - \ell(K-(E+gP)) = \deg(\cancel{E+gP}) + 1 - \cancel{g}$$

$$\Rightarrow \ell(E+gP) \geq 1 \Rightarrow \exists f \in k(X)^* \text{ such that}$$

$$(f) + E + gP \geq 0. \quad \text{Call } D := (f) + E + gP.$$

it is an effective divisor of degree g, and

$$[D - gP] = [E + gP - gP] = [E] \qquad //$$

Jacobians over special fields

1) $k = \mathbb{F}_q$ finite field, then X automatically has a divisor of degree 1, and $J(\mathbb{F}_q)$ is a finite abelian group.

2) k number field, the Mordell-Weil Thm says that $J(k)$ is a finitely generated abelian group.

3) $k = \mathbb{C}$, then $J(\mathbb{C})$ is a connected compact commutative Lie group $/\mathbb{C}$ because it's projective

so analytically,

$$J(\mathbb{C}) \xleftarrow{\exp} \mathbb{C}^g/\Lambda$$

where ~~rank~~ Λ is a discrete $\mathbb{Z}$-submodule of rank $2g$.

Suppose $P \in X(k)$ (or more generally, P is a divisor of degree 1):
Then the map:

$$\begin{aligned} X &\longrightarrow J \\ Q &\longmapsto [Q-P] \end{aligned} \qquad \forall Q \in X(L)$$

is a morphism of varieties.
If $g \geq 1$, then it is an embedding.

Faltings' Theorem (previously Mordell's conjecture):

$$\left.\begin{array}{l} K \text{ number field} \\ X \text{ curve}/_K \text{ of genus} \geq 2 \end{array}\right\} \Rightarrow X(K) \text{ is finite.}$$

The two known proofs (due to Faltings, Vojta simplified by Bombieri) are not effective, even in principle: they give bounds on the number of K-points but not on their "size" (height) of the solutions.

Alternative strategy:

We'll work over a field K such that X has a known divisor of degree 1.
(if we are able to solve this problem, we'll be able to solve the original one).

Embed $X \hookrightarrow J$.

1) Determine generators for $J(K)$ (and the corresponding relations).
2) Try to figure out which points in $J(K)$ lie on X. (these are the points in $X(k)$).

Problem: there exists NO guaranteed algorithm for either of the two previous steps.

• Descent on Jacobians of some hyperelliptic curves. (2-descent)

X has a model of the form $y^2 = f(x)$ — f squarefree, $\deg f = 2g+1$.

$$X \xrightarrow{x} \mathbb{P}^1 = \mathbb{A}^1 \cup \{\infty\}$$

X can be put in this form iff one of the $2g+2$ branch points is a K-point

~~X~~ can be put in this ~~form~~ if (because then can move it to ∞).

Since $\deg f$ is odd, there is a unique point $\infty \in X(\mathbb{Q})$ above $\infty \in \mathbb{P}^1(\mathbb{Q})$.

◦ The 2-torsion of hyperelliptic Jacobians.

$J[2] := \{P \in J(\overline{\mathbb{Q}}) : 2P = 0\}$

If we fix an embedding $\overline{\mathbb{Q}} \hookrightarrow \mathbb{C}$, then $J[2] = \{P \in J(\mathbb{C}) : 2P = 0\}$

But now $J(\mathbb{C})$ is, analytically, $\simeq \mathbb{C}^g/\Lambda$ where Λ is a discrete g-module of rank $2g$.

So $J[2] \simeq \dfrac{\frac{1}{2}\Lambda}{\Lambda} \left(\simeq \left(\mathbb{Z}/2\mathbb{Z}\right)^{2g} \text{ (as an abstract group)} \right)$

Let $\alpha_1, \dots, \alpha_{2g+1}$ be the zeroes of f in $\overline{\mathbb{Q}}$; let $W_i = (\alpha_i, 0) \in X(\overline{\mathbb{Q}})$.

Let $\mathcal{W} := \{W_i\}_{1 \le i \le 2g+1}$. $\mathcal{W} \cup \{\infty\}$ is called the set of ~~ramification points~~ / the set of Weierstrass points.

$\mathcal{W}$ is a G-set $(G = \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}))$.

<u>Claim</u>: $[W_i - \infty] \left(\in \mathrm{Pic}^0(X_{\overline{\mathbb{Q}}}) = J(\overline{\mathbb{Q}})\right)$ belongs to $J[2]$.

Pf: Consider the function $x - \alpha_i$, on $X_{\overline{\mathbb{Q}}}$, which has a double pole at ∞ $(v_\infty(x-\alpha_i) = -2)$. As it is well defined everywhere else and it is zero only when $x = \alpha_i$, and it has to be double because $\deg(\delta) = 0$. So $\mathrm{div}(x - \alpha_i) = 2W_i - 2\infty$.

In $J(\overline{\mathbb{Q}}) = \mathrm{Pic}^0(X_{\overline{\mathbb{Q}}})$, $0 = [2W_i - 2\infty] = 2[W_i - \infty]$. //

Claim: $\sum_{i=1}^{2g+1} [W_i - \infty] = 0$ in $J(\bar{\mathbb{Q}})$.

Pf: The function y:

$v_\infty(y) = -(2g+1)$ and it has a zero at each W_i.

So $\mathrm{div}(y) = W_1 + \dots + W_{2g+1} - (2g+1)\infty$.

In J, $0 = [W_1 - \infty] + \dots + [W_{2g+1} - \infty]$.

Proposition: There exists an split exact sequence of G-modules:

$$0 \to \mathbb{Z}/2\mathbb{Z} \to (\mathbb{Z}/2\mathbb{Z})^W \xrightarrow{s} J[2] \to 0$$

this is $\cong_{\text{abstract}}$ $(\mathbb{Z}/2\mathbb{Z})^{2g+1}$, but with the added galois action given by W.

$1 \mapsto (1,1,\dots,1)$

$(a_1, \dots, a_{2g+1}) \longmapsto \sum a_i [W_i - \infty]$

$\sum a_i \longleftarrow$

Pf: Since $J[2] \cong (\mathbb{Z}/2\mathbb{Z})^{2g}$, it suffices to show that $\ker s$ is not bigger than $\langle (1,1,\dots,1) \rangle$.

Suppose $(\varepsilon_1, \dots, \varepsilon_{2g+1}) \in \ker(s)$ for $\varepsilon_i \in \{0,1\}$ not all 1.

i.e. $\sum \varepsilon_i [W_i - \infty] = 0 \to \sum \varepsilon_i W_i - (\sum \varepsilon_i)\infty = \mathrm{div}(h)$ for some rational function h on $X_{\bar{\mathbb{Q}}}$.

The only pole of h is in ∞, so $h \in \bar{\mathbb{Q}}[x,y]$, and also:

$$h = h_1(x) + h_2(x) y \quad \text{for some } h_1(x), h_2(x) \in \bar{\mathbb{Q}}[x]$$

$$2g \geq \sum \varepsilon_i = -v_\infty(h) = \max\{2 \deg h_1, 2 \deg h_2 + (2g+1)\}$$

$v_\infty(h_1)$ is even, $v_\infty(y h_2)$ is odd | val. is exactly the minimum of valuations

We must have $h_2 = 0$, and so $h = h_1(x) = \prod (x - \lambda_j)$.

$v_{W_i}(x - \lambda_j)$ is either 0 or 2 (2 iff $\lambda_j = \alpha_i$).

So, $v_{W_i}(h)$ is even; but $v_{W_i}(h) = \varepsilon_i$. So $\varepsilon_i = 0$ $\forall i$ //.

Exercise: For $y^2 = f(x)$ with $\deg f = 2g+2$, let

$\alpha_1, \dots, \alpha_{2g+2}$ be the zeros of f, $w_i := (x_i, 0)$, $W = \{w_i\}_{1 \le i \le 2g+2}$

Then $\exists$ exact sequence $$0 \to \mathbb{Z}/2\mathbb{Z} \to \left(\mathbb{Z}/2\mathbb{Z}\right)^W_{\text{sum}=0} \to J[2] \to 0$$

Corollary of prop:

Let $L := \mathbb{Q}[T]/(f(T))$ (a product of number fields, one for each factor of f).
(by CRT)

Define $\underset{\bar{\mathbb{Q}} \nearrow}{\bar{L}} := L \otimes_{\mathbb{Q}} \bar{\mathbb{Q}} = \bar{\mathbb{Q}}[T]/(f(T)) \underset{CRT}{\cong} \prod \bar{\mathbb{Q}}(T)/(T-\alpha_i) \simeq \bar{\mathbb{Q}}^W$

$\rightsquigarrow \bar{\mathbb{Q}} \hookrightarrow \bar{\mathbb{Q}}^W$, $c \longmapsto (c, c, c, \dots, c)$

For any ring R, let $\mu_2(R) := \{r \in R : r^2 = 1\}$.

Then there is an split exact sequence of G-modules.

$$0 \to J[2] \to \mu_2(\bar{L}) \xrightarrow{N_{\bar{L}/\bar{\mathbb{Q}}}} \mu_2(\bar{\mathbb{Q}}) \to 0$$

Pf

$$\begin{tikzcd}
 & & & & J[2] \arrow[dl] & 0 \arrow[l] \\
\mu_2(\bar{L}) \arrow[r, equal] \arrow[d, "N_{\bar{L}/\bar{\mathbb{Q}}}"'] & \mu_2(\bar{\mathbb{Q}}^W) \arrow[r, equal] & \{\pm 1\}^W \arrow[r, "\cong"] & (\mathbb{Z}/2\mathbb{Z})^W \arrow[d, "\text{sum}"] & & \\
\mu_2(\bar{\mathbb{Q}}) \arrow[rrr, "\sim"] & & & \mathbb{Z}/2\mathbb{Z} \arrow[d] & & \\
 & & & 0 & &
\end{tikzcd}$$

Can reverse the sequence because it's split. Then, reinterpret by these isomorphisms. //

We want to see that $J(\mathbb{Q}) \simeq \mathbb{Z}^r \oplus T$ ← torsion

There is an exact sequence:

$$0 \to J[2] \to J(\bar{\mathbb{Q}}) \xrightarrow{[2]} J(\bar{\mathbb{Q}}) \to 0$$

(To see that $[2]$ is surjective, argue that $J(\mathbb{C}) \xrightarrow{[2]} J(\mathbb{C})$ is, because of the analytic representation, and then if we start with an elmt of $J(\bar{\mathbb{Q}})$, its preimage will have to be also in $J(\bar{\mathbb{Q}})$ because it will be the solution of a finite number of equations).

So we have the long exact sequence:

$$\cancel{0 \to J[2] \to J(\bar{\mathbb{Q}}) \to}$$

$$0 \to J[2] \to J(\mathbb{Q}) \to J(\mathbb{Q}) \to H^1(\mathbb{Q}, J[2]) \to H^1(\mathbb{Q}, J) \xrightarrow{2} H^1(\mathbb{Q}, J) \to \cdots$$

$$H^1(\mathbb{Q}, J) = H^1(G, J(\bar{\mathbb{Q}})).$$

Then,

$$0 \to \frac{J(\mathbb{Q})}{2J(\mathbb{Q})} \to H^1(\mathbb{Q}, J[2]) \to H^1(\mathbb{Q}, J)[2] \to 0$$

<u>Lemma</u>: $\dim_{\mathbb{F}_2} \dfrac{J(\mathbb{Q})}{2J(\mathbb{Q})} = r + \dim_{\mathbb{F}_2} J(\mathbb{Q})[2]$

Pf: As $J(\mathbb{Q}) \simeq \mathbb{Z}^r \oplus T$,

$$\frac{J(\mathbb{Q})}{2J(\mathbb{Q})} = \frac{\mathbb{Z}^r \oplus T}{2(\mathbb{Z}^r \oplus T)} = \left(\mathbb{Z}/2\mathbb{Z}\right)^r \oplus \frac{T}{2T}$$

and $\# \frac{T}{2T} = \# T[2] = \# J(\mathbb{Q})[2]$.

It is easy to see that $\dim_{\mathbb{F}_2} J(\mathbb{Q})[2] = (\# G\text{-orbits in } W) - 1$ (from the previous exact sequences).

To see what $H^1(\mathbb{Q}, J[2])$ is, remember we had the split seq:

$$0 \to J[2] \to \mu_2(\bar{L}) \xrightarrow{N} \mu_2(\bar{\mathbb{Q}}) \to 0.$$

Taking $H^1(\mathbb{Q}, -)$ (as it is split) we get:

$$\cancel{0 \to} H^1(\mathbb{Q}, J[2]) \cong \ker\left(H^1(\mathbb{Q}, \mu_2(\bar{L})) \longrightarrow H^1(\mathbb{Q}, \mu_2(\bar{\mathbb{Q}}))\right).$$

<u>Recall</u>: $0 \to \mu_2(\bar{\mathbb{Q}}) \to \bar{\mathbb{Q}}^* \xrightarrow{2} \bar{\mathbb{Q}}^* \to 0$, so get $\cdots \mathbb{Q}^* \to H^1(\mathbb{Q}, \mu_2) \to H^1(\mathbb{Q}, \bar{\mathbb{Q}}^*)$, $H^1(\mathbb{Q}, \bar{\mathbb{Q}}^*) = 0$ by H90.

Therefore, $H^1(\mathbb{Q}, \mu_2(\bar{\mathbb{Q}})) \simeq \mathbb{Q}^*/\mathbb{Q}^{*2}$

A generalization of H90 says that $H^1(\mathbb{Q}, \bar{L}^*) = 0$

And this implies $H^1(\mathbb{Q}, \mu_2(\bar{L})) = \bar{L}^*/\bar{L}^{*2}$

<u>Conclusion:</u> $H^1(\mathbb{Q}, J[2]) \simeq \ker\left(L^*/L^{*2} \xrightarrow{N_{L/\mathbb{Q}}} \mathbb{Q}^*/\mathbb{Q}^{*2} \right)$

To find $J(\mathbb{Q})/2J(\mathbb{Q})$, we also need to know about the maps.

So, what is the map $J(\mathbb{Q})/2J(\mathbb{Q}) \to H^1(\mathbb{Q}, J[2])$ concretely?

First, define an homomorphism

$$(\mathrm{Div}\,\bar{X})_{\substack{\text{no points}\\ \text{in } W\cup\{\infty\}}} \longrightarrow \bar{L}^*$$

$$P \longmapsto x(P) - T \qquad \text{(where } T \text{ is the image of } T \text{ in } \bar{\mathbb{Q}}[T]/(f(T))\text{).}$$

and extend it by linearity.

This induces a map $(\mathrm{Div}\,X)_{\text{no } W\cup\{\infty\}} \to L^*$.

By Weil reciprocity, $\mathrm{div}(h) \mapsto$ an element of L^{*2} $\quad (h \in \mathbb{Q}(X)^*)$.

Also $(\mathrm{Div}\,X)_{\substack{\text{no}\\ W\cup\{\infty\}}} \hookrightarrow \mathrm{Div}\,X \twoheadrightarrow \mathrm{Pic}\,X$ and it turns out that

the composition is <u>surjective</u> (exercise).

Therefore, $(\mathrm{Div}\,X)_{\text{no } W\cup\{\infty\}} \to L^*/L^{*2}$ induces $\mathrm{Pic}\,X \to L^*/L^{*2}$

$$\begin{tikzcd} \mathrm{Pic}\,X \arrow[r] & L^*/L^{*2} \\ \mathrm{Pic}^0 X \arrow[d, equal] & \\ J(\mathbb{Q}) \arrow[r] & J(\mathbb{Q})/2J(\mathbb{Q}) \arrow[uu, "\text{``}x-T\text{''}"'] \end{tikzcd}$$

• Jacobians over local fields, and computations of $Sel^2(J)$.

Remember that $0 \to \dfrac{J(\mathbb{Q})}{2J(\mathbb{Q})} \xrightarrow{x-T} \ker\left(\dfrac{L^*}{L^{*2}} \xrightarrow{N} \dfrac{\mathbb{Q}^*}{\mathbb{Q}^{*2}}\right)$

so we'd like to find the image of $x-T$, but the $\ker(- \to -)$ is infinite while we know that $\dfrac{J(\mathbb{Q})}{2J(\mathbb{Q})}$ is finite. Furthermore, there is no guaranteed algorithm to test whether a given element of that kernel comes from $\dfrac{J}{2J}$. What we can do is to work locally:

$$\begin{tikzcd}
0 \arrow[r] & \dfrac{J(\mathbb{Q})}{2J(\mathbb{Q})} \arrow[r, "x-T"] \arrow[d] & \ker\left(\dfrac{L^*}{L^{*2}} \xrightarrow{N} \dfrac{\mathbb{Q}^*}{\mathbb{Q}^{*2}}\right) \cong H^1(\mathbb{Q}, J[2]) \\
0 \arrow[r] & \prod_p \dfrac{J(\mathbb{Q}_p)}{2J(\mathbb{Q}_p)} \arrow[r, "x-T"] & \prod_p \ker\left(\dfrac{L_p^*}{L_p^{*2}} \xrightarrow{N} \dfrac{\mathbb{Q}_p^*}{\mathbb{Q}_p^{*2}}\right)
\end{tikzcd}$$

where we define, for each p prime, $L_p := L \otimes_{\mathbb{Q}} \mathbb{Q}_p = \dfrac{\mathbb{Q}_p[T]}{(f(T))}$

$$Sel = Sel^2(\mathbb{Q}, J) := \left\{ \xi \in \ker\left(\frac{L^*}{L^{*2}} \xrightarrow{N} \frac{\mathbb{Q}^*}{\mathbb{Q}^{*2}}\right) : \text{the image } \xi_p \in \ker\left(\frac{L_p^*}{L_p^{*2}} \to \frac{\mathbb{Q}_p^*}{\mathbb{Q}_p^{*2}}\right) \text{ is contained in the image of the local } x-T \text{ map for all } p \leq \infty \right\}$$

Selmer condition at p

So for the commutativity of the diagrams, $\dfrac{J(\mathbb{Q})}{2J(\mathbb{Q})} \overset{x-T}{\hookrightarrow} Sel$

<u>Theorem</u>: Sel is <u>finite</u> and <u>computable</u>.

- Jacobians over $\mathbb{C}$

If E is an elliptic curve $/\mathbb{C}$, then $E \xrightarrow[\text{analitically}]{\sim} \mathbb{C}/\Lambda$ ← as groups; Λ ← rank 2 discrete $\mathbb{Z}$-lattice.

We'll generalize that to higher-dimensions:

$$\omega = \frac{dx}{y} \longleftarrow dz$$
$$O \longleftarrow 0$$
$$Q \longmapsto \int_O^Q \frac{dx}{y}$$
← well defined modulo $\Lambda := \{\int_\gamma \omega : \gamma \text{ is a 1-cycle}\}$

Abel-Jacobi thm: $X/\mathbb{C}$ curve of genus g; let $\omega_1, \dots, \omega_g$ be a $\mathbb{C}$-basis for the regular differentials on X.

For each 1-cycle γ in $X(\mathbb{C})$ (← this is a compact Riemann surface), we get a period, by $\left(\int_\gamma \omega_1, \dots, \int_\gamma \omega_g\right) \in \mathbb{C}^g$.

This induces the period map:

$$H_1(X(\mathbb{C}), \mathbb{Z}) \longrightarrow \mathbb{C}^g$$
$$H_1(X(\mathbb{C}), \mathbb{Z}) \overset{\text{non-canonical}}{\cong} \mathbb{Z}^{2g}$$

Whose image Λ is called the period lattice.

Fix $P \in X(\mathbb{C})$ (will play the role of $O \in$ elliptic curve). Then

$$X(\mathbb{C}) \longrightarrow \mathbb{C}^g/\Lambda$$
$$Q \longmapsto \left(\int_P^Q \omega_1, \dots, \int_P^Q \omega_g\right)$$

is the same map as

$$X(\mathbb{C}) \longrightarrow J(\mathbb{C})$$
$$Q \longmapsto [Q-P]$$

- Jacobians over $\mathbb{R}$:

$$J(\mathbb{R}) \xrightarrow{\text{analitically } \sim} \left(\frac{\mathbb{R}}{\mathbb{Z}}\right)^g \times \left(\mathbb{Z}/2\mathbb{Z}\right)^m \quad \text{where } 0 \leq m \leq g$$

$J(\mathbb{R})$: g-dimensional compact commutative Lie-group (not necessarily connected)

- Jacobians over p-adics:

- Facts about $\mathbb{Q}_p^*$:

1) there's an exact sequence $0 \to \mathbb{Z}_p^\times \to \mathbb{Q}_p^\times \xrightarrow{v} \mathbb{Z} \to 0$

2) " " " " $0 \to 1+p\mathbb{Z}_p \to \mathbb{Z}_p^* \to \mathbb{F}_p^\times \to 0$

$1+p\mathbb{Z}_p \supseteq 1+p^2\mathbb{Z}_p \supseteq \cdots$ quotients isomorphic to $\mathbb{F}_p$

3) There's an analytic homomorphism:

$$1+p\mathbb{Z}_p \xrightarrow{\log} \mathbb{Q}_p$$

$$1+x \longmapsto \int_1^{1+t} \frac{dt}{t} = \int_0^x \frac{du}{1+u} = \int_0^x (1-u+u^2-u^3+\cdots)\,du = x-\frac{x^2}{2}+\frac{x^3}{3}-\cdots$$

invariant differential 1-form; identity of the group

4) If n is sufficiently large $\left(n > \frac{1}{p-1}\right)$ (in this case, it doesn't say much for $p\neq 2$, but it can then be generalized), then

$$1+p^n\mathbb{Z}_p \underset{\exp}{\overset{\log}{\rightleftarrows}} p^n\mathbb{Z}_p \text{ (under addition)}$$ is an analytic (in the sense of p-adic analysis) isomorphism:

$$1+x+\frac{x^2}{2!}+\cdots \longleftarrow\!\shortmid\ x$$

5) The function log can be extended uniquely to a homomorphism

$$\mathbb{Z}_p^\times \to \mathbb{Q}_p$$
$$c \longmapsto \frac{\log(c^{p-1})}{p-1}$$

If we chose the value of $\log p$ (usually $\log p = 0$) then get $\mathbb{Q}_p^\times \xrightarrow{\log} \mathbb{Q}_p$

- Facts about $J(\mathbb{Q}_p)$: (they are analogue to the previous ones!):

1) $0 \to J^0(\mathbb{Q}_p) \to J(\mathbb{Q}_p) \to \Phi(\mathbb{F}_p) \to 0$ — finite group, composed of the $\mathbb{F}_p$-points of the component group of the Neron model.

(if X has good reduction, then J has also good reduction, and then Φ is trivial).

2) $0 \to J^1(\mathbb{Q}_p) \to J^0(\mathbb{Q}_p) \xrightarrow{\text{red}} J^0(\mathbb{F}_p) \to 0$ — $\mathbb{F}_p$-points of the connected component of $J \bmod p$ (its Neron model mod p). (is an algebraic group over $\mathbb{F}_p$)

$J^1(\mathbb{Q}_p)$ (kernel of reduction) $\supseteq J^2(\mathbb{Q}_p) \supseteq \cdots$ quotients isomorphic to $\mathbb{F}_p^g$ as vec-spaces over $\mathbb{F}_p$.

$\downarrow$

3) $\exists$ analytic homomorphism,

$$J^1(\mathbb{Q}_p) \xrightarrow{\log} \bigoplus_g \mathbb{Q}_p \quad \leftarrow \text{under addition}$$

$$P \longmapsto \left(\int_0^P \omega_1, \int_0^P \omega_2, \dots, \int_0^P \omega_g \right)$$ where $\omega_1, \dots, \omega_g$ is a basis for the space of regular 1-forms on J

4) If $n > \frac{1}{p-1}$, we get isomorphisms

points that reduce to identity mod p^n $\rightarrow$ $J^n(\mathbb{Q}) \underset{\exp}{\overset{\log}{\rightleftarrows}} \bigoplus_g (p^n \mathbb{Z}_p)$

5) Log extends uniquely to $J(\mathbb{Q}_p) \longrightarrow \bigoplus_g \mathbb{Q}_p$

Corollary: $J^1(\mathbb{Q}_p)$ is torsion-free if $p > 2$

Corollary: $J(\mathbb{Q})_{tors} \xrightarrow{red} J(\mathbb{F}_p)$ is injective if $p > 2$ is a prime of good reduction.

Prop: $\# \dfrac{J(\mathbb{R})}{2J(\mathbb{R})} = \dfrac{\# J(\mathbb{R})[2]}{2^g}$

Pf: $J(\mathbb{R})$ is a compact topological group.

Let μ be a Haar measure on $J(\mathbb{R})$. Then

$J(\mathbb{R}) \xrightarrow{\times 2} J(\mathbb{R})$

locally scales μ by 2^g. but it is a d-to-1 map onto its image, where d is $\# \ker = \# J(\mathbb{R})[2]$.

So $\mu(2J(\mathbb{R})) = \dfrac{2^g \mu(J(\mathbb{R}))}{d} \Rightarrow \# \dfrac{J(\mathbb{R})}{2J(\mathbb{R})} = \dfrac{\mu(J(\mathbb{R}))}{\mu(2J(\mathbb{R}))} = \dfrac{d}{2^g}$ //

Note: to prove this theorem, could just use $J(\mathbb{R}) \simeq \left(\frac{\mathbb{R}}{\mathbb{Z}}\right)^g \oplus \left(\mathbb{Z}/2\mathbb{Z}\right)^m$.

The same proof shows:

Prop: $\# \dfrac{J(\mathbb{Q}_p)}{2J(\mathbb{Q}_p)} = \dfrac{\# J(\mathbb{Q}_p)[2]}{\|2\|_p^g}$ (where $\|2\|_p = \begin{cases} 2 & \text{if } p = \infty \\ 1/2 & \text{if } p = 2 \\ 1 & \text{otherwise} \end{cases}$)

• Unramifiedness.

Take $X: y^2 = f(x)$ (of odd degree, sqfree, coeffs in $\mathbb{Z}$)

Let S ("bad primes") be a finite set of places of $\mathbb{Q}$ containing ∞, 2, all primes dividing the discriminant of $F(x,z) = z^{2g+2} f\left(\frac{x}{z}\right)$ (i.e. those that make $\tilde{F}(x,z)$ be not squarefree)

Prop: If $p \notin S$, then

$$\operatorname{Im}\left(\frac{J(\mathbb{Q}_p)}{2J(\mathbb{Q}_p)} \xrightarrow{x-T} \ker\left(\frac{L_p^*}{L_p^{*2}} \to \frac{\mathbb{Q}_p^*}{\mathbb{Q}_p^{*2}}\right)\right) = \left\{\text{unramified elements in the kernel of } \frac{L_p^*}{L_p^{*2}} \to \frac{\mathbb{Q}_p^*}{\mathbb{Q}_p^{*2}}\right\}$$

Def: If K is a local field, $a \in \frac{K^*}{K^{*2}}$, say that a is <u>unramified</u> iff $\frac{K(\sqrt{a})}{K}$ is unramified.

Extend the definition to products of local fields: unramified iff all components are.

Example:

Let X be a smooth, projective model of $y^2 = f(x)$, where $f(x) = x^5 + x + 3$.

It is a genus-2 curve.

$\operatorname{disc}(f) = 253381$ (prime). So $S = \{2, 253381, \infty\}$.

Lemma: $J(\mathbb{Q})_{tors}$ is trivial.

Pf We know that $J(\mathbb{Q})_{tors} \xhookrightarrow{\text{red}} J(\mathbb{F}_p)$ $\forall p \notin S$

p	$\#J(\mathbb{F}_p)$
3	12
5	36
7	81
11	144
13	126
17	205

$\#J(\mathbb{F}_p)$ ← can be computed from knowing $X(\mathbb{F}_p), X(\mathbb{F}_{p^2}), \dots, X(\mathbb{F}_{p^g})$

$\to \gcd(\dots) = 1$, so $J(\mathbb{Q})_{tors}$ is trivial.

Search for $\mathbb{Q}$-points on X and J:

$\nexists$ nonconstant $X \to E$ (E elliptic curve), because that would induce $J \to J(E) \cong E$, so $J \overset{\text{isogenous}}{\sim} E \times E'$ and $\underline{\operatorname{cond}(J)} = \operatorname{cond}(E) \cdot \operatorname{cond}(E')$ so either E or E' has conductor $= 1$, but the smallest possible conductor for $E/\mathbb{Q}$ is ≥ 11.

If the case was that we had $X \to E$, then computing the rational points on E and their preimages would give us all the rational points on X.

So we search for $\mathbb{Q}$-points on X and J.

We find $\infty, (-1, \pm 1), (23, \pm 2537)$. (on X)

So let $P := [(-1,1) - \infty]$ on $J(\mathbb{Q})$

$[(-1,-1) - \infty] = -P$ on $J(\mathbb{Q})$ (use $\mathrm{div}(x+1)$)

So we only use $(-1, 1)$ and not the other one. Similarly, only use $(23, 2537)$

$Q := [(23, 2537) - \infty]$

As f is irreducible, $L := \dfrac{\mathbb{Q}[T]}{(f(x))}$ is a number field of degree 5.

$$\frac{J(\mathbb{Q})}{2J(\mathbb{Q})} \xhookrightarrow{x-T} \mathrm{Ker}\left(\frac{L^*}{L^{*2}} \xrightarrow{N} \frac{\mathbb{Q}^*}{\mathbb{Q}^{*2}}\right)$$

$P \longmapsto -1-T$

$Q \longmapsto 23-T$

Neither $-1-T$ nor $23-T$ are squares, but they product are squares.

We need more points on J, so we can search for point on X defined over quadratic extension of $\mathbb{Q}$.

$R := [(\omega, 2) + (\bar{\omega}, 2) - 2\infty]$ where $\omega^2 - \omega + 1 = 0$ (6th root of 1).

$R \longmapsto (\omega - T)(\bar{\omega} - T) = 1 - T + T^2$.

$-1-T, 1-T+T^2$ are independent in L^*/L^{*2}. So P, R are $\mathbb{F}_2$-indep in $\dfrac{J(\mathbb{Q})}{2J(\mathbb{Q})}$

So P, R are $\mathbb{Z}$-independent in $J(\mathbb{Q})$.

So $\mathrm{rank}(J(\mathbb{Q})) \geq 2$.

Claim: $\mathrm{rank}(J(\mathbb{Q})) = 2$.

Pf Show $\dim_{\mathbb{F}_2} \mathrm{Sel} \leq 2$.

$Cl(L) = \{1\}$, implies {elements of $\frac{L^*}{L^{*2}}$ unramified outside S} $= \dfrac{\mathcal{O}_{L,S}^*}{\mathcal{O}_{L,S}^{*2}}$ (S-units)

Today: The method of Chabauty & Coleman

X curve $/\mathbb{Q}$ (or number field) of genus $g \geq 2$ (so $X(\mathbb{Q})$ is finite).

Let J be its jacobian.

Suppose $\exists$ $O \in X(\mathbb{Q})$. So we have an embedding $\begin{matrix} X \hookrightarrow J \\ P \mapsto [P-O]. \end{matrix}$

(Note that if $\nexists O$, then $\exists D \in \mathrm{Div}X$ of some degree $d>0$, and the morphism $\begin{matrix} X \longrightarrow J \\ P \longmapsto [dP-D] \end{matrix}$ is a good substitute (but not an embedding, in general!))

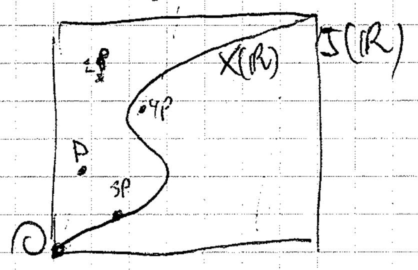
Suppose that $J(\mathbb{Q})$ is known (this is a big supposition, as there's no known algorithm for that!).

Then $X(\mathbb{Q})$ is the subset of points in $J(\mathbb{Q})$ lying on X.

This is easy to determine if $J(\mathbb{Q})$ is finite (rank 0) (using Riemann-Roch).

So assume now $J(\mathbb{Q})$ is infinite (rank $J \geq 1$).

Idea (that usually doesn't work): look in $J(\mathbb{R}) \simeq \left(\frac{\mathbb{R}}{\mathbb{Z}}\right)^g + \{\text{finite}\}$



Typically, $J(\mathbb{Q})$ will be dense in $J(\mathbb{R})$ (or at least its connected component).

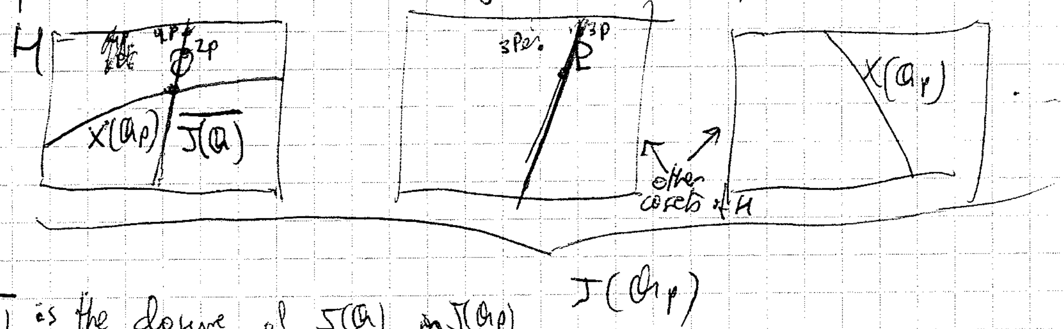
So it won't work.

- Better idea (Chabauty) (inspired by Skolem's method for Thue equations).

Instead of looking in $\mathbb{R}$, look in $\mathbb{Q}_p$ for some finite p!

Recall: $J(\mathbb{Q}_p)$ has a subgroup H of finite order, isomorphic (as topological group) to $\bigoplus_g \mathbb{Z}_p$ (eg. if $p>2$ is of good reduction, can take $H = J^1(\mathbb{Q}_p)$
$\qquad\qquad \mathrel{\rotatebox{90}{=}}$
$\qquad\qquad \ker(J(\mathbb{Q}_p) \to J(\mathbb{F}_p))$)

The simplest nontrivial case, $g=2$: $J(\mathbb{Q}) \simeq \mathbb{Z}$ as abelian groups generated by P



($\overline{J(\mathbb{Q})}$ is the closure of $J(\mathbb{Q})$ in $J(\mathbb{Q}_p)$ resp. the p-adic topology)

This $\overline{J(\mathbb{Q})}$ will be an analytic submanifold of $J(\mathbb{Q}_p)$

Note that $X(\mathbb{Q}) \subseteq X(\mathbb{Q}_p) \cap \overline{J(\mathbb{Q})}$ (inside $J(\mathbb{Q}_p)$).

Let $r := \operatorname{rank} J(\mathbb{Q})$.

Then $\overline{J(\mathbb{Q})}$ has a finite-index subgroup that is a $\mathbb{Z}_p$-module generated by r elements.

Therefore: $\dim \overline{J(\mathbb{Q})} \leq r$

If $r < \dim J = g$, then $\overline{J(\mathbb{Q})}$ has codimension ≥ 1 in $J(\mathbb{Q}_p)$, so we expect that $X(\mathbb{Q}) \cap \overline{J(\mathbb{Q})}$ will be 0-dimensional (and discrete). Also it will be compact ('cause closed in a compact). This implies it will be finite.

Theorem (Chabauty 1941, Coleman 1985): (see a course by Serre ~1980s).
If $r < g$, then $X(\mathbb{Q}_p) \cap \overline{J(\mathbb{Q})}$ is finite, and hence $X(\mathbb{Q})$ is finite.

- How do we bound $X(\mathbb{Q}_p) \cap \overline{J(\mathbb{Q})}$ in practice?

There are two methods:

i) (Flynn). For simplicity, assume $g=2$, $J(\mathbb{Q}) = \mathbb{Z}\cdot P$, $P \in J^1(\mathbb{Q}_p)$, p is a prime of good reduction $p>2$.
Find functions ϕ on $J(\mathbb{Q}_p)$ vanishing on $X(\mathbb{Q}_p)$, and restrict them to a parametrization of $\overline{J(\mathbb{Q})}$.

To do that, (assuming we've already found the ϕ functions), calculate the power series for

$$p\cdot J^1(\mathbb{Q}_p) \underset{\exp}{\overset{\log}{\rightleftarrows}} (p\mathbb{Z}_p)^{\oplus 2} \qquad p>2$$

(to some precision, both p-adically and as a power series).

Use this power series to calculate the coordinates in $J \subseteq \mathbb{P}^N$ of

$$n\cdot P = \exp(\underset{\text{normal multiplication}}{n\cdot}\log P) = (x_0(n), x_1(n), \dots, x_N(n)) \in J(\mathbb{Q}_p),$$

where $x_i(n) \in \mathbb{Q}_p[[n]]$ is computed to some precision (in both senses, again).

We can then plug-in these power series in ϕ: $\phi(x_0(n), \dots, x_N(n))$, and solve the equations $\phi(x_0(n), \dots, x_N(n)) = 0$ for $n \in \mathbb{Z}_p$.

(for solutions n iff the point $nP \in X(\mathbb{Q}_p) \cap \overline{J(\mathbb{Q})}$).

Note that $\phi(x_0(n), \dots, x_N(n)) \in \mathbb{Q}_p[[n]]$

[for an example, see Flynn-Poonen-Schaefer, 1997].

2) (Coleman): It seems to be better.

Find functions on $J(\mathbb{Q}_p)$ vanishing on $\overline{J(\mathbb{Q})}$, and restrict them to (a parametrization of) the curve $X(\mathbb{Q}_p)$. Assume $r<g$,

$$J(\mathbb{Q}_p) \xrightarrow{\log} \mathbb{Q}_p^{\oplus g} = Lie(J/\mathbb{Q}_p) \overset{\lambda}{\twoheadrightarrow} \mathbb{Q}_p$$

Choose linear functional $\lambda: Lie(J/\mathbb{Q}_p) \twoheadrightarrow \mathbb{Q}_p$ that kills $\log(\overline{J(\mathbb{Q})})$.

This λ corresponds canonically to some $\underset{(\Leftrightarrow\text{ invariant})}{\text{regular}}$ 1-form ω_J on $J_{\mathbb{Q}_p}$.

Notation:
- $J(\mathbb{Q}_p) \xrightarrow{\lambda\circ\log} \mathbb{Q}_p$, $\quad Q \longmapsto$ "$\int_0^Q \omega_J$"
- If $Q \in J^1(\mathbb{Q}_p)$, then $\int_0^Q \omega_J$ can be evaluated by expanding ω_J in power series in local coordinates, and integrate them formally, and evaluating the resulting power series (convergent) at the local coordinates of Q.

If $D \in \mathrm{Div}^\circ X_{\mathbb{Q}_p}$, define $\int^D \omega_J := \int_0^{[D]} \omega_J$

This function $Q \mapsto \int_0^Q \omega_J$ is the function vanishing on $\overline{J(\mathbb{Q})}$.

Now we want to restrict it to $X(\mathbb{Q}_p)$

Get $\quad X(\mathbb{Q}_p) \hookrightarrow J(\mathbb{Q}_p) \longrightarrow \mathbb{Q}_p$

$$Q \longmapsto \text{“}\int_{\mathcal{O}}^{Q} \omega\text{”} := \int^{Q-\mathcal{O}} \omega_J$$

where ω is a regular 1-form on $X_{\mathbb{Q}_p}$

(the pullback of ω_J under $X_{\mathbb{Q}_p} \hookrightarrow J_{\mathbb{Q}_p}$).

We want the zeroes of $\quad Q \mapsto \int_{\mathcal{O}}^{Q} \omega$.

More generally, if $Q_1, Q_2 \in X(\mathbb{Q}_p)$, $\int_{Q_1}^{Q_2} \omega := \int^{[Q_2 - Q_1]} \omega_J = \int_{\mathcal{O}}^{Q_2} \omega - \int_{\mathcal{O}}^{Q_1} \omega$

<u>Properties of $\int \omega, \int \omega_J$:</u>

1) $\int^{\sum n_i Q_i} \omega_J = \sum n_i \int^{Q_i} \omega_J$ for any $\sum n_i Q_i \in \mathrm{Div}^\circ X$. (with $Q_i \in X(\mathbb{Q}_p)$).

2) If $\sum n_i Q = \mathrm{div}(f)$ then $\sum n_i \int_0^{Q_i} \omega = 0$

3) If $[D] \in J(\mathbb{Q}_p)_{\text{tors}}$, then $\int^D \omega_J = 0$

4) Suppose X has good reduction at p (not really necessary).

Let t be a uniformizing parameter at $\mathcal{O}$, scaled that it reduces modulo p to a unif. parameter at $\overline{\mathcal{O}} \in X(\mathbb{F}_p)$.

a) $\{Q \in X(\mathbb{Q}_p) : \overline{Q} = \overline{\mathcal{O}}\} \xrightarrow{t} p\mathbb{Z}_p$ is a bijection with analytic inverse.

$$\vec{x}(t) \longleftarrow\!\shortmid\; t$$

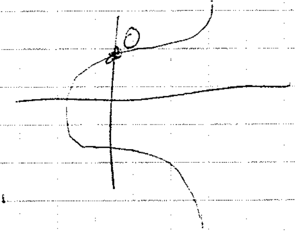
a power series that converges when $t \in p\mathbb{Z}_p$

b) $\omega = \left(\sum_{i \geq 0} a_i t^i\right) dt$ for $a_i \in \mathbb{Z}_p$ (converges for $t \in p\mathbb{Z}_p$).

c) $\int_{\mathcal{O}}^{Q} \omega = \int_0^{t(Q)} \left(\sum a_i t^i\right) dt = \sum_{i \geq 0} a_i \frac{t^{i+1}}{i+1} \in \mathbb{Q}_p$ (where $\overline{Q} = \overline{\mathcal{O}}$)

Example: $X: y^2 = x^5 + 1$, hyperelliptic curve of genus 2.

$\mathcal{O} = (0,1)$.



At $\mathcal{O}$, $t = x$ is a unif. parameter

Take $p = 3$ (X has good reduction at 3).

$\{Q \in X(\mathbb{Q}_3) : \bar{Q} = \bar{\mathcal{O}}\} = \{(x,y) \in \cancel{\mathbb{Z}_3} \times \mathbb{Z}_3 : y^2 = x^5 + 1 \text{ and } \begin{matrix} x \equiv 0 \text{ mod } 3\mathbb{Z}_3 \\ \cancel{x} \equiv 1 \text{ mod } 3\mathbb{Z}_3 \end{matrix}\} =$

$= \{(t, \underbrace{(1+t^5)^{1/2}}_{\text{expand as power series } 1 + \frac{1}{2}t^5 - \frac{1}{8}t^{10} \dots}) : t \in 3\mathbb{Z}_3\}$

A basis for the regular 1-forms are $\frac{dx}{y}$, $\frac{x\,dx}{y}$.

$(3, \sqrt{244})$ ← 3-adic square root, $\equiv 1 \pmod 3$

$$\int_{\mathcal{O}}^{(3,\sqrt{244})} \frac{dx}{y} = \int_0^3 \frac{dt}{(1 + \frac{1}{2}t^5 + \dots)} = \int_0^3 (1 - \frac{1}{2}t^5 - \dots)\,dt = \Big[t - \frac{1}{2}\frac{t^6}{6} \dots \Big]_0^3 =$$

$$= 3 - \frac{1}{2}\left(\frac{3^6}{6}\right) + \dots$$

More properties...

5) If $D \in \mathrm{Div}^0 X_{\mathbb{Q}}$, then $\int^D \omega_J = 0$ (because $[D] \in J(\mathbb{Q}) \subset \overline{J(\mathbb{Q})}$).

Corollary: If $Q, Q' \in X(\mathbb{Q})$, then $\int_Q^{Q'} \omega = 0$.

• Newton Polygons of power series.

Suppose $f(t) = a_0 + a_1 t + \dots$ with $a_0 \in \mathbb{Q}_p$.

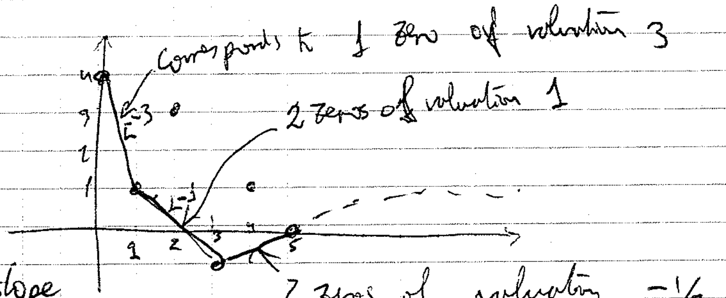
The Newton polygon of f is the lower convex hull of the set of points $(i, v_p(a_i)) \in \mathbb{R}^2$ for $i \geq 0$

Theorem: For every $s \in \mathbb{R}$,

$\#\{\text{zeroes of } f \text{ in } \hat{\bar{\mathbb{Q}}}_p \text{ of valuation } s, \text{ counted with multiplicity}\}$

$\parallel$

horizontal width of the segment of slope $-s$ in the Newton polygon.



Exercise: apply it to $\log(1+t) = t - \frac{t^2}{2} + \frac{t^3}{3} - \dots$

We define a map, given a 1-form ω on $X_{\mathbb{Q}_p}$

$$X(\mathbb{Q}_p) \longrightarrow \mathbb{Q}_p$$
$$P \longmapsto \int_{O}^{P} \omega$$

characterized by:

1) If $[\sum n_i P_i] \in J(\mathbb{Q}_p)_{tors}$ then $\sum n_i \int_O^{P_i} \omega = 0$

2) If $Q, Q' \in X(\mathbb{Q}_p)$ have the same reduction in $X(\mathbb{F}_p)$, then $\int_Q^{Q'} \omega$ can be computed using power series in a local parameter.

3) If $rk(J(\mathbb{Q})) < g$, then $\exists\, \omega \neq 0$ s.t. $\int_Q^{Q'} \omega = 0 \quad \forall Q, Q' \in X(\mathbb{Q})$

<u>Example</u> (Flynn - Poonen - Schaefer 1997, McCallum 1999):

$$X : y^2 = \underbrace{x^6 + 8x^5 + 22x^4 + 22x^3 + 5x^2 + 6x + 1}_{f(x)} \quad /\mathbb{Q}.$$

$g = 2$ (because f is a squarefree).

$\mathrm{disc}(f) = 2^{12} \cdot 3701$

<u>Prop</u>: $J(\mathbb{Q}) \cong \mathbb{Z}$

Pf

$$\left.\begin{array}{l} \# J(\mathbb{F}_3) = 9 \quad \text{(explained in next lecture)} \\ \# J(\mathbb{F}_5) = 41 \end{array}\right\} \Rightarrow J(\mathbb{Q})_{tors} = 0$$

also shows that $J \not\cong E_1 \times E_2$ over $\mathbb{Q}$, because for that we'd need $\# J(\mathbb{F}_5) = \underbrace{\# E_1(\mathbb{F}_5)}_{\text{cannot be } 41} \cdot \# E_2(\mathbb{F}_5)$

(too big for Hasse-Weil bounds, or even too many for the projective space).

$$\frac{J(\mathbb{Q})}{2J(\mathbb{Q})} \subseteq \mathrm{Sel}^2 \simeq \mathbb{Z}/2\mathbb{Z}$$

This implies that $J(\mathbb{Q}) \simeq \mathbb{Z}^r$ for some $r \in \{0, 1\}$.

But $[\infty_+ - \infty_-] \in J(\mathbb{Q})$ is nontrivial, because otherwise

the 2 points at infinity

$[\infty_+ - \infty_-] = \mathrm{div}\, f$, where $f : X \to \mathbb{P}^1$ is of degree $1 \Rightarrow X \simeq \mathbb{P}^1 \Rightarrow !!$

genus 2 $\quad$ genus 1

Theorem: $X(\mathbb{Q}) = \{\infty_+, \infty_-, (0,\pm 1), (-3, \pm 1)\}$.

Pf: Chabauty's method with $p=3$.

$X(\mathbb{F}_3) = \{\infty_-, \infty_+, (0,\pm 1)\}$

ω is a $\mathbb{Q}_p$-linear combination of $\frac{dx}{y}$, $x\frac{dx}{y}$, which one?

$$\int_{(0,1)}^{(-3,1)} \frac{dx}{y} = \int_0^{-3} (1 + 6x + 5x^2 + \cdots)^{-1/2}\, dx = \int_0^{-3} \underbrace{(1 - 3x + 11x^2 - 56x^3 + \cdots)}_{\text{coeff's in } \mathbb{Z}_3} dx =$$

$$= \left[x - \frac{3x^2}{2} + \frac{11x^3}{3} \cdots\right]_0^{-3} = -3 - \frac{3}{2}(3^2) + \cdots \equiv -3 \pmod{3^2}$$

↑ this is enough precision for what we'll do.

$$\int_{(0,1)}^{(-3,1)} x\frac{dx}{y} = \cdots \equiv -9 \pmod{3^3}$$

Therefore, up to a scalar multiple that doesn't matter,

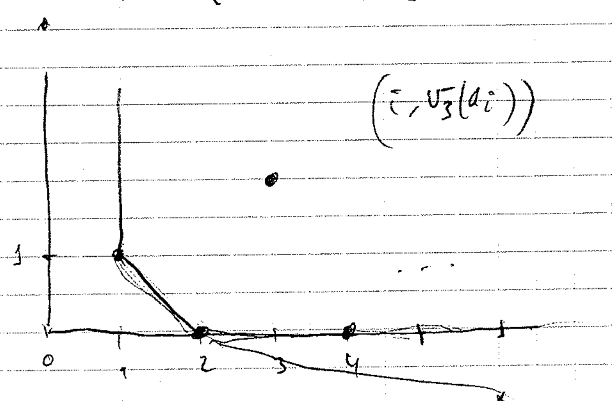
$$\omega = \varepsilon \frac{dx}{y} + x\frac{dx}{y} \quad \text{where} \quad (-3 + \cdots)\varepsilon + (-9 + \cdots) = 0 \text{ in } \mathbb{Q}_3$$

so $\varepsilon \equiv -3 \pmod 9$

For $t \in 3\mathbb{Z}_3$

$$I(t) = \int_{(0,1)}^{(t, (1+6t+\cdots)^{1/2})} \omega = \int_0^t (\varepsilon + x)(1 + 6x + \cdots)^{-1/2}\, dx =$$

$$= \varepsilon t + (-3\varepsilon + 1)\frac{t^2}{2} + (11\varepsilon - 3)\frac{t^3}{3} + (-56\varepsilon + 11)\frac{t^4}{4} + \cdots$$



$\{$zeros of valuation $\geq 1\} \longleftrightarrow \{$segments of slope $\leq 1\} \Rightarrow$ at most 2 zeros!

So $I(t)$ has at most 2 zeros in $3\mathbb{Z}_3$.

Therefore, $t=0, t=-3$ are the only zeros of $I(t)$. //

Exercise:

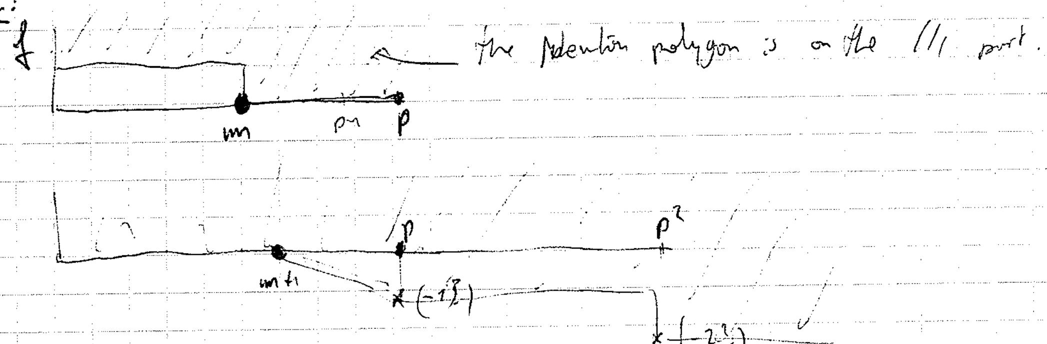
Suppose $f = \sum a_i t^i \in \mathbb{Z}_p[[t]]$

Let $m := \mathrm{ord}_{t=0}(f \bmod p)$.

If $p > m+2$,

then the power series $\int f = \sum_{i \geq 0} \frac{a_i t^{i+1}}{i+1}$ has at most $m+1$ zeros in $p\mathbb{Z}_p$.

Solution:



So past the point $(m+1)$ there are no segments of slope ≤ -1.

Corollary: (Coleman's Theorem, 1985)

$X/_{\mathbb{Q}} \hookrightarrow J$, of good reduction at a prime $p > 2g$

Assume also $\mathrm{rk}\, J(\mathbb{Q}) = r < g$.

Choose $\omega \neq 0$ st. $\int \omega$ vanishes on $X(\mathbb{Q})$.

Scale ω st. $(\omega \bmod p)$ is a nonzero regular 1-form (on $X \bmod p$).

Then: $\# X(\mathbb{Q}) \leq \# X(\mathbb{F}_p) + (2g-2)$.

Pf

- Chose ω ...
- The number of zeros of $(\omega \bmod p)$ (with multiplicity) is $= 2g-2$.

By the exercise, $p > (2g-2)+2 \Rightarrow$

$\#\{\mathbb{Q}\text{-points on } X \text{ reducing to } \bar{x} \in X(\mathbb{F}_p)\} \leq \mathrm{ord}_{\bar{x}}\, \omega + 1$.

Sum over $\bar{x} \in X(\mathbb{F}_p)$: so $\# X(\mathbb{Q}_g) \leq 2g-2 + \# X(\mathbb{F}_p)$. //

- Problems with Chabauty's method

1) Not every point in $X(\mathbb{Q}_p) \cap \overline{J(\mathbb{Q})}$ will be in $X(\mathbb{Q}_p)$.

This is a common problem when $r = g-1$.

2) If $X(\mathbb{Q}_p)$ and $\overline{J(\mathbb{Q})}$ are tangent, this might foil any attempt to compute $\#\left(X(\mathbb{Q}_p) \cap \overline{J(\mathbb{Q})}\right)$. This is a less practical problem. (not serious in practice.

- Descent via unramified covers.

Example: (Flynn):

Let X be the smooth proj. model of $y^2 = (x^2+1)(x^4+1)$ / $\mathbb{Q}$.

and we want to find its rational points.

General fact:

$X: \quad y^2 = f(x^2) \quad \deg f = 3$

There is an obvious morphism $X \longrightarrow E: y^2 = f(t)$

$(x,y) \mapsto (x^2, y)$

Also $X \simeq \left(y^2 = f^{rev}(x^2)\right) X'$

and this X' has a map to $E': y^2 = f^{rev}(T)$.

E and E' have nothing in common and $J \sim E \times E'$.

In our case, X and X' are the same, so $J \simeq E \times E$

where $E: y^2 = (x+1)(x^2+1)$.

$rk(E(\mathbb{Q})) = 1 \Rightarrow rk\, J(\mathbb{Q}) = 2$.

Also genus $X = 2$ so cannot use Chabauty's method.

Elementary argument:

write $x = \dfrac{X}{Z}$, $X, Z \in \mathbb{Z}$ $\gcd(X,Z) = 1$.

$y = \dfrac{Y}{Z^3}$ $\gcd(Y, Z) = 1$

we get $Y^2 = (X^2+Z^2)(X^4+Z^4)$

Claim: $\gcd(X^2+Z^2, X^4+Z^4)$ is a power of 2.

Pf: Suppose p is an odd prime dividing both.

Then $Z^2 \equiv -X^2 \pmod p$

$Z^4 \equiv -X^4 \pmod p$

$$\left.\begin{array}{l} 2X^4 \equiv 0 \pmod p \\ 2\cancel{Z}^4 \equiv 0 \pmod p \end{array}\right\} \Rightarrow p \mid X^4,\ p \mid Z^4 \Rightarrow !!$$

So we have $X^4+Z^4 = cW^2$ where $c \in \{\pm 1, \pm 2\}$

Divide by $Z^4 \Rightarrow E_c: \ cw^2 = x^4+1 \qquad c=1,2$

E_1, E_2 are <u>both</u> elliptic curves. Can find the Weierstrass equations.

They have both rank 0.

This allows us to find $X(\mathbb{Q}) = \{(0,\pm 1), \dots\}$.

<u>Explanation:</u>

Let Z be the smooth projective model of $\begin{cases} y^2 = (x^2+1)(x^4+1) \\ w^2 = x^4+1 \end{cases}$

$$k(Z) = \mathbb{Q}\left(x, \sqrt{x^2+1}, \sqrt{x^4+1}\right) \supseteq \mathbb{Q}\left(x, \sqrt{(x^2+1)(x^4+1)}\right) = k(X).$$

For $c \in \mathbb{Q}^*$, can define:

$$Z_c: \begin{cases} y^2 = (x^2+1)(x^4+1) \\ cw^2 = x^4+1 \end{cases}$$ (a quadratic twist of Z).

We have a degree-2 morphism

$$\begin{array}{ccc} Z_c & (x,y,w) & \\ {\scriptstyle f_c}\downarrow & \downarrow & \\ X & (x,y) & \end{array}$$ is a twist of $\begin{array}{c} Z \\ \downarrow \\ X \end{array}$

The elementary argument was:

- Each point of $X(\mathbb{Q})$ is in the image of $f_c: Z_c(\mathbb{Q}) \to X(\mathbb{Q})$ for some $c \in \mathbb{Q}^*/\mathbb{Q}^{*2}$
- Up to multiplication of c by elements of $\mathbb{Q}^{*2}$, there are only finitely many $\overset{\mathbb{Q}^*}{\check{c}}$ such that Z_c has $\mathbb{Q}_p$-points for all $p \leq \infty$. This set of c can be computed effectively.

So what we did is reduce the problem of finding $X(\mathbb{Q})$ to the problem of determining $Z_c(\mathbb{Q})$ for finitely many $c \in \mathbb{Q}^*$.
In this example it was easier to compute the rational points of the genus-3 curves than one genus-2 curve. This was because

$Z_c \searrow E_c \leftarrow$ genus 1.

<u>Key of argument:</u> $\begin{array}{c} Z \\ \downarrow \\ X \end{array}$ is an unramified covering such that $\begin{array}{c} \bar{Z} \\ \downarrow \\ \bar{X} \end{array}$ is Galois.

<u>Abhyankar's Lemma:</u>

X, Y, X', Y' smooth projective geometrically curves $/ k = \bar{k}$

$$\begin{array}{ccc} X' & \longrightarrow & X \\ \downarrow & & \downarrow \pi \\ Y' & \xrightarrow{\phi} & Y \end{array}$$

suppose $k(X')$ is the composition of $k(X)$ and $k(Y')$ over $k(Y)$.

Assume also that $\forall\, x \in X(k)$, $y' \in Y'(k)$ with $\pi(x) = \phi(y')$,

$e_\phi(y') \mid e_\pi(x)$ and $\operatorname{char} k \nmid e_\phi(y')$. (tame ramification).

Then $X' \longrightarrow X$ is unramified.

(in the example, $k(Z) = \mathbb{Q}(x, \sqrt{\ }, \sqrt{\ }) \leftarrow$ unramified

$$\begin{array}{ccc} \mathbb{Q}(x, \sqrt{(x^2+1)(x^4+1)}) = k(X) & & \\ | & \diagdown & \\ \mathbb{Q}(x, \sqrt{x^4+1}) & - & \mathbb{Q} \end{array}$$

).

(in number fields:

$$\begin{array}{ccc} \mathbb{Q}(\sqrt{3}, \sqrt{5}) & & \\ | & \diagdown & \\ & & \mathbb{Q}(\sqrt{15}) \\ \mathbb{Q}(\sqrt{5}) & & | \\ & \diagdown & \\ & & \mathbb{Q}. \end{array}$$

)

Geometric class field theory.

Work over $k = \bar{k}$

$$\begin{tikzcd} Z \arrow[r, dashed] \arrow[d] & A \arrow[d, "\pi\ \text{separable isogeny}"] \\ X \arrow[r] & J \end{tikzcd}$$

and Z the fiber product of this diagram.
(in this case $Z = \pi^{-1}(X)$).

If π is separable isogeny then $A \to J$ is unramified and abelian extension.
And this will make $Z \dashrightarrow X$ an unramified abelian extension.

What class field theory says is that all unramified abelian extension arise in this way.

<u>Thm</u> (Geom. C.F.T.)

All unramified abelian covers of X arise in this way.

<u>Examples of isogenies</u>: $J \xrightarrow{n} J$ when char $k \nmid n$. (to make them separable).

- Weil Conjectures

- Examples:

1) $\mathbb{P}^d(\mathbb{F}_q) = \dfrac{(\mathbb{F}_q)^{d+1} - \{0\}}{\mathbb{F}_q^*} \Rightarrow \#\mathbb{P}^d(\mathbb{F}_q) = \dfrac{q^{d+1}-1}{q-1} = 1 + q + \cdots + q^d$

Similarly, $\#\mathbb{P}^d(\mathbb{F}_{q^n}) = (1)^n + (q)^n + (q^2)^n + \cdots (q^d)^n$

2) E elliptic curve $/\mathbb{F}_q$.

By Hasse, $\#E(\mathbb{F}_{q^n}) = 1 - (\alpha^n + \beta^n) + q^n$

complex numbers, $|\alpha| = |\beta| = q^{1/2}$, and $\alpha\beta = q$.

1(&2) X smooth ~~d~~ d-dimensional projective variety $/\mathbb{C}$.

$X(\mathbb{C})$ is a $\begin{cases} \text{complex manifold of dim } d \\ \text{real manifold of dim } 2d \end{cases}$

$b_i := \operatorname{rk} H^i(X(\mathbb{C}), \mathbb{Z})$

For $\mathbb{P}^d(\mathbb{C})$,

i	0	1	2	---	2d
b_i	1	0	1	...	1

For $E(\mathbb{C})$

i	0	1	2
b_i	1	2	1

Theorem:

i) X variety $/\mathbb{F}_q$. Then, $\exists\, \alpha_1, \ldots, \alpha_r, \beta_1, \ldots, \beta_s \in \overline{\mathbb{Z}}$ ← ring of all algebraic integers.

such that $(\forall n \geq 1)$ $\#X(\mathbb{F}_{q^n}) = \alpha_1^n + \cdots + \alpha_r^n - \beta_1^n - \cdots - \beta_s^n$

ii) If, in addition, X is a smooth projective variety of dimension d, $\forall n \geq 1$

$$\#X(\mathbb{F}_{q^n}) = (\alpha_{01}^n + \cdots + \alpha_{0,b_0}^n) - (\alpha_{11}^n + \cdots + \alpha_{1,b_1}^n) + \cdots (\alpha_{2d,1}^n + \cdots + \alpha_{2d,b_{2d}}^n)$$

Where:
- the $b_i \in \mathbb{Z}_{\geq 0}$ satisfy $b_{2d-i} = b_i$
- the $\alpha_{ij} \in \overline{\mathbb{Z}}$ are such that, for each i, the $\alpha_{2d-i,*}$ equal the values $\dfrac{q^d}{\alpha_{i,*}}$, in some order.
- $|\alpha_{ij}| = q^{i/2}$ ($|\cdot|$ is any archimedean absolute value on $\mathbb{Q}(\alpha_{ij})$).
- $\alpha_{i1}^n + \cdots + \alpha_{i,b_i}^n = \operatorname{Tr}(\mathrm{Frob}^n \mid H^i_{\acute{e}t}(\overline{X}, \mathbb{Q}_\ell))$.

(ctd)

Moreover, if X is also geometrically irreducible, then

$b_0 = 1$, $\alpha_{0,1} = 1$

$b_{2d} = 1$, $\alpha_{2d,1} = q^d$

(iii) Let k be a number field with $k \hookrightarrow \mathbb{C}$. X smooth, projective variety $/k$.

Let $\mathfrak{p}$ be a prime of good reduction (?)

Let $\mathbb{F}_q = \mathcal{O}_k/\mathfrak{p}$.

Then the b_i in (ii) equals $\operatorname{rk} H^i(X(\mathbb{C}), \mathbb{Z})$ (the topological Betti numbers).

Example:

X curve (smooth, proj, geom. irr) of genus g.

Over $\mathbb{C}$, we have $H^0(X(\mathbb{C}), \mathbb{Z}) = \mathbb{Z}$

$H^1(X(\mathbb{C}), \mathbb{Z}) = \mathbb{Z}^{2g}$ (dual to $H_1(X(\mathbb{C}), \mathbb{Z})$)

$H^2(X(\mathbb{C}), \mathbb{Z}) = \mathbb{Z}$

So $b_0 = 1$, $b_1 = 2g$, $b_2 = 1$ for any curve as above over $\mathbb{F}_q$.

It implies (a little more work) that $\# X(\mathbb{F}_{q^n}) = 1 - (\lambda_1^n + \dots + \lambda_{2g}^n) + q^n$

where $|\lambda_i| = q^{1/2}$ and $\lambda_{g+i} = \dfrac{q}{\lambda_i}$ for $i = 1, \dots, g$

can still be real! (but in pairs)

Zeta functions

- Riemann zeta function: For $\operatorname{Re} s > 1$, $\zeta(s) = \zeta_{\operatorname{Spec}\mathbb{Z}}(s) := \sum_{n \geq 1} n^{-s} = \dots$

$$\dots = \prod_{\text{prime } p} (1 - p^{-s})^{-1} \quad \text{(Euler product)}$$

$$= \prod_{\substack{\mathfrak{m} \subset \mathbb{Z} \\ \text{maximal}}} \left(1 - \left(\# \mathbb{Z}/\mathfrak{m}\right)^{-s}\right)^{-1}$$

- $$\zeta_{\mathbb{A}^1_{\mathbb{F}_q}}(s) = \zeta_{\operatorname{Spec}\mathbb{F}_q[t]}(s) := \prod_{\substack{\mathfrak{m} \subseteq \mathbb{F}_q[t] \\ \text{maximal}}} \left(1 - \#\left(\frac{\mathbb{F}_q[t]}{\mathfrak{m}}\right)^{-s}\right)^{-1} =$$

$$= \prod_{\substack{\text{monic irreducible} \\ \text{polynomials } f \in \mathbb{F}_q[t]}} \left(1 - \left(q^{\deg f}\right)^{-s}\right)^{-1} = \prod_{\substack{\text{irred 0-dim subvars} \\ P \subseteq \mathbb{A}^1_{\mathbb{F}_q}}} \left(1 - (q^{-s})^{\deg P}\right)^{-1}$$

We can substitute $T = q^{-s}$, and a irred. 0-dim subvar is a closed point, so

$$\zeta_{\mathbb{A}^1_{\mathbb{F}_q}}(s) = \prod_{\substack{\text{closed points} \\ P \in \mathbb{A}^1_{\mathbb{F}_q}}} \left(1 - T^{\deg P}\right)^{-1} \in \mathbb{Z}[[T]]$$

Def: X any variety $/\mathbb{F}_q$,

$$Z_X(T) := \prod_{\substack{\text{closed points} \\ P \in X}} \left(1 - T^{\deg P}\right)^{-1}$$

$$\zeta_X(s) := Z_X(q^{-s})$$

Can prove that $Z_X(T)$ converges for Re s sufficiently positive ($s \in \mathbb{C}$)

We are going to reformulate the Weil conjectures in terms of $Z(T)$.

Let $N_d :=$ # closed points of degree d on X. $=$ # $Gal(\overline{\mathbb{F}_q}/\mathbb{F}_q)$-orbits of size d in $X(\overline{\mathbb{F}_q})$.

Then, $X(\mathbb{F}_{q^n}) = \overset{\text{disjoint}}{\dot{\bigcup_{d|n}}} \begin{pmatrix} \text{all orbits of} \\ \text{size } d \end{pmatrix}$, So, $\# X(\mathbb{F}_{q^n}) = \sum_{d|n} d N_d$

Plugging it in the expression of Z_X, exercise

$$Z_X(T) = \prod_{d \geq 1} \left(1 - T^d\right)^{-N_d} = \exp\left(\sum_{n=1}^{\infty} \# X(\mathbb{F}_{q^n}) \frac{T^n}{n}\right)$$

- Weil conjectures in terms of $Z_X(T)$

i) $Z_X(T)$ is the Taylor series of a rational function ($\in \mathbb{Q}(T)$).

$$\frac{(1-\beta_1 T) \cdots (1-\beta_s T)}{(1-\alpha_1 T) \cdots (1-\alpha_r T)} \quad \text{(rationality of } Z_X)$$

ii) If X is smooth proj. of dimension d, then $Z_X(T) = \dfrac{P_1(T) \cdots}{P_0(T) P_2(T) \cdots P_{2d}(T)}$

where $P_i \in 1 + T\mathbb{Z}[T]$; $\deg P_i = b_i$, $b_{2d-i} = b_i$

and over $\mathbb{C}$, $P_i(T)$ factors as $\prod_{j=1}^{b_i} (1 - \alpha_{ij} T)$; $|\alpha_{ij}| = q^{i/2}$ ← Riemann Hypothesis

and $Z_X\left(\frac{1}{q^d T}\right) = \pm q^{\frac{d\varepsilon}{2}} T^{\varepsilon} Z_X(T)$ ← functional equation, where $\varepsilon = b_0 - b_1 + b_2 - \cdots + b_{2d}$ (Euler characteristic)

iii) If, in addition, X is geom. irreducible, then $P_0(T) = 1 - T$; $P_{2d}(T) = 1 - q^d T$.

Notice the same for "Riemann Hypothesis": if X is a curve $/\mathbb{F}_q$,
$Z_X(T)=0 \Rightarrow |T| = q^{-1/2} \Leftrightarrow |q^{-s}| = q^{-1/2} \Leftrightarrow \operatorname{Re} s = 1/2$.

<u>Example</u>: X curve of genus g (sm, proj. geom irr.)

$$Z_X(T) = \frac{P_1(T)}{(1-T)(1-qT)} \quad \text{where} \quad P_1(T) = \prod_{i=1}^{2g}(1-\alpha_i T)$$

and $|\alpha_i| = \sqrt{q}$

The functional equation says $P(T) = 1 + a_1T + a_2T^2 + \dots + \overset{\text{middle}}{a_g T^g} + q a_{g-1} T^{g+1} + \dots + q^g T^{2g}$

Naive algorithm for computing $P(T)$ for a curve X:

Compute $\# X(\mathbb{F}_{q^n})$ for $n = 1, 2, \dots, g$ (by counting!).

Compute $P(T) = (1-T)(1-qT)\, Z_X(T)$ where $Z_X(T) = \exp\left(\sum_{n=1}^{g} \# X(\mathbb{F}_{q^n}) \frac{T^n}{n} + O(T^{g+1})\right)$.

$$= 1 + a_1 T + a_2 T^2 + \dots + a_g T^g + O(T^{g+1})$$

and put the other coefficients $a_{g+1} - a_{2g}$ using the symmetry.

- Connection with $J = \operatorname{Jac} X$. If V has basis $e_1, \dots, e_n$, then $\Lambda^m V$ has basis $e_{i_1} \wedge \dots \wedge e_{i_m}$, $1 \le i_1 < \dots < i_m \le n$.

<u>Fact</u>: $H^m_{ét}(\bar{J}, \mathbb{Q}_\ell) \cong \Lambda^m H^1_{ét}(\bar{X}, \mathbb{Q}_\ell)$

If the eigenvalues for F on $H^1_{ét}(\bar{X}, \mathbb{Q}_\ell)$ are $\alpha_1, \dots, \alpha_{2g}$,
then the eigs for F on $\Lambda^m H^1_{ét}(\bar{X}, \mathbb{Q}_\ell)$ are $\alpha_{i_1}\alpha_{i_2}\cdots\alpha_{i_m}$ for $i_1 < \dots < i_m$

So $\operatorname{Tr}(F \mid H^m_{ét}(\bar{J}, \mathbb{Q}_\ell)) = m^{th}$ symmetric polynomial in $\alpha_1, \dots, \alpha_{2g}$.

$$\boxed{\# J(\mathbb{F}_q)} = \operatorname{Tr}(F \mid H^0) - \operatorname{Tr}(F \mid H^1) \cdots + \operatorname{Tr}(F \mid H^{2g}) =$$

$$= 1 - \sum \alpha_i + \sum_{i_1 < i_2} \alpha_{i_1}\alpha_{i_2} - \dots + \alpha_1 \cdot \alpha_2 \cdots \alpha_{2g} = (1-\alpha_1)(1-\alpha_2)\cdots(1-\alpha_{2g})$$

$$\boxed{= P(1)}$$

To compute $\#J(\mathbb{F}_{q^2})$, first find the P for $X_{\mathbb{F}_{p^2}}$ (call it $P_{(2)}$) and plug $T=1$ in it.

The zeros of $P_{(2)}(T)$ are the squares of the zeros of $P(T)$.

$$P_{(2)}(T) = \mathrm{Res}_u \left(P(U), U^2 - T \right)$$

<u>Example</u>: H smooth hypersurface in $\mathbb{P}^{d+1}$.

Then H has the same cohomology as $\mathbb{P}^d$, except in the middle (i.e H^d).

$$Z_{\mathbb{P}_d}(T) = \frac{1}{(1-T)(1-qT)\cdots(1-q^dT)}$$

$$Z_H(T) = \frac{1}{(1-T)(1-qT)\cdots(1-q^dT)\,Q(T)^{(-1)^d}}$$ ← may be in the numerator if d is odd.

where $Q(T) = \prod_i (1 - \alpha_i T)$ with $|\alpha_i| = q^{d/2}$